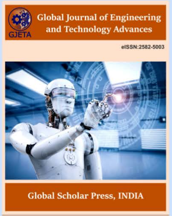
Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/



(Research Article)

Leveraging artificial intelligence to mitigate money laundering risks through the detection of cyberbullying patterns in financial transactions

Shuvo Kumar Mallik [1, *], Md. Raisul Islam [2], Imran Uddin [3], Md. Azam Ali [4] and Sadia Maliha Trisha [5]

[1] *Department of Economics, Southeast University, Dhaka, Bangladesh.*
[2] *Associate Professor, Department of Law and Land Administration, University of Rajshahi, Bangladesh.*
[3] *A2Z Finance Australia (Easy Mortgage Solutions Australia), Australia.*
[4] *Department of Marketing, Jagannath University, Dhaka, Bangladesh.*
[5] *Dublin Business School, Dublin, Ireland.*

Global Journal of Engineering and Technology Advances, 2025, 22(01), 094-115

Publication history: Received on 10 December 2024; revised on 21 January 2025; accepted on 24 January 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.22.1.0015

Abstract

Money laundering (ML) is a vital source to clean the money from the financial system with illegal funds. Corruption, exploitation of a given community, drug use, and much more are all associated with it. Due to the massive number of transactions worldwide, detection of ML operations is complex. But it makes it possible for criminals to exploit financial systems to facilitate illicit transactions. This is primarily about reducing the risk that someone will be out of pocket because of money laundering. AI- driven applications of AML tools are now monitoring transactions to deal with it. In total, 112 research papers are reviewed (identified the gap in literature) which serves as a guide for the future direction of this research domain. The outcome of this systematic literature review effort will not only pave the way for the research community, also aid the state agencies to formulate an ideal AML ecosystem to tackle these prominent concerns while ensuring a healthy environment for their inhabitants. Those starting points can be taken to evaluate the current state of affairs from diverse perspectives and pave the way towards future research directions to explore and develop the high levels of authenticity and security that artificial intelligence (AI) can bring to the finance sector.

Keywords: Money Laundering; AI- Driven; Financial Systems; Artificial Intelligence (AI)

1. Introduction

The ability of AI to automate functions that many have come to think of as “tedious” is yielding tremendous dividends, such as freeing up time for those seeking to collect money to do vital donor engagement and strategy. While the phrases may seem to read like generic buzz words, AI, data analytics and machine learning (ML) are being woven into organization technology systems as innovative approaches to challenges in risk management, human resources and compliance. Ageing-and-banking-sector Fraud: It is common for many industries to lose millions of dollars to fraud every year, including banking and financial institutions

insurance companies, government agencies, telecommunication industries, and law enforcement (Jamshidi and Reza Hashemi 2012). We exist in a tradition that criminal circumstances against senior people are frequently rising. With the increasing level of dangers and incursions in society, desperation for a security system to help assure their well-being and safety is becoming more common. The opposite, global result in terms of cyber hazards (Suresh et al. 2020). It may pay off well to engage in criminal activities, like smuggling, bribery and drug trafficking. Illegally acquired money must be disguised as legitimate before it can be spent freely (Wang and Yang 2007). Fraud detection is a popular topic in the data mining community. Fraudulent transactions are often characterized by a high degree of sophistication.

[*] Corresponding author: Shuvo Kumar Mallik.

There are extremely unusual in a huge chunk of regular transactions, and manipulators are thoroughly planned and far dropped (Kunlin 2018). Detecting fraud can be a pretty hard job for a lot of businesses. Due to easy accessibility to personal information and sophisticated password cracking techniques, hackers can commit online fraud easily. In this case, customers lose billions of dollars each year due to online transaction fraud (Song 2020). The damage inflicted on the banks and their customers as a result of fraud has increased the need for fraud detection and prevention technology. Fraud detection systems are increasingly using AI and machine learning techniques (Erdoğan et al. 2020; Guevara, Garcia-Bedoya and Granados 2020).

Hamid, Ali R. (2017). The National Law Review. It is the risk used for laundering illegal proceeds so it can be reinjected into the authorized financial system or used to fund other illegal activity (Ketenci et al. 2021). Money laundering is the process of switching dirty money to clean money. The money, for instance, comes from illegal activities such as human trafficking, kidnapping, hired assassination, bribes, tax evasion, and drug dealing. This is because an organization or an individual cannot deposit money directly into a bank, for the bank sees the transaction as anomalous, and the user cannot prove the origin of the money. This money is termed as "black money" which has an adverse effect on the economy. This is why the anti-money laundering regulations are rather stringent among the two sides of the coin, emerging and wealth countries (Samanta et al. 2019). ML is the practice of making illegal earned income appear to be legitimate, a process used by criminal offenders to hide the illegal origin and ownership of their criminally-obtained assets. It is now a serious threat to the financial system and the nation as a whole. This nefarious activity is becoming more sophisticated all the time, and, yes, has grown beyond the cliché of smuggling of drugs to include financing of terrorists and, of course, personal profit. Money laundering refers to the process of the act of criminals trying to disguise illegally obtained funds using of a legitimate source like as large investment or pension funds or investing in banking products (Le Khac, Markos, and Kechadi 2010).

Money laundering is a huge metropolitan menace, and the identification of illegal financial transactions through ML applications is tough and time-consuming. However, most current anti-money laundering (AML) systems are limited to link analysis, networking analysis, risk scoring categorization and outlier detection to identify suspicious transactions (Thi et al. 2020). Re-attachment of a criminal analysis is a complicated operation, requiring to process large amount of data and from many data sources, for example from billings or from bank account activities, what collect information useful in the view of an investigator (Dreżewski, Sepielak, Filipkowski 2015). Definition. AML systems are used by financial institutes (e.g., banks and other credit-issuing institutions) for the purpose of combating money laundering by detecting risks, transactions, and potential money launderers (Han et al. 2020). The FAIS (AI System) of the American Financial Crime Enforcement Network utilized a combination of human intelligence and software agents to detect suspected ML across a large data landscape. The use of such computer analysis system in artificial intelligence can significantly increase work efficiency and is an important means for the development of anti-money laundering (AML) system (Wang and Yang 2007).

AI is a phrase that has been used a lot in science fiction, but now it is more commonly known as it has become more part of our daily life. Some of the Fast-Retiring Sectors Include Transportation, Healthcare, Retail And Finance A word processor AI drive heuristically a pc with the exact features to animated a variety of individual-intellectual responsibilities, just as observing, making, thinking and difficulties in 1955. In modern era, various businesses have been developed with the help of AI applications (Guan, Mou and Jiang 2020). Money laundering has been identified since increased reporting of large transactions by financial institutions to the public department in 1970 (Soltani et al. 2016). Money laundering prevention systems are employed by financial institutions (banks and other credit suppliers do such) to fight money laundering (ML) which they do by ways of identification risks, transactions, and identifying money launderers (Han et al. 2020). These papers were reviewed to see if they:

- List all the tools & channels used for ML in the financial sector;
- Recognize proposed AI-based generic solutions to restrict money laundering;
- Several indicators that denote the risk of money laundering; and
- Explain the economic and social effects of ML on the society and on various financial sectors.

This is mainly to mitigate the actual threats associated with ML. To counter this, anti- money laundering systems are relying on AI-driven apps that best track transactions. Main issues and concerns include the security and safety of the financial sector from ML. Embedding security into AI-based applications seems to be the solution for them to achieve this goal.

The word ML confines to separating criminal proceeds from their sources; or to make money, earned through unlawful means, seem legal or clean (Bashir et al. 2020). It is also defined as "the process of moving illegally gained funds through a legitimate person or an account so that it can no longer be traced to its illegal source." It is a worldwide issue that has caused political upheaval and impeded economic development. It remains a constant worry for many officials in many countries. There are several techniques that can be used to perform money laundering. The first is in the import and export sectors, which are routes through which money can be converted into goods and then exported or legitimately brought back into the country (Alnasser Mohammed 2021). The fight against money laundering has almost come to dominate the anti-crime policy agenda in recent years (Rusanov and Pudovochkin 2021). All human trafficking and acts of drug, bribery, extortion, kidnapping-for- ransom, terrorist financing, tax evasion, and others are indeed linked to ML (Ketenci et al. 2021). Due to its severity, it is receiving growing interest from scholars and governments worldwide. Partly, ML-related money represents a significant percentage of the global GDP each year (Xie et al. 2010). Such a huge, complex and deep underground market is nearly impossible to estimate exactly; around two trillion USD (International Monetary Fund (IMF) (Hunter and Biglaiser 2020)) are laundered every year through financial institutes around the world, securing ML the spot as one of the biggest markets in the world. 2021). Money laundering is believed to be worth around $3.2 trillion (or 3 percent of global GDP) per year according to the IMF. Earnings from money laundering are commonly used to finance criminal activities including illegal arms trading, drug trafficking, human trafficking and terrorist attacks (Han et al. 2020). The FIU (the Financial Intelligence Unit) receives reports from financial organizations on suspicious actions. FIU collects information from various financial sectors, both inside and outside the authority, and communicates to law enforcement authorities (LEA) when appropriate (Ketenci et al. 2021). Fraud detection is a crucial component in minimizing losses. Hard-hitting security software aren't as the fraudsters conquer their invasion by evading with their rotten evasions and by making state-of-the-art fraudulent techniques. Fraud in bank is a type of federal offense that may include deceiving financial institutions to obtain a monetary benefit as a result of someone else's actions. Fraud costs banks and Fintech's billions of dollars every year. Scams that have elements of bribery where bankers are lured to earn financial assets.

Banks and insurance firm are a favorite target for fraudsters. They capture billions of dollars in financial resources every year. The common types of bank fraud are Credit and debit card fraud, False selling insurance, Money laundering, Account fraud (Sarma et al. 2020). Worldwide, there is a concerted global effort to defend these financial organizations from the increasing use by terrorists of nonprofit organizations (NPOs). In order to assist other countries in assessing the adequacy of their current laws and regulations concerning nonprofit organizations, the FATF (Financial Action Task Force) published Special Recommendation (SR) VIII (Molla Imeny et al. 2021; Omar, Johari, and Arshad 2014; Savona and Riccardi 2019). The performance of a country's financial institution evaluates its compliance with the FATF 40 + 90 (Choo 2014) guidelines and a full evaluation report serves as the instrument to enable each country to draft its AML rules that comply with the system (Young and Woodiwiss 2021). Enhanced due diligence in the United States covers the monitoring of risky and terrorism-related funding and customer identification in high-risk jurisdictions and large banks' transactions. This has lead to a dirigisme policy- that suits many G20 submitting nations to collect and distribute information - crypto currency around the world may soon free banking bodies to be globally managed with vast amounts of alternative deposits and transactions that are growing outside the limits of needing to be identified by those participating in G20 and other 'good guys' within donation Terrorism or the AML/CFT system to completely harmonize globally collecting information on events/trends of terrorism finance especially in the poorer regions that have increasingly included less complicated solutions provided by banks (Bashir et al. 2020).

Technologies in this space have given rise to a number of new challenges that regulators and others are playing catch-up to respond to. Economic rationality can push people to commit acts of AI and to legitimize the operations of AI (Gudkov 2020). Due to conventional security breaches and the concerns over how firms handle personal data extracted from customers or ordinary users, Cybersecurity has become a fundamental subject. (2) One of the most basic principles of cybersecurity in banking transactions is the protection of client assets while meeting tight data privacy normative requirements. Not only technologically, but also legally and ethically, the development of AI poses many challenges (Nizioł 2021). It is considered a threat to jobs because it will replace manual labor. Financial services are under threat as well (Lee 2020). AI and machine learning are rapidly changing and shaping emerging nations political, economic, and social fabric. Consequently, experts believe that AI-based solutions will be a game-changer with significant implications for increasing financial inclusion of poor individuals (Garcia- Bedoya, Granados, and Cardozo Burgos 2021; Kshetri 2021). —It has become a crucial resource for big banks grappling with regulatory shifts, heightened anti-money laundering (AML) laws, and target-theft infiltration-prone consumers. Internet banking is convenient, but it also brings serious issues (Jullum et al. 2020). Concurrently, Internet banking security has collected the consideration of individuals from varying backgrounds Although many of day-to-day exchange of money is done in many non-cash payment methods (such as E-Cash, Debit/Credit cards, Mobile Payment Systems, etc.), but in many situations confidentiality and availability of payment information has been there. Such incidents can happen on the client (funds owners) as well as the bank (or outlet) side and also, during the transfer of payment information in communication networks (Plaksiy, Nikiforov and Miloslavskaya 2018).

1.1. Research Protocol

SLR is established method of identifying and evaluating research output relevant to a specific research question. SLR attempts to provide an unbiased assessment of a research problem by adopting a rigorous, reliable, and auditable process (Kitchenham 2004). SLR has been disseminated in several fields, such as FinTech, remittance (Hussain et al. 2020) and health care systems (Nazir et al. 2020). The objective of this SLR approach is to reconstruct the application of machine learning and AI in financial institutions to prevent the likelihood of money laundering. The following bullets show the key to explain this SLRs purpose:

- Emission of the exploratory research and inquiry into previous studies of the technology. The above set of questions was formulated using the AI at hand, on the premise of providing high security and authentication mechanism in different fields of business to mitigate the threat of Machine learning.
- To discover needs in technology that will cause further research These new domain will help the business sectors and its employees by providing great level of authentication for the security purposes to avoid money laundering.
- All the selected articles from online libraries are the most suitable ones for this SLR work. (2) Researchers will critically evaluate the fundamental research articles in AI and ML fields.

The SLR approach followed in this prospective research effort follows the proposed guidelines suggested by Kitchenham et al. (Keele 2007; Kitchenham et al. 2010). The process uses in this SLR review methodology is shown in figure 1. As shown in Figure 1, the review process comprises of seven important steps and all of the stages are described in detail.

2. Research Process Methodology

Systematic literature review (SLR) emphasizes the vital aspects of pre-review processes (research question formulation, identifying keywords, error formulation in question selected by considering publication of the digital libraries available on the web for the inclusion/exclusion criteria for the original articles for the review process). The current systematic review was conducted due to the recent increase in the research interest associated with AI and money laundering. With a strong research approach and literature review knowledge in the area of AI-based AML systems in particular, the safety and security of the financial sector is assured.

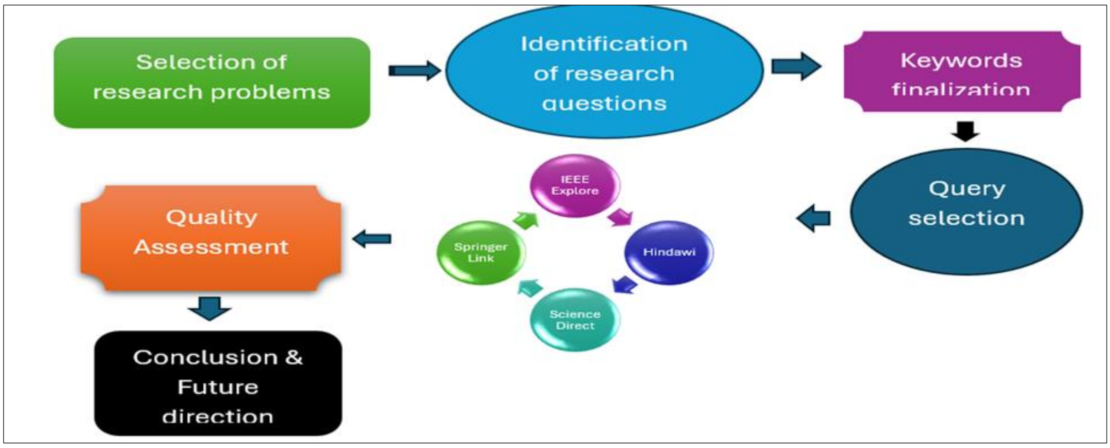


Figure 1 Purposed SLR procedure.

2.1. Research Question Identification

Most importantly, having established research questions help to perform an SLR. Different characteristics of AI-based platform is critically examined and reported to ascertain the most appropriate research queries. This led to the formation of the five research questions in Table 1. SLR is yet another way of critically reviewing a situation.

2.2. Formulation of Query

Once the research question and keyword formulation from the selected online digital libraries were identified and finalized, the next step was to formulate query.

Table 1 Selected research questions and corresponding explanation

RQ1) What are the different tools and channels utilized for ML in the financial sector?	ML is converting 'dirty' money to conceal the source of the cash. ML has become a significant issue in the global market. The primary object of this RQ is to identify the various methods used for machine learning in third-world countries.
RQ2) What are the most AI-based generic solutions proposed for restricting ML?	The aims of this RQ is to counter the various AI-based methods established to provide generic solutions for restricting ML. Furthermore, question is to present new direction to the research work which enhance the competencies of AI-based system and provide various solution to overcome the risk of ML.
RQ3) What are the various components that can determine the risk money laundering?	This research question identifies different types of embedded solutions proposed for real-time security analysis.
RQ4) Using the literature as evidence, how can we minimize the risk factor of ML within financial sectors?	Based on the literature, the prime object of this question is to increase the capabilities of existing AI based system within the financial sector to provide enhance security to count the risk of ML.
RQ5) What are the economic and social impacts of money laundering on society?	Aimis expending vastly in the global village. The aim of this RQ is explain the social and economic impacts of money laundering in the society.

2.3. Review Process

The 112 articles were selected according to the defined criteria for SLR after screening the assigned online libraries for important primary articles and the inclusion and exclusion circulation. The final group of materials includes workshop papers, conference proceedings, book parts, journal pieces, and review/survey articles. During this phase, a voting schema was proposed. If a majority of the authors felt that the paper should be on this final list of the most relevant papers, it was included; otherwise, it was removed. From all these online digital libraries, four are selected as the most appropriate for gathering relevant research papers for this SLR process are Taylor & Francis, IEEE Xplore, Springer Link, and Elsevier. Table 2 summarizes the entire inclusion process.

Review and assessment of 112 research articles have been completed. Figure 2 below shows the total number of publications from the identified peer-reviewed digital online libraries that added publications to this final pool.

Table 2 Selection of articles for final development process.

Digital Library	Total articles	Filtered articles	Final selected articles
IEEE	212	91	35
Elsevier	234	111	22
Taylor & Francis	221	76	24
Springer Link	311	56	21
Total			112

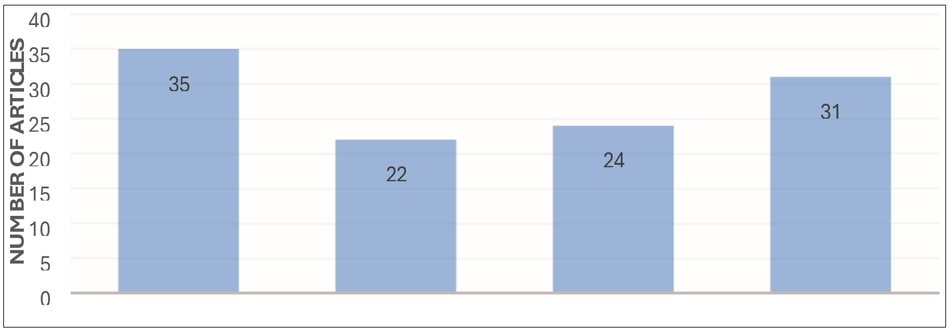


Figure 2 Collection of online libraries for articles

A total of 112 articles are fetched based on the defined criteria for SLR after scanning the specified online libraries for suitable primary articles and implementing the inclusion and exclusion sequence. The final pool of materials consists of workshop papers, conference proceedings, parts of books or long articles like journal papers, review/survey papers. During this stage, a voting mechanism was suggested. If the paper was deemed a good fit by more than half of the writers, it made the final list of the most relevant papers; otherwise, it was excluded. For this purpose, the four most relevant online digital libraries that will help to collect relevant research papers for this SLR process are chosen, which are Taylor & Francis, IEEE Xplore, Springer Link, and Elsevier. An overview of the entire inclusion process can be found in Table 2.

We have compiled and indexed 112 publications for review and scoring. Figure 2 below shows the total number of publications using the selected peer reviewed digital online libraries that culminated the final pool.

2.4. Quality Assessment

To assess the papers' relevancy to the SLR protocol, we followed the criteria given in the SLR protocol. We evaluated all the RQs and the respective criteria proposed in the study against relevant papers (Khan, Nazir and Khan 2021).

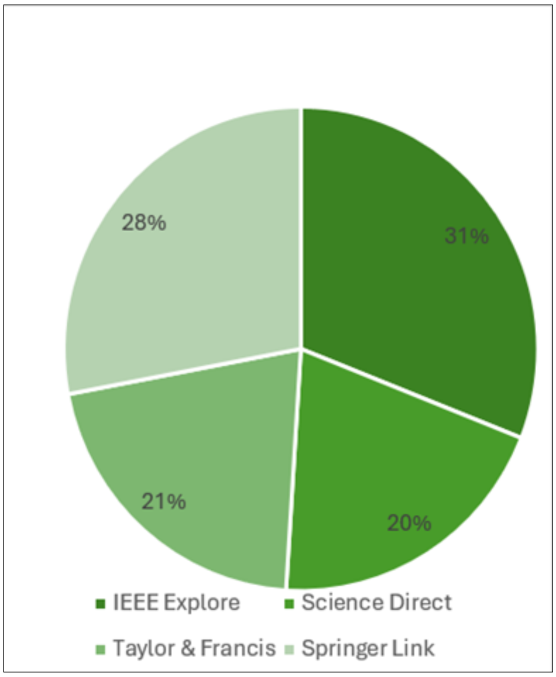


Figure 3 Contribution percentage for each library

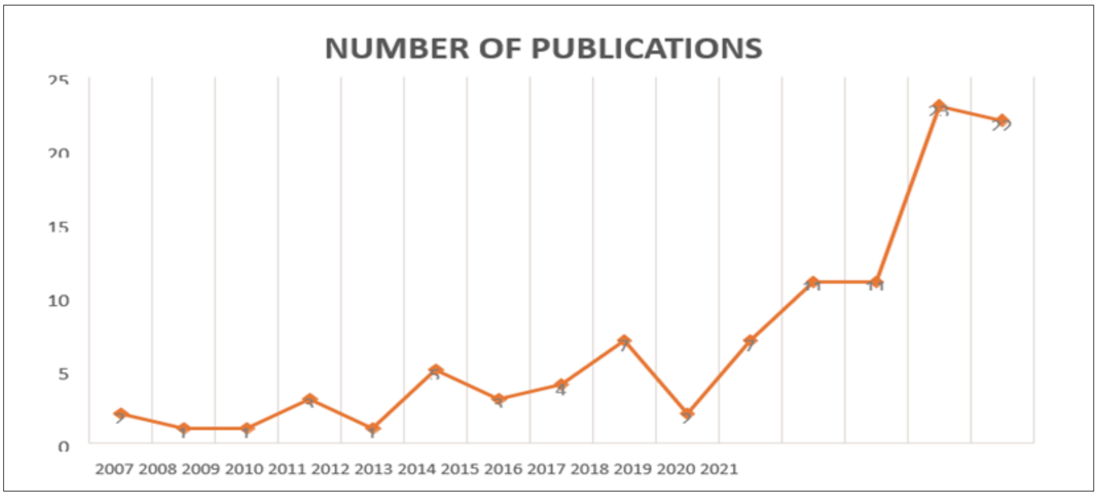


Figure 4 Year-wise contribution of selected articles.

Such evaluation ensured the quality of each SLR paper. In addition, all study topics were weighted based on the following criteria:

- If a certain research article completely fulfilled that research question then it was given a weighted value of 1
- If an article was neither fully or partially fulfilled that research question then it was assigned a weighted value of 0.5, otherwise 0

Node weights were calculated by aggregating the values corresponding to relevant articles based on the varied research topics in the quality assessment; and further, while the leaf nodes are the weighted values of their research topics, the terminal node is the calculated mean value that expresses the input of the procedure for evaluation as depicted in Figure 5. The most significant circular shape means the higher the relevance of a given research paper to the research subject under examination in this SLR paper.

3. Analysis and Results

Each question is then followed by insights that retrieve information on each proposed research area made for the current SLR study. Each of the keys below relates specifically to each associated research topic posed in the current SLR study.

3.1. RQ1) Which Tools and Channels are Being Used for Money Laundering in the Financial Sector?

Now a day's ML is becoming one of the serious threats for the banking sector. The banking sectors (Villar and Khan 2021) are having harsh penalty on customers for incompetent ML risk assessment like it happened to HSBC Bank London, which was charged about USD $2 billion by a US regulator for negligence to prevent Mexican drug criminal to launder using banking channel (Isa et al. 2015). There are multiple ways it can be done. They can mask the origins of their money by goading its way into real estate, casinos and inflated legal bills.

ML methods typically cover three steps; layering, integration, and placement (Mahootiha, Golpayegani and Sadeghian 2021; Matanky-Becker and Cockbain 2021; Philippson 2001; Seymour 2008). For more than 30 years, legislators and stakeholders have enacted ML-related laws and regulations throughout the world. Placement is the method of injecting dirty money into the financial industry. However, layering is a method of executing complex transactions to hide the origin of funds. Lastly, integration means pulling funds out of a dedicated bank account. When layering is sophisticated, AML instruments are confused (Soltani et al. 2016). Table 3 briefly explains the various used tools for ML as below.

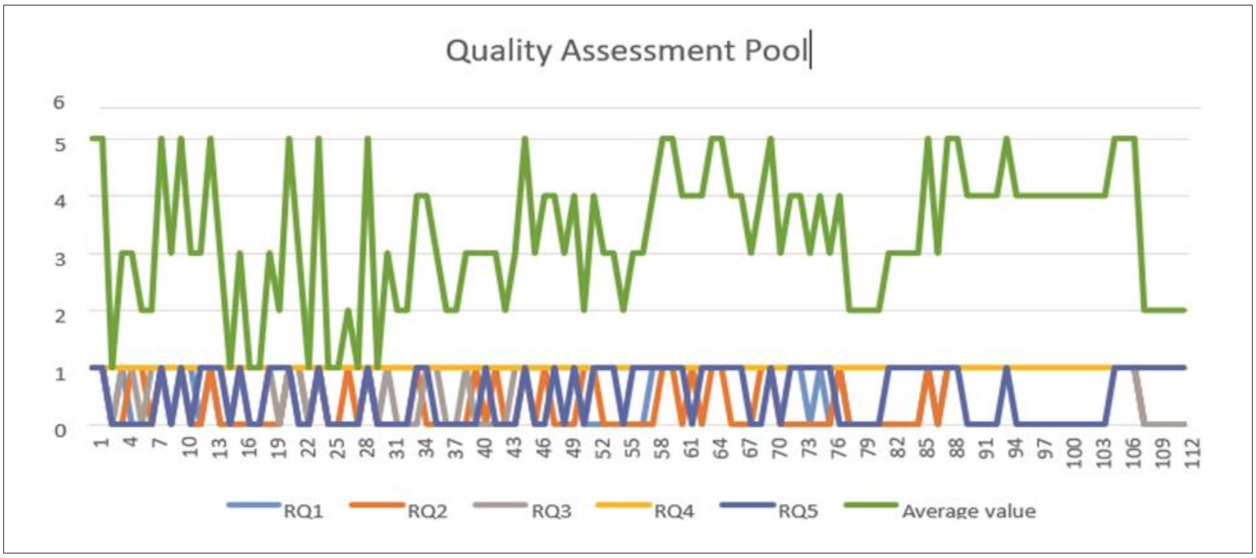


Figure 5 Representation the relevant articles.

3.2. RQ2) What Are the Most AI-Based Generic Solutions Applied to Restrict Money Laundering?

And every year, ML is a threat to the world economy. "Such proceeds could be reinvested into further criminal activity and pose a threat to the integrity of international financial systems. For this reason, many countries regard money laundering as a significant threat. This research question implies various generic approaches presented in the papers on constraining ML. The focus of this research question provides a background of the various AI based methods and approaches that can be used for mitigating money laundering. There is a series of proposed solutions to these problems, which can be seen in table 4.

3.3. RQ3) What are the different components that can identify / determine money laundering risk?

Terrorist organizations depend on funds and illicit financing to sustain themselves. Without a constant and reliable source of funding, terrorist groups would be unable to manage daily paperwork, feed their members, or undertake operations (Fletcher, Larkin, and Corbet 2021). Other researchers had used different AI methods to strengthen ML ability. Technological advancements have transformed the finance industry in such a way as to reduce the risks of ML. The main objective of this RQ is to enunciate the different elements that may characterize the risk of money-laundering. Table 5: Description of various components influencing ML.

3.4. RQ4) How Do Financial Sectors Avoid Money Laundering as a Risk — as per the Literature?

Since the 9/11 terrorist attack of 2001, the US has adopted a heightened sensitivity to movements of illegal money, owing to the belief that such networks facilitate global terrorist and criminal activity (Ferwerda et al. 2013). The spread of the internet has allowed for online financial transactions on everything from mobile device to PCs and even similar devices. There are many intermediary nodes in the network through which any user's action in gaining access to the financial services must go through.

Table 3 Different tools used for Money Laundering**.**

S.No	Channels selected for Money Laundering	Description	References
1.	Social Network	The suggested strategy presents an (Dreżewski, Sepielak, and Filipkowski 2015; efficient method to update the social Jamshidi and Reza Hashemi 2012; network since one of the obstacles of Mahootiha, Golpayegani, and a real-world electronic transaction Sadeghian 2021; Shaikh, Al-Shamli, and system is the vast volume of data and Nazir 2021) users.	

2.	Credit Card	Credit cards have become one of the most (Erdoğan et al. 2020; Sarma et al. 2020) popular on-site and online purchasing payments due to their simplicity of use. Due to the demand for credit cards rising, a slew of new fraud techniques, including as identity theft and phishing, arise to steal money from credit card scammers	
3.	Banking	This paper describes the Anomaly-based (Al-Nuemat 2013; Mishra and Yadav 2020) Intrusion Detection Systems for AIDS for attack exposure. Intrusion Detection Systems IDS is implemented in research field in AI and various machine learning algorithms.	
4.	Digital Stolen Funds	According to the findings, cybercrime is particularly in paying out electronic stolen monies, which they accomplish predominantly through money mules and virtual casinos.	(Mikhaylov and Frank 2016)
5.	Security and safety	The study covers decision-making about critical infrastructure safety, with perceptions about unintentional risk serving as a corresponding point of debate.	(Dai and Boroomand 2021; Guzman et al. 2016; Kose and Vasant 2017; Link et al. 2018; Rindell and Holvitie 2019; Srivastava, Bisht, and Narayan 2017)
6.	Network attack	The paper analysis the possibility of network attacks and promotes the development of artificial intelligence.	(Shu et al. 2020)
7.	Online Transactions	This research looks at the effectiveness of reporting doubtful transaction made to a FIU (Financial intelligence unit) to prevent ML.	(Dalla Pellegrina et al. 2020; Singla 2021; Xia et al. 2021)
8.	Account	The paper's focuses on identifying every questionable ML account. Further in contrast, digs deeper into the highly suspicious ones to improve the recall and precision of ML account identification.	(Tai and Kan 2019)
9.	Employee dishonest	The study proposed a model for criminals to compete against one another in a market but collaborate with other criminals and employee's dishonesty in an engage to launder their criminal activity to process through change ML linkages	(Imanpour et al. 2019)
10.	Pressure Policies	The consequences of political pressure to (Picard and Pieretti 2011) offshore financial hubs with the capacity to enforce compliance with AML legislation are discussed in this study.	
11.	Illicit Incomes	Estimates of illegal revenue from drug (Loayza, Villa, and Misas 2019) trafficking and general crime are significant components of the dataset assembled in the article.	
	Channels selected for Money Laundering	Description	References
12.	Smuggling	This article focuses on preventing a transnational criminal organization's (TCO) interconnected contraband smuggling, money and money laundering (ICSML) networks.	(Shen et al. 2021)
13.	Criminal bargain	This study reviews about the professional money laundering and examines how the launderer and the criminal negotiate a fee for the money- laundering service.	(McCarthy, van Santen, and Fiedler 2015)
14.	Non-Profit organization	The entire assessment adds to the body of knowledge on terrorist use of non- governmental organizations (NPOs) while	(Omar, Johari, and Arshad 2014)

		also assisting member nations in putting effective policies in place.	
15.	Dark web	This article examines current developments in the listed areas and provides an overview of criminal markets such as the Dark Web, counterstrategies, and money laundering.	(Weber and Kruisbergen 2019)
16.	Casinos	Theoretically and empirically, this article explores how the risks factor may be calculated which show that hotels, casinos, art industry and entertainment industry have the highest ML risks in the Netherlands.	(Ferwerda and Kleemans 2019)
17.	Internet	The paper purposed the contribute complex problem of cyber-laundering by examining the challenges and risk faced in electronic money laundering impose to regulators and law enforcement agencies, as well as showing a path forward for more effectively preventing the ML of illegal profits earn on internet.	(Tropina 2014)
18.	Unusual prices	The research demonstrates how to scientifically approach the latter two by utilizing economic data such as anomalous pricing and other features to determine the degree of money laundering in these industries.	(Unger and Den Hertog 2012)
19.	Offshore	According to the research, Kyrgyzstan's two post-communist political administrations exploited offshore accounts to money launder and arrange profitable transactions with foreign commercial partners.	(Marat 2015)
20.	Information Technology	This exploratory study gives depth about how criminals are engage in the organized crime of money laundering using IT platform.	(Kruisbergen et al. 2019)

Table 4 List of solutions proposed for restricted ML

S.No	Solutions for Restrict Money Laundering	Description	References
1.	Hybrid Data mining- based algorithm	They frequently utilize model classifiers that (Song 2020) are too weak to fit a vast quantity of data. Researchers proposed a hybrid data mining-based algorithm method for fraud detection to address this issue.	
2.	Data Mining	The articles are presented to create data (Le Khac, Markos, and Kichadi mining techniques as effective methods for 2010; Watkins et al. 2003) detecting money laundering.	
3.	Secure Intelligent Framework	This article aims to safeguard money transfers (Sobh 2020) to prevent money laundering. It delivers a Safe and Intelligent Anti-Money Laundering Framework (SIFAML).	
4.	Visualization technique	This research explores on the use of (Singh and Best 2019) visualization methods to aid in the effective identification of ML tendencies.	
5.	Fraud-Memory	In this article fraud-memory is a revolutionary (Kunlin 2018) fraud detection algorithm proposed. It combines sequential neural networks with memory networks to achieve great performance and resilience.	
6.	Decision tree method	The decision tree approach is utilized in this (Wang and Yang 2007) research to build money laundering risk determination rules based on customer detail of a bank in China.	

7.	Clustering method	These papers provide framework then (Soltani et al. 2016; Xia et al. searches the condensed data to identify 2021; Zand, Orwell, and pairs of transactions with shared Pfluegel 2020) characteristics and behaviors that may be implicated in ML activities. After that, a clustering method is used to find probable ML groupings.	
8.	AutoML	This article shows how to assess data in (Thi et al. 2020) suspicious behaviors, client connections, and consumer retrieval from the financial industry on social media platforms using an innovative approach.	
9.	Suspicious activity detection models	The study presents a technique for detecting suspicious activity detection model based on statistics data to identify suspect sequences at the transaction level for financial institutions.	(Xie et al. 2010)
10.	Time-frequency analysis	The article provides a new feature based on time-frequency analysis that uses 2-D demonstrations to financial transactions. It features are distinguishing factors for suspicious and non-suspicious transactions.	(Ketenci et al. 2021)
11.	Game-theoretic analysis	This paper presents a game-theoretic analysis of social networks in the ML process.	(Imanpour et al. 2019)
12.	Bitcoin Fog and Blockchain.info	Researchers aim to employ reverse- engineering tools to figure out how the system works and link anonymized transactions to our probing accounts. Our test transactions were successfully anonymized via Bitcoin Fog and Blockchain. info.	(Campbell-Verduyn 2018; Möser, Böhme, and Breuker 2013)
S.No	Solutions for Restrict Money Laundering	Description	References
13.	Typology	The paper presents a strategy for producing variants of typologies based on instances constructed on typologies. The software was built to implement and verify this method, and it was successfully tested on case graphs based on typologies.	(Plaksiy, Nikiforov, and Miloslavskaya 2018)
14.	Community detection algorithm	This research developed a technique for detecting bank fraud that uses a community detection algorithm to identify trends that might lead to fraud.	(Dreżewski, Sepielak, and Filipkowski 2012; Sarma et al. 2020)
15.	CatBoost	This research offers a fraud detection machine learning algorithm based on CatBoost. Researchers use feature engineering to develop extremely significant features and input them into CatBoost for classification to boost detection accuracy.	(Chen and Han 2021)
16.	Deep Learning	A deep learning online based system to detect scam in the transaction, these studies compare three thresholding strategies based on Receiver Operating Characteristic (ROC) max - G-Mean criterion, Youden Index (J), and Curve i.e., Closest to (0,1).	(Choi and Lee 2018; Singla 2021)
17.	Support Vector Machine	To test the correctness of the suggested solution, three distinct types of data were employed. The proposed technique also compared to other essential solutions, including the support vector machine, deep learning and decision tree	(Mahootiha, Golpayegani, and Sadeghian 2021)
18.	ML Detection Systems	This article briefly discusses the processes of money laundering as well as the system itself. The primary section focuses on the implemented algorithms that aid in detecting suspect money movement patterns.	(Dreżewski et al. 2015; Dreżewski, Sepielak, and Filipkowski 2015)

19.	Explainable AI Techniques	The article is to examine the present literature on DL and Explainable AI techniques (XAI) for detecting suspicious ML and recommend new research topics in the same domain.	(Kute et al. 2021)
20.	Multi-agent architecture	A unique and multi-agent architecture for AML is offered, along with several agents. A prototype system is created d to detect the money laundering to show the advancements of the existing system architecture and enhance business value.	(Gao et al. 2006)
21.	Innovative model	The aim is to present a new paradigm for automating verifying banned transactions in watch-list filtering systems.	(Alkhalili, Qutqut, and Almasalha 2021)
22.	Anomaly detection techniques	This article aims to explore and give a comprehensive evaluation of the most common and successful anomaly detection approaches used to identify financial fraud, with an emphasis on semi-supervised and unsupervised learning.	(Pourhabibi et al. 2020)
23.	Bi-level integer programming model	A bi-level integer programming model is proposed that is particularly presented to criminal networks' interdependencies to solve the bi-level issue; a dual-based reformulation is used.	(Shen et al. 2021)
	Solutions for Restrict Money Laundering	Description	References
24.	Cross sectional model	The paper investigates the valuation impacts of the 4AMLD on a sample of European banks to make restrictions and influence on banks and then, utilizing a cross-sectional model to discover that the positive value effect was greater for riskier, more lucrative, bigger more lucrative institutions with unconventional income streams.	(Haffke, Fromberger, and Zimmermann 2020; Premti, Jafarinejad, and Balani 2021)
25.	Multivariate analysis	In this study, the multivariate analysis reflects transaction monitoring via RegTech and time saving and cost saving elements of RegTech, driving ML prevention efficacy to a statistically significant amount.	(Turki et al. 2020)
26.	Graph convolution neural networks (GCN)	A hybrid ML prediction model based on GCN and long short-term memory (LSTM), abbreviated MGC-LSTM, and to developed the understanding of interdependence among distinct ML transactions.	(Xia et al. 2021)
27.	MFBAA: Enhancing Algorithm Performance with Multi-Feature Behaviour Approximation	Multi feature behaviour A unique MFBAA approach has been approximation developed in this paper to boost algorithm (MFBAA) performance. The multi-feature behaviour approximation method keeps track of each transaction made by distinct users and their behaviours while servicing access status, services, etc.	(Jayasree and Balan 2017)
28.	Bitmap Index-based The BIDT	Bitmap Index-based The BIDT approach is proposed in this study to Decision Tree (BIDT) assess the adaptation risk in money laundering.	(Jayasree and Balan 2017)
29.	Evaluating STR Effectiveness	Theoretical models This research aims to give a preliminary empirical assessment of the effectiveness of suspicious transaction reporting (STR) to the FIU in preventing money laundering and minimizing the legal economy's susceptibility to criminal infiltration. The theoretical models of baseline and two provinces are utilized to organize the empirical analysis.	(Dalla Pellegrina et al. 2020)

This is especially the case when new forms of crime, particularly cybercrime or new technologies in traditional organized crime, are linked to established knowledge, concepts, and theories within the field. But it is important to think about intended as well as unintended consequences of the use of technology for organized groups of criminals as they emerge and develop (Kruisbergen et al. 2019).

There are different hybrid AML based systems now, but not all of them addressed with real money and virtual currency. They also tend to generate false positives, are disconnected from related financial networks, and are highly dependent on the analyst's skill (Sobh 2020). It was a simple task to construct a facade which was the current international standard on AML/QTF and the content of its obligations (Goldbarsht 2020). That being said, international organizations serve a crucial role in the international adoption of AM legislation (Maguchu 2018).

Table 5 List of various components that determine ML.

S.No	List of various components that determine ML	Description	References
1.	Know Your Customer	The paper presents no information about new clients in KYC to AML inspections, it is more beneficial use of this service instead of time and money wasting on many other websites.	(Alkhalili, Qutqut, and Almasalha 2021; Möser, Böhme, and Breuker 2013; Thi et al. 2020)
2.	Cryptographic code	An innovative method is suggested that meets these limitations. It therefore gives the option for banks to mutually utilize existing system for producing each transaction cryptographic code, which checks some transaction data to only the authorized party.	(Zand, Orwell, and Pfluegel 2020)
3.	Data enrichment scheme	This research aims to present a data enrichment technique that focuses on employing social network analysis to aid the detection system by providing information that is buried in the relationships between entities.	(Jamshidi and Reza Hashemi 2012)
4.	Qualitatively analyzing	The study examines two big Russian- speaking carding and hacking forums by qualitatively evaluating and measuring term use circumstances.	(Mikhaylov and Frank 2016)
5.	IEEE-CIS	The use of memory compression to speed (Chen and Han 2021) up detection is described in this study as a fundamental contribution of our work. Our method's performance is measured using a publicly available IEEE-CIS Fraud dataset given by the Kaggle competition site.	
6.	CoDetect	In this research, CoDetect is proposed, (Huang et al. 2018) a novel fraud detection system that can identify financial fraud using both network and feature information.	
7.	Graph Computing	The use of graph computing ideas in AI (Kurshan, Shen, and Yu 2020) and machine learning solutions has piqued the interest of this article. Neural graph networks and upcoming adaptive solutions provide enticing possibilities for fraud and financial crime detection.	
8.	Machine learning	These papers propose an intelligent two- (Alkhalili, Qutqut, and Almasalha 2021; phase strategy for spotting suspicious Canhoto 2021; Chen et al. 2018; Choi ML accounts from transaction data and Lee 2018; Domashova and based on data analysis techniques and Mikhailina 2021; Plachouras and machine learning. Leidner 2015; Tai and Kan 2019)	
9.	Digital forensics	This article discusses a new sub-discipline (Nikkel 2020) of digital forensics called Fintech, which deals with financial technology.	
10.	Economic analysis	This article adds to the economic (Loayza, Villa, and Misas 2019) understanding of illegal operations and money laundering.	

11.	Sensitivity analysis	Sensitivity analysis investigates this (Shen et al. 2021) impact by looking at specific interdictions for network disruptions.
	List of various components that determine ML	Description
12.	Adaptive resource allocation model	A unique Adaptive AML Resource Allocation Model (AAMLRAM) based on the Semi-Markov Decision Process (SMDP) is suggested in this study to allocate AML resources domain to assess suspicious transaction reports submitted by financial sectors
13.	Artificial neural network (ANN)	The research proposed a machine learning-based method to identify financial fraud and compares it to ANN to detect fraud and analyze huge volumes of financial data.
14.	Sampling schemes	This research delves into machine learning and sampling strategies to ML detection and unusual event categorization in general.
15.	Game theory approach	This article uses a game theory method to examine the efficiency of Portugal's AML efforts, both in the financial and non-financial sectors of the economy.
16.	Work Domain Analysis	This research gives a system model of the crypto laundering system that is the first. Using the unique language and perspective of crypto launderers, the authors used Work Domain Analysis (WDA) to characterize the functioning of the crypto laundering sociotechnical system.
17.	Gravity model	The classic gravity model that we give can explain Trade-Based ML flows over the earth.

Regulation creates comfort and safety but does not heal us from impunity (Pol 2020). The change from human-centered towards computer- driven financial services is set to create a substantial shift in traditional financial services systems as technology takes over. For example, progressive transition to a computer and data- driven financial system and rapid emergence of the financial technology (FinTech) sector (Truby, Brown and Dahdal 2020). The access of a corrupt dictatorship to global financial sectors and offshore markets facilitates regime control of political and economic concerns and cultivates a veneer of invulnerability of the regime both domestically and internationally (Marat 2015).

3.5. How does Money Laundering Affect the Economy and Society?

ML has been a global problem for decades and potentially a serious social problem. The governments, regulatory bodies, and financial entities are all fighting desperately to get on top of this issue, but billions of dollars in government funds still continue to hit the headlines. Specifically, money launderers seek out methods to hide their proceeds, which is the essence of the process. Emerging nations therefore share identifiable characteristics and features that make them appealing for money launderers to commit their crime. It impacts these countries' political, societal and economic dimensions. The fight against money laundering requires an understanding of these emerging nations' economic and social conditions, and political climates. According to estimates of the united nation office on drugs and crime (UNODC), ML being responsible for 2 to 5% of world gross domestic product (GDP) or $800 billion-$2 trillion per year, is one of the primary threats to the world economy and security. With the increase in usage of AI and machine learning technology in financial sectors, anti-money laundering systems have also evolved to automate data and time-intensive processes to identify suspicious activity (Kute et al. 2021).

4. Limitations

This particular research paper includes 112 most relevant literature reviews for the protection and security measures to safeguard this system in the organization based on how the techniques had been adopted. Moreover, this SLR work has mined rich information about different types of security threats, along with their effect on economic entities. Moreover, this comprehensive neglect presented a new direction in research and it is believed to pave the way for the evolution of efficient AI-based risk mitigation and high security and authenticity guaranteeing systems. Apart from these major benefits, below are some of the limitations that endured with this SLR efforts:

- Art museums were selected for collections and articles downloads sparingly online. We wanted to detect only those that had been solidly investigated by most researchers.

- Over 15 years this SLR analysis undergoes, however, new papers on AI and money laundering are published every day.
- Assessment and analysis are done purely on published material. There is no work conducted in experimental labs for perspective, valuation, and analytical purposes.
- Papers are aggregated from certain search terms and keywords. This means if the article has no 'name' that corresponds to the keywords — it gets skipped entirely during the article collection.

4.1. Future Research Direction

The analysis of the research questions used Most the researches selected in the papers did not study bias of researchers and effect of results in Few of them made made comments on limits of methodologies and instruments applied in each of studies. However, it cannot be considered thorough as it covers only the highlights of the topics covered in time, balance the interests of information security studies and anti-money laundering research, but the study is perceived to be good reading material for any interested in anti-money laundering research using information technology and will stimulate new interests in the area. This was limited to only four unique majority peer-reviewed, open online digital repositories for the two of the primary study publications. We retrieved a total of 112 relevant publications (articles, parts of books, conference papers, and survey work) for analysis and assessment. The research will help companies and practitioners by laying out the diverse impacts of ML on our society and economy and the incorporation of AI within financial institutions. The Institutions may also use an AI risk mitigation plan to enhance the efficiency and security of financial companies. It will figure out many threats before they are posed. This systematic literature review will serve as a knowledge base for practitioners and researchers interested in the design of safe and secure anti-money laundering1 systems in the financial industry in the future. The work of this SLR assumes to establish a close bond between the community and the AML system in light of the emerging trends of research. Future studies should further expand the search scope, manually checking references of selected articles in this study, as well as pertinent journals, books, survey and conference, using the snowball technique.

5. Conclusion and Discussion

During the decade, attention to the phenomenon of money laundering has increased globally and this crime itself has been enshrined. But much of the research has focused on money laundering from the perspective of wealthier countries. Hence developed country requirements have been the basis for all international legislation, policies, and opinion, to curb money laundering. Every day, the technology was used by several people or agencies to create other means and give the platforms to launder money and illegal currency. For a long time, ML has been considered a tremendous threat to the world's economy and financial system. It undermines public trust in the financial system, and endangers the soundness and stability of financial sectors and the financial system as a whole. Due to the threat ML poses to the global financial system and national economies most governments have undertaken steps to reduce the incidence of ML. As a result, the growth of ai applications in financial sectors is facing serious challenges in money laundering and fraud.

Financial institutions and banking sectors are investing a massive budget to protect their processes. AI could help CTF/ML be controlled and maintained. Technology adoption and AI application should work with every sector across the country. Implementation of various elements and techniques of artificial intelligence algorithms such as ANN, machine learning, deep learning, intelligent robotics, and so on in the existing scheme to counteract the danger of ML/CTF. In order to prevent the conversion of money, Organizations must design an artificial intelligence-supported AML system. Need to verify the continuous process of government and regulatory agencies to monitor it at every level in order to have sustainable economic growth. Anti-money laundering legislation is designed to enhance the reputation of financial sectors, and that of the global financial system, as well as that of customers' confidence and trust. Machine learning in the finance industry and AI-based analytics build rapid growth in the finance industry by giving useful analysis and understanding of potential risks linked to money laundering for financial organizations and establishments. It has demonstrated incredible prowess across a host of domains, even the financial and regulatory space.

At the international level, FATF is the main body in reducing the risk of ML/CTF. And each country has pledges to provide different reports for FATF authorities to justify that it is implementing AML/CTF Likewise, the FATF is very clear in regards to some organizations that are abused in the name of charitable endeavor, such charity on accounting for their finances as well. However, the administration has to really want and be committed to doing this instead of just unfreezing them (as it previously did). Despite precautionary measures by the government and the regulatory authorities of different countries, there are alternative networks that people are adopting, to transfer illegal foreign exchange remittances that escape banking channels. The intention of this paper is to study the current state of affairs from different angles and to propose potential lines of research to conduct the study and construct high levels of authenticity and security in the financial sector by using AI. To overcome this concern SLR has been performed analyzing for high security, authentication, and safety the best articles gathered from online peer-reviewed digital libraries.

Compliance with ethical standards

Acknowledgments

The authors are grateful to the anonymous referees of journal for their extremely useful suggestion to improve the quality of the article.

Disclosure of conflict of interest

The author declared no potential conflicts of interest with respect to the research, authorship and publication of this article. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

[1] Al Hammadi, A., I. A. Zualkernan, and R. Ahmed. 2007. Impediments to adoption of e-Learning technology in combating anti-money laundering in UAE banks. Paper read at Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007), Niigata, Japan.

[2] Alkhalili, M., M. H. Qutqut, and F. Almasalha. 2021. Investigation of applying machine learning for watch-list filtering in anti-money laundering. *Institute of Electrical and Electronics Engineers Access* 9:18481–96.

[3] Alnasser Mohammed, S. A. S. 2021. Money laundering in selected emerging economies: Is there a role for banks? *Journal of Money Laundering Control* 24 (1):102–10.

[4] Al-Nuemat, A. A. 2013. Money laundering and banking secrecy in the Jordanian legislation. *Journal Information and Communications Technology* 34 (9):91–104.

[5] Al-Rashidi, K. S. 2021. Indirect method of proof'and the Kuwaiti anti-money laundering law: a lesson from the UK. Paper read at Criminal Law Forum.

[6] Bashir, R., R. Rajeev, A. Shatarah, and N. Bashir. 2020. A risk score analysis related to money laundering in financial institutions across nations. Paper read at 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India.

[7] Butler, S. 2019. Criminal use of cryptocurrencies: A great new threat or is cash still king? *Journal of Cyber Policy* 4 (3):326–45.

[8] Campbell-Verduyn, M. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law, & Social Change* 69 (2):283–305.

[9] Canhoto, A. I. 2021. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research* 131:441–52.

[10] Chen, Y., and X. Han. 2021. CatBoost for fraud detection in financial transactions. Paper read at 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China.

[11] Chen, Z., L. D. Van Khoa, E. N. Teoh, A. Nazir, E. K. Karuppiah, and K. S. Lam. 2018. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems* 57 (2):245–85.

[12] Choi, D., and K. Lee. 2018. An AIapproach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks* 2018:15.

[13] Choo, K.-K. R. 2014. Designated non-financial businesses and professionals: A review and analysis of recent financial action task force on money laundering mutual evaluation reports. *Security Journal* 27 (1):1–26.

[14] Dai, D., and S. Boroomand. 2021. A review of AIto enhance the security of big data systems: state-of-art, methodologies, applications, and challenges. *Archives of Computational Methods in Engineering* 29:1–19.

[15] Dalla Pellegrina, L., G. Di Maio, D. Masciandaro, and M. Saraceno. 2020. Organized crime, suspicious transaction reporting and anti-money laundering regulation. *Regional Studies* 54 (12):1761–75.

[16] Desmond, D., P. Salmon, and D. Lacey. 2021. Functional systems within cryptolaundering processes: A work domain analysis model of cryptolaundering activities. *Journal of Cyber Policy* 6 (2):155–76.

[17] Dhaya, A., and R. Ravi. 2021. Multi feature behavior approximation model based efficient botnet detection to mitigate financial frauds. *Journal of Ambient Intelligence and Humanized Computing* 12 (3):3799–806.

[18] Domashova, J., and N. Mikhailina. 2021. Usage of machine learning methods for early detection of money laundering schemes. *Procedia Computer Science* 190:184–92.

[19] Dreżewski, R., G. Dziuban, Ł. Hernik, and M. Pączek. 2015. Comparison of data mining techniques for money laundering detection system. Paper read at 2015 International Conference on Science in Information Technology (ICSITech).

[20] Dreżewski, R., J. Sepielak, and W. Filipkowski. 2012. System supporting money laundering detection. *Digital Investigation* 9 (1):8–21.

[21] Dreżewski, R., J. Sepielak, and W. Filipkowski. 2015. The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences* 295:18–32.

[22] Erdoğan, Í., O. Kurto, A. Kurt, and Ş. Bahtıyar. 2020. A new approach for fraud detection with artificial intelligence. Paper read at 2020 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, Turkey.

[23] Ferwerda, J., M. Kattenberg, H.-H. Chang, B. Unger, L. Groot, and J. A. Bikker. 2013. Gravity models of trade-based money laundering. *Applied Economics* 45 (22):3170–82.

[24] Ferwerda, J., and E. R. Kleemans. 2019. Estimating money laundering risks: An application to business sectors in the Netherlands. *European Journal on Criminal Policy and Research* 25 (1):45–62.

[25] Fletcher, E., C. Larkin, and S. Corbet. 2021. Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance* 56:101387.

[26] Gao, S., D. Xu, H. Wang, and Y. Wang. 2006. Intelligent anti-money laundering system. Paper read at 2006 IEEE International Conference on Service Operations and Logistics, and Informatics, Shanghai, China.

[27] Garcia-Bedoya, O., O. Granados, and J. Cardozo Burgos. 2021. AI against money laundering networks: The Colombian case. *Journal of Money Laundering Control* 24 (1):49–62. doi:10. 1108/JMLC-04-2020-0033 .

[28] Goldbarsht, D. 2020. Am I my corporate's keeper? Anti-money laundering gatekeeping opportunities of the corporate legal officer. *International Journal of the Legal Profession* 29:1–20.

[29] Gowin, K. D., D. Wang, S. Rakesh Jory, R. Houmes, and T. Ngo. 2021. Impact on the firm value of financial institutions from penalties for violating anti-money laundering and economic sanctions regulations. *Finance Research Letters* 40:101675.

[30] Guan, C., J. Mou, and Z. Jiang. 2020. Artificial intelligence innovation in education: A twenty-year data-driven historical analysis. *International Journal of Innovation Studies* 4:134–47.

[31] Gudkov, A. 2020. On Fiduciary Relationship with AISystems. *The Liverpool Law Review* 41 (3):251–73.

[32] Guevara, J., O. Garcia-Bedoya, and O. Granados. 2020. Machine learning methodologies against money laundering in non-banking correspondents. Paper read at Applied Informatics: Third International Conference, ICAI 2020, Ota, Nigeria, October 29–31, 2020, Proceedings 3.

[33] Guzman, A., S. Ishida, E. Choi, and A. Aoyama. 2016. Artificial intelligence improving safety and risk analysis: A comparative analysis for critical infrastructure. Paper read at 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bali, Indonesia.

[34] Haffke, L., M. Fromberger, and P. Zimmermann. 2020. Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation* 21 (2):125–38.

[35] Hamid, O. H. 2017. Breaking through opacity: A context-aware data-driven conceptual design for a predictive anti money laundering system. Paper read at 2017 9th IEEE-GCC conference and exhibition (GCCCE), Manama, Bahrain.

[36] Han, J., Y. Huang, S. Liu, and K. Towey. 2020. Artificial intelligence for anti-money laundering: A review and extension. *Digital Finance* 2 (3):211–39.

[37] Hong, X., H. Liang, Z. Gao, and H. Li. 2017. An adaptive resource allocation model in anti-money laundering system. *Peer-To-Peer Networking and Applications* 10 (2):315–31.

[38] Huang, D., D. Mu, L. Yang, and X. Cai. 2018. CoDetect: Financial fraud detection with anomaly feature detection. *Institute of Electrical and Electronics Engineers Access* 6:19161–74.

[39] Hunter, L. Y., and G. Biglaiser. 2020. The effects of the international monetary fund on domestic terrorism. *Terrorism and Political Violence* 34: 1–25.

[40] Hussain, A., S. Nazir, S. Khan, and A. Ullah. 2020. Analysis of PMIPv6 extensions for identifying and assessing the efforts made for solving the issues in the PMIPv6 domain: A systematic review. *Computer Networks* 179:107366.

[41] Imanpour, M., S. Rosenkranz, B. Westbrock, B. Unger, and J. Ferwerda. 2019. A microeconomic foundation for optimal money laundering policies. *International Review of Law and Economics* 60:105856.

[42] Isa, Y. M., Z. Mohd Sanusi, M. Nizal Haniff, and P. A. Barnes. 2015. Money laundering risk: From the bankers' and regulators perspectives. *Procedia Economics and Finance* 28:7–13.

[43] Jakobi, A. P. 2018. Governing illicit finance in transnational security spaces: The FATF and anti-money laundering. *Crime, Law, & Social Change* 69 (2):173–90.

[44] Jamshidi, S., and M. Reza Hashemi. 2012. An efficient data enrichment scheme for fraud detection using social network analysis. Paper read at 6th International Symposium on Telecommunications (IST), Tehran, Iran.

[45] Jayantilal, S., S. Ferreira Jorge, and A. Ferreira. 2017. Portuguese anti-money laundering policy: A game theory approach. *European Journal on Criminal Policy and Research* 23 (4):559–74.

[46] Jayasree, V., and R. V. Siva Balan. 2017. Money laundering regulatory risk evaluation using bitmap index-based decision tree. *Journal of the Association of Arab Universities for Basic & Applied Sciences* 23:96–102.

[47] Jullum, M., A. Løland, R. Bang Huseby, G. Ånonsen, and J. Lorentzen. 2020. Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control* 23 (1):173–86.

[48] Keele, S. 2007. *Guidelines for performing systematic literature reviews in software engineering*.

[49] UK: Citeseer.

[50] Ketenci, U. G., T. Kurt, S. Önal, C. Erbil, S. Aktürkoglu, and H. Şerban İlhan. 2021. A time-frequency based suspicious activity detection for anti-money laundering. *Institute of Electrical and Electronics Engineers Access* 9:59957–67.

[51] Khan, S., S. Nazir, and H. Ullah Khan. 2021. Analysis of navigation assistants for blind and visually impaired people: A systematic review. *IEEE Access* 9:26712–26734. doi:10.1109/ ACCESS.2021.3052415 .

[52] Kitchenham, B. 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University* 33 (2004):1–26.

[53] Kitchenham, B., R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, and S. Linkman. 2010. Systematic literature reviews in software engineering–a tertiary study. *Information and Software Technology* 52 (8):792–805.

[54] Kose, U., and P. Vasant. 2017. Fading intelligence theory: A theory on keeping AIsafety for the future. Paper read at 2017 International AIand Data Processing Symposium (IDAP).

[55] Kruisbergen, E. W., E. R. Leukfeldt, E. R. Kleemans, and R. A. Roks. 2019. Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime & Justice* 42 (5):569–81.

[56] Kshetri, N. 2021. The role of AIin promoting financial inclusion in developing countries. *Journal of Global Information Technology Management*.

[57] Kunlin, Y. 2018. A memory-enhanced framework for financial fraud detection. Paper read at 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA.

[58] Kurshan, E., H. Shen, and H. Yu. 2020. Financial crime & fraud detection using graph computing: Application considerations & outlook. Paper read at 2020 Second International Conference on Transdisciplinary AI (TransAI).

[59] Kute, D. V., B. Pradhan, N. Shukla, and A. Alamri. 2021. Deep learning and explainable AItechniques applied for detecting money laundering–a critical review *IEEE Access*, Irvine, CA, USA.

[60] Lawlor-Forsyth, E., and M. Michelle Gallant. 2018. Financial institutions and money laundering: A threatening relationship? *Journal of Banking Regulation* 19 (2):131–48.

[61] Lee, J. 2020. Access to finance for AIregulation in the financial services industry. *European Business Organization Law Review* 21 (4):731–57.

[62] Le Khac, N. A., S. Markos, and M.-T. Kechadi. 2010. A data mining-based solution for detecting suspicious money laundering cases in an investment bank. Paper read at 2010 Second International Conference on Advances in Databases, Knowledge, and Data Applications, Menuires, France.

[63] Link, J., K. Waedt, I. Ben Zid, and X. Lou. 2018. Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, Their Interoperability and Impact on Organizations: How to Manage RAMS+ S (Reliability Availability Maintainability Safety+ Security). Paper read at 2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS), Shanghai, China.

[64] Loayza, N., E. Villa, and M. Misas. 2019. Illicit activity and money laundering from an economic growth perspective: A model and an application to Colombia. *Journal of Economic Behavior and Organization* 159:442–87.

[65] Mabunda, S. 2018. Cryptocurrency: The new face of cyber money laundering. Paper read at 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa.

[66] Maguchu, P. 2018. Revisiting money-laundering legislation in Zimbabwe and the role of international organisations. *African Security Review* 27 (3–4):278–90.

[67] Mahootiha, M., A. H. Golpayegani, and B. Sadeghian. 2021. Designing a new method for detecting money laundering based on social network analysis. Paper read at 2021 26th International Computer Conference, Tehran, Iran, Computer Society of Iran (CSICC).

[68] Marat, E. 2015. Global money laundering and its domestic political consequences in Kyrgyzstan. *Central Asian Survey* 34 (1):46–56.

[69] Matanky-Becker, R., and E. Cockbain. 2021. Behind the criminal economy: Using UK tax fraud investigations to understand money laundering myths and models. *Crime, Law, & Social Change* 77:1–25.

[70] McCarthy, K. J., P. van Santen, and I. Fiedler. 2015. Modeling the money launderer: Microtheoretical arguments on anti-money laundering policy. *International Review of Law and Economics* 43:148–55.

[71] Mikhaylov, A., and R. Frank. 2016. Cards, money and two hacking forums: An analysis of online money laundering schemes. Paper read at 2016 European intelligence and security informatics conference (EISIC), Uppsala, Sweden.

[72] Mishra, A., and P. Yadav. 2020. Anomaly-based IDS to detect attack using various AI& machine learning algorithms: A review. Paper read at 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, February 28–29, 2020.

[73] Molla Imeny, V., S. D. Norton, M. Salehi, and M. Moradi. 2021. Perception versus reality: Iranian banks and international anti-money laundering expectations. *Journal of Money Laundering Control* 24 (1):63–76. doi:10.1108/JMLC-06-2020-0064 .

[74] Möser, M., R. Böhme, and D. Breuker. 2013. An inquiry into money laundering tools in the Bitcoin ecosystem. Paper read at 2013 APWG eCrime researcher's summit.

[75] Nazir, S., S. Khan, H. U. Khan, S. Ali, I. García-Magariño, R. Binti Atan, and M. Nawaz. 2020. A comprehensive analysis of healthcare big data management, analytics and scientific programming. *Institute of Electrical and Electronics Engineers Access* 8:95714–33.

[76] Nikkel, B. 2020. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation* 33:200908.

[77] Nizioł, K. 2021. The challenges of consumer protection law connected with the development of AIon the example of financial services (chosen legal aspects. *Procedia Computer Science* 192:4103–11.

[78] Omar, N., Z. Amirah Johari, and R. Arshad. 2014. Money laundering–FATF special recommendation VIII: A review of evaluation reports. *Procedia-Social and Behavioral Sciences* 145:211–25.

[79] Omar, N., R. Juhaida Johari, and M. Sathye. 2015. Malaysian DNFBPs' perceptions on awareness, perceived impact and views on the AML/CFT requirements. *Procedia Economics and Finance* 31:595–600.

[80] Philippson, S. 2001. Money laundering on the internet. *Computers & Security* 20 (6):485–485.

[81] Picard, P. M., and P. Pieretti. 2011. Bank secrecy, illicit money and offshore financial centers. *Journal of Public Economics* 95 (7–8):942–55.

[82] Plachouras, V., and J. L. Leidner. 2015. Information extraction of regulatory enforcement actions: From anti-money laundering compliance to countering terrorism finance. Paper read at Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, Paris, France.

[83] Plaksiy, K., A. Nikiforov, and N. Miloslavskaya. 2018. Applying big data technologies to detect cases of money laundering and counter financing of terrorism. Paper read at 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain.

[84] Pol, R. F. 2020. Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice* 3 (1):73–94.

[85] Pourhabibi, T., K.-L. Ong, B. H. Kam, and Y. Ling Boo. 2020. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems* 133:113303.

[86] Premti, A., M. Jafarinejad, and H. Balani. 2021. The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks. *Research in International Business and Finance* 57:101397.

[87] Rindell, K., and J. Holvitie. 2019. Security risk assessment and management as technical debt. Paper read at 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, June 3–4, 2019.

[88] Romero, V. 2020. Bloody investment: Misaligned incentives, money laundering and violence. *Trends in Organized Crime* 25:1–29.

[89] Rudner, M. 2010. Hizbullah terrorism finance: Fund-raising and money-laundering. *Studies in Conflict & Terrorism* 33 (8):700–15.

[90] Rusanov, G., and Y. Pudovochkin. 2021. Money laundering in the modern crime system. *Journal of Money Laundering Control* 24 (4):860–68.

[91] Samanta, S., B. Kumar Mohanta, S. Prasad Pati, and D. Jena. 2019. A framework to build user profile on cryptocurrency data for detection of money laundering activities. Paper read at 2019 International Conference on Information Technology (ICIT).

[92] Sarma, D., W. Alam, I. Saha, M. Nazmul Alam, M. J. Alam, and S. Hossain. 2020. Bank fraud detection using community detection algorithm. Paper read at 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India.

[93] Savona, E. U., and M. Riccardi. 2019. Assessing the risk of money laundering: Research challenges and implications for practitioners. *European Journal on Criminal Policy and Research* 25 (1):1–4.

[94] Seymour, B. 2008. Global money laundering. *Journal of Applied Security Research* 3 (3–4):373–87.

[95] Shaikh, A. K., M. Al-Shamli, and A. Nazir. 2021. Designing a relational model to identify relationships between suspicious customers in anti-money laundering (AML) using social network analysis (SNA). *Journal of Big Data* 8 (1):1–22.

[96] Shehu, A. Y. 2012. Promoting financial inclusion for effective anti-money laundering and counter financing of terrorism (AML/CFT). *Crime, Law, & Social Change* 57 (3):305–23.

[97] Shen, Y., T. C. Sharkey, B. K. Szymanski, and W. Al Wallace. 2021. Interdicting interdependent contraband smuggling, money and money laundering networks. *Socio-Economic Planning Sciences* 78:101068.

[98] Shu, F., S. Chen, F. Li, J. Zhang, and J. Chen. 2020. Research and implementation of network attack and defense countermeasure technology based on AItechnology. Paper read at 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China.

[99] Singh, K., and P. Best. 2019. Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems* 34:100418.

[100] Singla, J. 2021. Comparing ROC curve based thresholding methods in online transactions fraud detection system using deep learning. Paper read at 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).

[101] Sittlington, S., and J. Harvey. 2018. Prevention of money laundering and the role of asset recovery. *Crime, Law, & Social Change* 70 (4):421–41.

[102] Sobh, T. S. 2020. An intelligent and secure framework for anti-money laundering. *Journal of Applied Security Research* 15 (4):517–46.

[103] Soltani, R., U. Trang Nguyen, Y. Yang, M. Faghani, A. Yagoub, and A. An. 2016. A new algorithm for money laundering detection based on structural similarity. Paper read at 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA.

[104] Song, Z. 2020. A data mining based fraud detection hybrid algorithm in E-bank. Paper read at 2020 International Conference on Big Data, AIand Internet of Things Engineering (ICBAIE), Fuzhou, China.

[105] Srivastava, S., A. Bisht, and N. Narayan. 2017. Safety and security in smart cities using artificial intelligence—A review. Paper read at 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence.

[106] Stokes, R. 2012. Virtual money laundering: The case of Bitcoin and the Linden dollar. *Information & Communications Technology Law* 21 (3):221–36.

[107] Suresh, A., A. P. Subeer, A. Mary Philip, J. Shaji Varughese, and J. Mathew. 2020. Comprehensive home security for elderly people using IoT and artificial intelligence. Paper read at 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangluru, India.

[108] Tai, C.-H., and T.-J. Kan. 2019. Identifying money laundering accounts. Paper read at 2019 International Conference on System Science and Engineering (ICSSE), Dong Hoi, Vietnam.

[109] Thi, M. H., C. Withana, N. Thi Huong Quynh, and N. Tran Quoc Vinh. 2020. A novel solution for anti-money laundering system. Paper read at 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia.

[110] Tropina, T. 2014. Fighting money laundering in the age of online banking, virtual currencies and internet gambling. Paper read at Era Forum.

[111] Truby, J., R. Brown, and A. Dahdal. 2020. Banking on AI: Mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review* 14 (2):110–20.

[112] Turki, M., A. Hamdan, R. Thomas Cummings, A. Sarea, M. Karolak, and M. Anasweh. 2020. The regulatory technology “RegTech” and money laundering prevention in Islamic and conventional banking industry. *Heliyon* 6 (10):e04949. doi:10.1016/j.heliyon. 2020.e04949 .

[113] Unger, B., and J. Den Hertog. 2012. Water always finds its way: Identifying new forms of money laundering. *Crime, Law, & Social Change* 57 (3):287–304.

[114] Villar, A. S., and N. Khan. 2021. Robotic process automation in banking industry: A case study on Deutsche Bank. *Journal of Banking and Financial Technology* 5 (1):71–86.

[115] Von Solms, J. 2021. Integrating Regulatory Technology (RegTech) into the digital transformation of a bank Treasury. *Journal of Banking Regulation* 22 (2):152–68.

[116] Wang, S.-N., and J.-G. Yang. 2007. A money laundering risk evaluation method based on decision tree. Paper read at 2007 International conference on machine learning and cybernetics.

[117] Watkins, R. C., K. M. Reynolds, R. Demara, M. Georgiopoulos, A. Gonzalez, and R. Eaglin. 2003. Tracking dirty proceeds: Exploring data mining technologies as tools to investigate money laundering. *Police Practice & Research* 4 (2):163–78.

[118] Weber, J., and E. W. Kruisbergen. 2019. Criminal markets: The dark web, money laundering and counterstrategies-An overview of the 10th Research Conference on Organized Crime. *Trends in Organized Crime* 22 (3):346–56.

[119] Xia, P., Z. Ni, H. Xiao, X. Zhu, and P. Peng. 2021. A novel spatiotemporal prediction approach based on graph convolution neural networks and long short-term memory for money laundering fraud. *Arabian Journal for Science & Engineering* 47:1–17.

[120] Xie, P., J. H. Li, X. Ou, P. Liu, and R. Levy. 2010. Using Bayesian networks for cyber security analysis. Paper read at 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), Chicago, IL.

[121] Young, M. A., and M. Woodiwiss. 2021. A world fit for money laundering: The Atlantic alliance’s undermining of organized crime control. *Trends in Organized Crime* 24 (1):70–95.

[122] Zand, A., J. Orwell, and E. Pfluegel. 2020. A secure framework for anti-money-laundering using machine learning and secret sharing. Paper read at 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland.

[123] Zhang, Y., and P. Trubey. 2019. Machine learning and sampling scheme: An empirical study of money laundering detection. *Computational Economics* 54 (3):1043–63.