Taylor & Francis
Taylor & Francis Group

Applied Artificial Intelligence
An International Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uaai20

Identifying the AI-based solutions proposed for restricting Money Laundering in Financial Sectors: Systematic Mapping

Habib Ullah Khan, Muhammad Zain Malik & Shah Nazir

To cite this article: Habib Ullah Khan, Muhammad Zain Malik & Shah Nazir (2024) Identifying the AI-based solutions proposed for restricting Money Laundering in Financial Sectors: Systematic Mapping, Applied Artificial Intelligence, 38:1, 2344415, DOI: 10.1080/08839514.2024.2344415

To link to this article: https://doi.org/10.1080/08839514.2024.2344415

Published online: 22 Apr 2024.

APPLIED ARTIFICIAL INTELLIGENCE
2024, VOL. 38, NO. 1, e2344415 (31 pages)
https://doi.org/10.1080/08839514.2024.2344415

Taylor & Francis
Taylor & Francis Group

Identifying the AI-based solutions proposed for restricting Money Laundering in Financial Sectors: Systematic Mapping

Habib Ullah Khan[a], Muhammad Zain Malik[a], and Shah Nazir[b]

[a]Department of Accounting & Information Systems, College of Business & Economics, Qatar University, Doha, Qatar; [b]Department of Computer Science, University of Swabi, KPK, Pakistan

ABSTRACT

Money laundering (ML) is a critical source of extracting the money illegally from the financial system. It is linked to various types of crimes, including corruption, exploitation of a specific community, drug use, and many others. Detection of ML operations is a difficult task on a global scale due to the large volume of financial transactions. However, it also allows criminals to use financial systems to carry out fraudulent transactions. It mainly concern minimizing the potentially risks associated with money laundering. Anti-money laundering-(AML) tools based on AI-driven applications are now tracking transactions to overcome this challenge. A total of 112 research papers are assessed to identify the literature's gaps and suggest new directions for the research area accordingly. The findings of this systemic literature review work will not only open new paths for the research community, but will also assist the state agencies in developing an optimal AML system to counter these major issues and provide a healthy environment for their residents. This article seeks to assess the existing situation from various angles and open up new pathways for future research directions to investigate and build high levels of authenticity and security in the financial industry using artificial intelligence (AI).

ARTICLE HISTORY
Received 15 December 2022
Revised 8 February 2024
Accepted 24 February 2024

Introduction

The capacity of AI to automate operations that are sometimes thought of as "tedious" produces enormous benefits, such as freeing up time for individuals looking to collect money to conduct essential donor networking and strategy. Although they may sound like generic buzzwords, AI, data analytics, and machine learning (ML) are being integrated into organization technology systems as creative solutions to problems with risk management, human resources and compliance. Every year many industries lose millions of dollars in fraud including banking and financial institutes,

CONTACT Habib Ullah Khan habib.khan@qu.edu.qa Department of Accounting & Information Systems, College of Business & Economics, Qatar University, P.O.Box 2713, Doha, Qatar

insurance companies, government agencies, telecommunication industries, and law enforcement (Jamshidi and Reza Hashemi 2012). We live in a culture where criminal cases involving senior persons are steadily growing. Due to the rise in the number of dangers and incursions in society, people desperately need a security system to ensure their well-being and safety. As the innovation in technology changes, the contrary, global effect in the shape of cyber threats (Suresh et al. 2020). Criminal activities, such as smuggling, bribery and drug trafficking, may be highly profitable. Before illegally obtained funds may be freely spent, they must be made to appear genuine (Wang and Yang 2007). The identification of fraud is a prominent topic in the data mining community. A high level of sophistication frequently marks fraudulent transactions. They are incredibly unusual among the millions of daily transactions, and their manipulators are well planned and thought out (Kunlin 2018). Fraud detection has become a challenging task for many companies. Hackers have more accessibility to the personal information and advanced password decoding tools, making it easier for them to commit online fraud. Customers lose billions of dollars each year due to online transaction fraud (Song 2020). Due to the harm caused to banks and their clients, fraud detection and prevention technologies have become essential. AI and machine learning techniques are increasing employed in fraud detection systems (Erdoğan et al. 2020; Guevara, Garcia-Bedoya, and Granados 2020).

Money laundering is repurposing unlawfully obtained funds to give them the appearance of legality (Hamid 2017). It is the terminology used to describe attempting to legitimize illegal gains so that they may be reinjected into the legitimate economy or used to fund more criminal activity (Ketenci et al. 2021). Changing dirty money to clean money is referred to as money laundering. For example, the money derives from illicit sources such as human trafficking, kidnapping, extortion contract, killing, bribes, tax evasion, and drug dealing. An organization or individual cannot deposit money straight into a bank since the bank identifies anomalous transaction activity, and the user cannot reveal the money's source. This money is known as "black money" and has a significant detrimental impact on the economy. As a result, anti-money laundering legislation is quite severe in both emerging and wealthy countries (Samanta et al. 2019). ML is a method of making unlawful income look legitimate and used by criminals to disguise the natural source and ownership of the profits of their criminal activities. It is becoming a severe danger to financial institutions and the entire country. This illegal activity is growing increasingly sophisticated, and it appears to have evolved beyond the stereotype of smuggling of drugs to include funding terrorist organizations and, of course, personal gain. Money laundering is the practice of criminals attempting to transform illicitly obtained funds using of a legal medium such as huge investment

or pension funds or investment in banking products (Le Khac, Markos, and Kechadi 2010). Money laundering is a large-scale societal issue, and detecting unlawful financial purchases using ML applications is difficult and time-consuming. However, most evaluated current anti-money laundering (AML) system operations use link analysis, networking analysis, risk scoring categorization and outlier detection to detect doubtful transactions (Thi et al. 2020).

A criminal analysis is a complex operation that necessitates processing massive volumes of data from many sources, such as billings and bank account activities, gathering information helpful to an investigator (Dreżewski, Sepielak, and Filipkowski 2015). A Financial organizations like banks and other credit-granting organizations use AML systems to combat money laundering by detecting risks, transactions, and possible money launderers (Han et al. 2020). The AI System (FAIS) of the American Financial Crime Enforcement Network combined clever human intelligence and software agents to recognize suspected ML over a vast data area. Using an AI computer analysis system may considerably improve work productivity and is a critical approach for AML (Wang and Yang 2007). AI, a term frequently used in science fiction, is becoming more generally recognized as it becomes more integrated into our daily lives. Transportation, Healthcare, retail, and finance are among the areas that are fast changing. A terminology AI drive as a computer having the capacity to execute a range of human cognitive activities, like as learning, interactive, thinking, and solving issues in 1955 by John McCarthy. In today's culture, AI applications have been applied to develop various businesses (Guan, Mou, and Jiang 2020). Since 1970, money laundering has been detected since financial institutions start reporting big transactions to their public department (Soltani et al. 2016). Financial institutions, such as banks and other credit-granting institutions, use AML systems to combat ML by detecting risks, transactions, and possible money launderers (Han et al. 2020). These papers were evaluated for their ability to:

- Outline the different tools and channels used for ML in the financial sector;
- Identify AI-based generic solutions proposed for restricting money laundering;
- Various components that can determine the risk of money laundering; and
- Describe the economical and social impacts of ML on society and different financial sectors.

It primarily focuses on reducing the serious dangers connected with ML. Anti-money laundering systems based on AI-driven apps are currently using track

transactions to address this issue. Researchers' main concerns and problems include the financial sector's security and safety from ML. Embedding security in AI-based applications has been recognized as a way for financial institutions to accomplish their goal.

Background Study

The word ML is described as separating criminal proceeds from their sources or attempting to make money earned via unlawful means look legal or clean (Bashir et al. 2020). It is also defined as "the act of moving unlawfully obtained funds via legitimate individuals or accounts to conceal the source of the funds." It is a global problem that has led to political unrest and slower economic progress. It is a continual source of concern for many officials in many nations. Several methods can be used to carry out money laundering. The first is the import and export sectors, which are avenues through which money may be transformed into commodities that are then either exported or legally brought back into the nation (Alnasser Mohammed 2021). In recent years, the battle against money laundering has nearly taken the top spot on the anti-crime policy priority list (Rusanov and Pudovochkin 2021). ML linked human trafficking and drug, bribery, extortion, kidnapping-for-ransom, terrorism financing, tax evasion, and various other acts are all connected by ML (Ketenci et al. 2021). Because of its seriousness, it is garnering increasing attention from scholars and governments worldwide. For one reason, ML-related money amounts to a significant portion of global GDP each year (Xie et al. 2010). It is impossible to provide an exact rough estimate of the size of such a complex, vast underground market; the IMF (International Monetary Fund) (Hunter and Biglaiser 2020) estimates that more than two trillion USD is ML annually through financial institutes around the world, making money laundering one of the world's biggest markets (Ketenci et al. 2021). According to the IMF, money laundering is estimated to be worth $3.2 trillion globally, or 3% of global GDP. Money laundering earnings are frequently used to fund criminal activities such as illegal arms sales, drug trafficking, human trafficking and terrorism (Han et al. 2020). Financial organizations report suspicious actions to the FIU (Financial Intelligence Unit). FIU gathers information from various financial sectors both inside and beyond the authority, which is then passed on to law enforcement authorities (LEA) as needed (Ketenci et al. 2021).

Fraud detection plays an essential role in reducing losses. Fraudsters endure their invasion by outsmarting all current and introducing advanced anti-fraudulent procedures with their devious evasions. Fraud in bank is a federal offense that includes the deception of financial institutions to get a monetary advantage. Every year, fraud costs banks and financial organizations billions of dollars. Bankers are enticed to participate in scams to get financial assets.

Fraudsters love to prey on banks and insurance firms. Every year, they successfully seize billions of dollars in financial resources. Credit and debit card fraud, false selling insurance, money laundering, and account fraud are the most frequent kinds of bank fraud (Sarma et al. 2020). Terrorists' increasing use of nonprofit organizations (NPOs) worldwide has prompted a concerted global effort to defend these financial organizations. The FATF (Financial Action Task Force) released Special Recommendation (SR) VIII to help others nations review appropriateness of their present rules and guidelines governing to nonprofit organizations (Molla Imeny et al. 2021; Omar, Johari, and Arshad 2014; Savona and Riccardi 2019). The performance of a country's financial institution is assessed using the FATF 40 + 90 (Choo 2014) guidelines and a full evaluation report; these are the instruments that will help each country design AML rules that are compliant with the system (Young and Woodiwiss 2021). In the United States, enhanced due diligence monitors risky and terrorism-related funding, including customer identification in high-risk jurisdictions and big bank transactions. In G20 submission nations are obliged to gather and share information, crypto currency around the world might decontrol banking institutions, thus worldwide AML/CFT has begun to gather and exchange information regarding terrorism funding, particularly in poor areas where banks are constrained (Bashir et al. 2020).

Technological advancements in this field have spawned a slew of new challenges that regulators and other officials must address. Economic rationality can compel people to carry out AI acts and legitimacy for AI operations (Gudkov 2020). Cybersecurity has become an essential topic due to conventional security breaches and worries about how firms handle personal data obtained from customers or ordinary users. The most obvious argument for cybersecurity in banking transactions is to secure client assets while maintaining a high level of data privacy. AI development poses several obstacles, not just technological but also legal and ethical (Nizioł 2021). It is viewed as a danger to jobs since it will eliminate manual work. Financial services are also under pressure (Lee 2020). AI and machine learning quickly evolve and transform emerging nations' political, economic, and social landscapes. As a result, AI-based solutions are predicted to be a game-changer with huge implications for boosting impoverished people's financial access (Garcia-Bedoya, Granados, and Cardozo Burgos 2021; Kshetri 2021). It has developed a vital resource for large banks that deal with regulatory changes, increased anti-money laundering (AML) regulations, and susceptible fraud-prone clientele. Internet banking offers both convenience and major concerns (Jullum et al. 2020). Meanwhile, Internet banking security has gathered the consideration of people from all walks of life. While everyday money transactions are made using various non-cash payment methods, many instances have involved payment information integrity, accessibility, and confidentiality. These accidents can occur on both the client's (funds

owners) and the bank's (or outlet's) sides, additionally during the payment information transmission over communication networks (Plaksiy, Nikiforov, and Miloslavskaya 2018).

Research Protocol

SLR is known method for discovering and assessing research output pertinent to a particular topic. By using a rigorous, trustworthy, and auditable method, SLR aims to provide a balanced appraisal of a studied issue (Kitchenham 2004). SLR has been published in many different domains, including FinTech, money transfer (Hussain et al. 2020) and healthcare systems (Nazir et al. 2020). This SLR method aims to summarize the implementation of machine learning and AI in financial businesses to mitigate the risk of money laundering. Below are the major point to elaborate the aim of this SLR:

- To explore and investigate previous research on this particular technology. The set of questions was created by utilizing AI technology to provide high security and authentication in various business sectors in order to control the threat of ML.
- To identify technological deficiencies that will lead to more research. These new domain will finally help business sectors and their employees by ensuring superior authentication for security purposes to prevent money laundering.
- The most suitable research articles were selected from online libraries for this SLR work. Researchers will assess and examine the most important research articles in the AI and ML areas.

The proposed study endeavor implements the SLR technique using the suggested recommendations by Kitchenham et al. (Keele 2007; Kitchenham et al. 2010). Figure 1 shows the process use in the review methodology of this SLR. The review process consists of seven important steps, as shown in Figure 1, which describes all of these stages in detail.

Research Process Methodology

The SLR highlights the essential pre-review processes, including research question creation, keyword identification, formulating questions, collecting digital libraries available online to collect relevant original articles for the review process, and inclusion/exclusion criteria. As a result of the recent increase in research interest in AIand money laundering, the current systematic review was conducted. A thorough literature review and research in the specific context of AI-based AML systems provide financial sector security and safety.

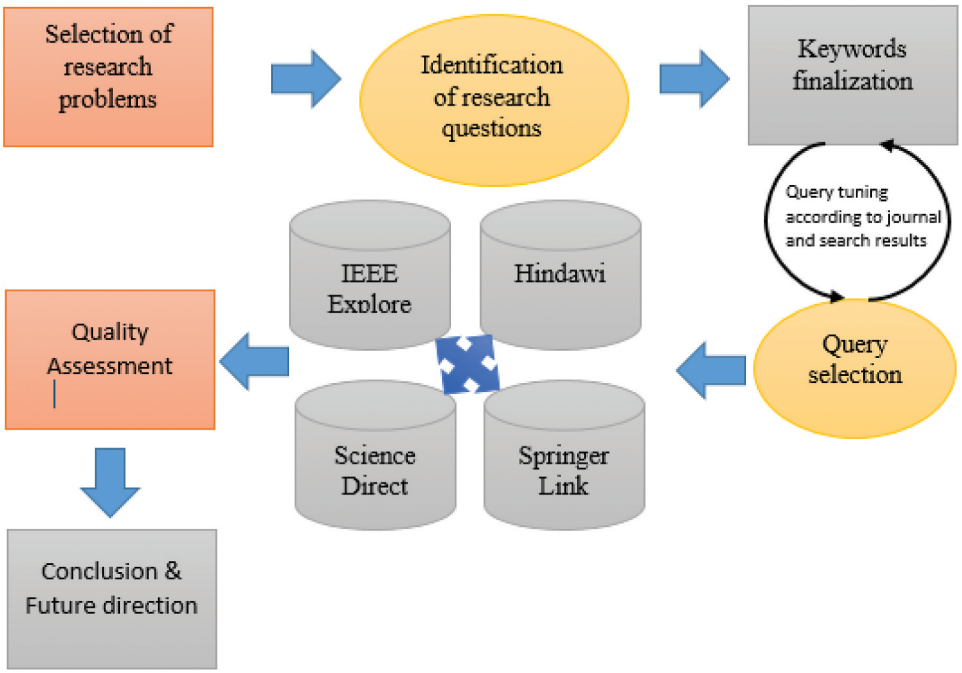

Figure 1. Purposed SLR procedure.

Identification of Research Question

As already stated, establishing research questions is important for conducting an SLR. Various features of the AI-based platform are assessed and presented critically to define the most suitable research questions. The five research questions listed in Table 1 was formed as a result. SLR is another method for critically assessing a given situation.

Identification of Keywords

After developing the RQs, the next crucial task was to categorize keywords and built a search query to choose the most suitable papers from the designated online libraries. The finalized keywords are: "*SECURITY, SAFETY, RISKS, THREATS, MITIGATE, MINIMIZE, EMBEDDED, ARTIFICIAL INTELLIGENCE, MONEY LAUNDERING, FRAUD, ORGANIZATION, SECTOR, INSTITUTE, IMPACT, OR EFFECT*." The above keywords are employed in query construction in accordance with database constraints and find out the best outcome in results of fetching suitable articles.

Formulation of Query

After finalizing the research question and keywords formulation from the selected online digital libraries, the following process is to formulate query

Table 1. Selected research questions and corresponding explanation.

Research questions	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 economical and social impacts of money laundering on society?*	Alis expending vastly in the global village. The aim of this RQ is explain the social and economical impacts of money laundering in the society.

("SECURITY" OR "SAFETY" OR "RISKS" OR "THREATS") AND ("RESTRICT" OR "MINIMIZE") AND ("MONEY LAUNDERING" OR "FRAUD") AND ("ARTIFICIAL INTELLIGENCE" OR "MACHINE LEARNING") AND ("ORGANIZATION" OR "SECTOR" OR "INSTITUTE" OR "IMPACT" OR "EFFECT"). These queries are further modified based on the formulation of keywords from the selected online libraries. Furthermore the query develop on title, abstract, and substance bases of the research article, almost 112 most suitable articles are finalized. The next subsection defines the aggregated research papers in its entirety.

Review Process

The 112 articles are selected based on defined criteria for SLR after screening the designated online libraries for relevant primary articles and executing the inclusion and exclusion procedure. Workshop papers, conference proceedings, book parts, journal pieces, and review/survey articles comprise the final pool of materials. For this phase, a voting method was proposed. If more than half of the writers felt that the paper should be included, it was added to the final list of the most relevant papers; otherwise, it was removed. The four most suitable online digital libraries are selected to gather pertinent research papers for this SLR process, which include Taylor & Francis, IEEE Xplore, Springer Link, and Elsevier. The following is an overview of the whole inclusion procedure in Table 2.

A total of 112 research articles have been completed for review and assessment. The total number of publications from the designated peer-reviewed digital online libraries which contributed to this final pool is shown in Figure 2 below.

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**

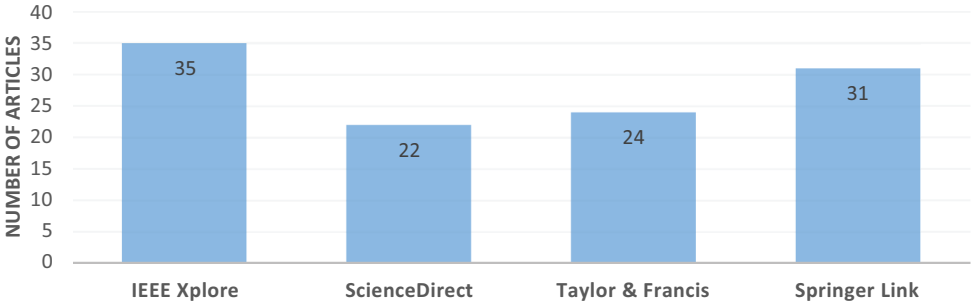

Figure 2. Collection of online libraries for articles.

Figure 3 shows the total contribution of the chosen online repositories to the published pertinent research publications. The percentage contribution was assessed, and it was determined that IEEE Xplore and Springer link contributed more, showing that the researchers' interest in publication their work in these libraries.

AI has grown to be exciting and appealing domain for the research community worldwide. The researchers implementation various techniques of AI and machine learning in many sectors, like tracking and navigation, healthcare, internet safety, profitable industries, businesses, organizations, and many others. Keeping in view these smart applications, the aim of researchers is to exploit these models in financial organizations to ensure their employees' high security and integrity. According to the selected questions, Figure 4 shows the annual contribution of various AI research publications.

After analysis of the outcome presented in Figure 4, it shows that the number of research papers exponentially increases over time, reflecting researchers' interest in the proposed field. From 2016, the publications increased abruptly, showing the organization's interest in AI to prevent the risk of ML enhancing the security and safety of the financial sector.

Quality Assessment

The quality of the papers' relevancy was evaluated using the SLR protocol's criteria. Each of the RQs and accompanying criteria stated in the study were examined and scored against relevant papers (Khan, Nazir, and Khan 2021).

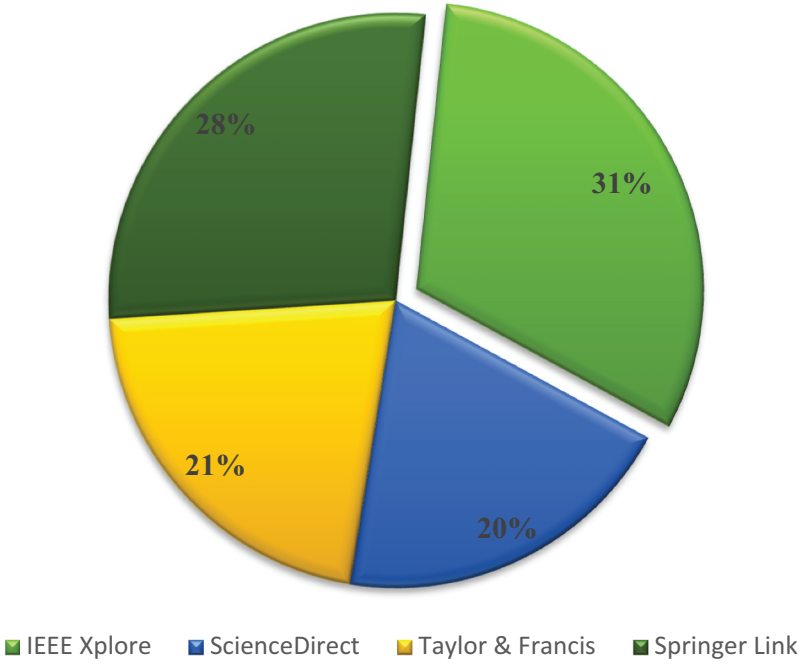

Figure 3. Contribution percentage for each library.

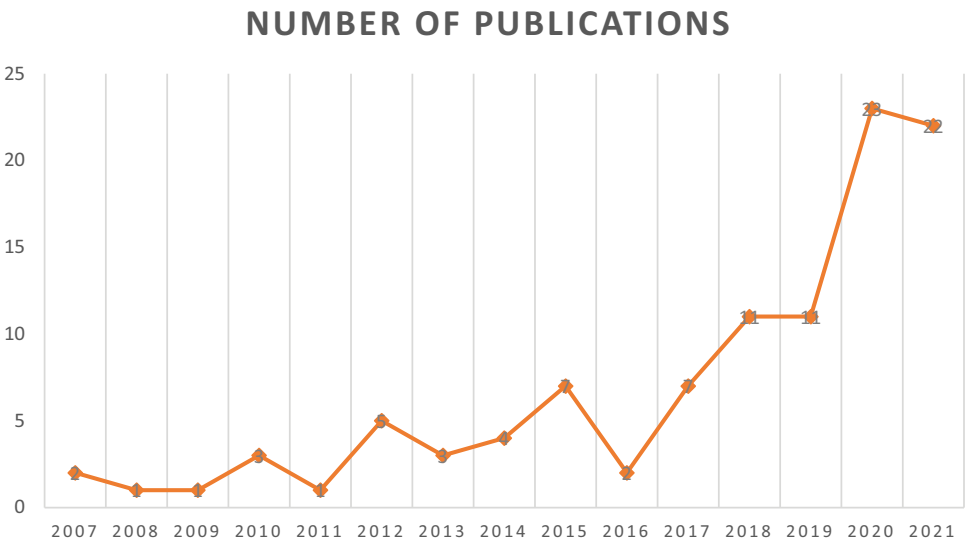

Figure 4. Year-wise contribution of selected articles.

This evaluation guaranteed the quality of each SLR paper. Furthermore, all study topics were given weightage on the below criteria:

- If a certain research article fully satisfied that research question then it was assigned a weighted value of 1
- While if an article partially satisfied that research question then it was assigned a weighted value of 0.5, otherwise 0.

The most relevant articles were identified after the quality assessment, as indicated in Figure 5, where the leaf nodes show weighted values for the associated research topics and the terminal nodes represent the average value of the evaluation procedure. The more important circular representation represents the greatest relevance of a certain research article to the specified research subject to be investigated in this SLR work.

Analysis and Results

Below each question contains information on each associated research topic posed for the current SLR study.

RQ1) What Are the Different Tools and Channels Utilized for Money Laundering in the Financial Sector?

ML is become one of the major threats for the financial institutions. Banking sectors (Villar and Khan 2021) are penalizing customers severely for improperly analyzing ML risk, such as HSBC Bank London, which was plenty about USD $2 billion by a US regulator for failing to prevent Mexican drug criminals from laundering money through banking channel (Isa et al. 2015). It can be done in a variety of ways. Criminals might conceal their money's origins by investing in real estate, casinos, and overvaluing legal invoices. A ML method, in general,

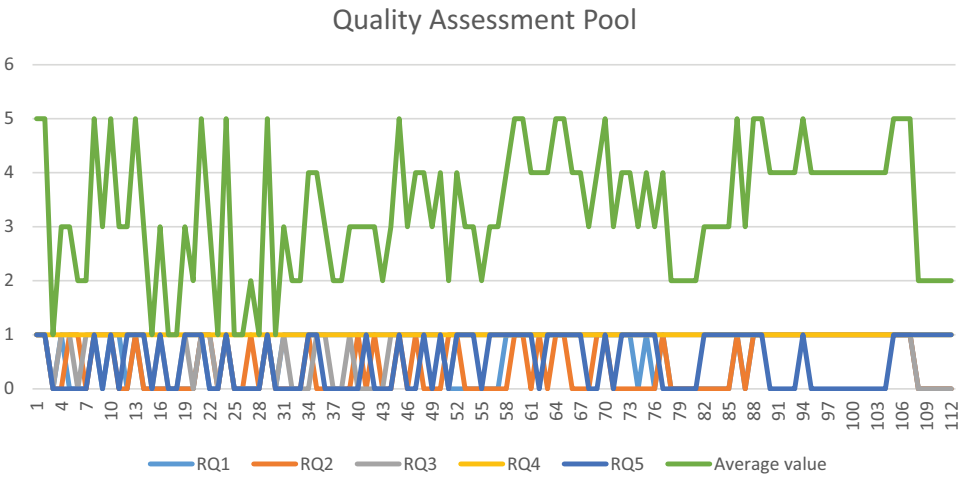

Figure 5. Representation the relevant articles.

consists of three basic steps: layering, integration, and placement (Mahootiha, Golpayegani, and Sadeghian 2021; Matanky-Becker and Cockbain 2021; Philippson 2001; Seymour 2008). Governments and corporations globally have adopted legislation and regulations to combat ML for many years. The practice of injecting filthy money into the financial sector is known as placement. However, layering is a technique for carrying out complicated transactions to conceal the source of funding. Finally, integration entails withdrawing funds from a specified bank account. AML instruments are confused when sophisticated layering is used (Soltani et al. 2016). The various tools used for ML is briefly explain in the Table 3 as below.

RQ2) What Are the Most AI-Based Generic Solutions Proposed for Restricting Money Laundering?

ML is a hazard to the world economy every year. Proceeds from these crimes might be used to fuel more criminal activity and jeopardize the integrity of global financial systems. As a result, money laundering is seen as a severe threat in many countries. This research question suggests different generic solutions proposed in the articles for restricting ML. The primary aim of this research question is to frame the different AI based methods and approaches to limiting money laundering. Table 4 shows the list of solutions proposed for restricting money laundering.

RQ3) What Are the Various Components That Can Determine the Risk Money Laundering?

Terrorist organizations rely on money and widespread illegal financing to survive. Terrorist organizations would be unable to handle daily administrative work, sustain their members, or carry out operations if they did not have a continuous and stable source of funding (Fletcher, Larkin, and Corbet 2021). Previous researchers have employed various AI techniques to enhance ML capabilities. The advancement of technology has changed the financial sector to minimize the threats of ML. The primary aim of this RQ is to highlight different components that can determine the risk of money laundering. Table 5 describes the list of various components that determine ML.

RQ4) Using the Literature As Evidence, How Can We Minimize the Risk Factor of Money Laundering within Financial Sectors?

The US has increased its sensitivity to illegal money flows since the 9/11 terrorist assault in 2001, since officials believe that such money transfers promote worldwide terrorist and criminal operations (Ferwerda et al. 2013). The advancement of internet technology has enabled people to conduct

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 efficient method to update the social network since one of the obstacles of a real-world electronic transaction system is the vast volume of data and users.	(Drężewski, Sepielak, and Filipkowski 2015; Jamshidi and Reza Hashemi 2012; Mahootiha, Golpayegani, and Sadeghian 2021; Shaikh, Al-Shamli, and Nazir 2021)
2.	Credit Card	Credit cards have become one of the most 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	(Erdoğan et al. 2020; Sarma et al. 2020)
3.	Banking	This paper describes the Anomaly-based Intrusion Detection Systems for AIDS for attack exposure. Intrusion Detection Systems IDS is implement in research field in AI and various machine learning algorithms.	(Al-Nuemat 2013; Mishra and Yadav 2020)
4.	Digital Stolen Funds	According to the findings, cybercrime are 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 offshore financial hubs with the capacity to enforce compliance with AML legislation are discussed in this study.	(Picard and Pieretti 2011)
11.	Illicit Incomes	Estimates of illegal revenue from drug trafficking and general crime are significant components of the dataset assembled in the article.	(Loayza, Villa, and Misas 2019)

(*Continued*)

Table 3. (Continued).

S.No	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 also assisting member nations in putting effective policies in place.	(Omar, Johari, and Arshad 2014)
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)

financial transactions using various devices, such as mobile phones, PCs, and other similar devices. Any user's action in gaining access to financial services must pass through a number of intermediary nodes in the network. Such data

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 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.	(Song 2020)
2.	Data Mining	The articles are presented to create data mining techniques as effective methods for detecting money laundering.	(Le Khac, Markos, and Kechadi 2010; Watkins et al. 2003)
3.	Secure Intelligent Framework	This article aims to safeguard money transfers to prevent money laundering. It delivers a Safe and Intelligent Anti-Money Laundering Framework (SIFAML).	(Sobh 2020)
4.	Visualization technique	This research explores on the use of visualization methods to aid in the effective identification of ML tendencies.	(Singh and Best 2019)
5.	Fraud-Memory	In this article fraud-memory is a revolutionary fraud detection algorithm proposed. It combines sequential neural networks with memory networks to achieve great performance and resilience.	(Kunlin 2018)
6.	Decision tree method	The decision tree approach is utilized in this research to build money laundering risk determination rules based on customer detail of a bank in China.	(Wang and Yang 2007)
7.	Clustering method	These papers provide framework then searches the condensed data to identify pairs of transactions with shared characteristics and behaviors that may be implicated in ML activities. After that, a clustering method is used to find probable ML groupings.	(Soltani et al. 2016; Xia et al. 2021; Zand, Orwell, and Pfluegel 2020)
8.	AutoML	This article shows how to assess data in suspicious behaviors, client connections, and consumer retrieval from the financial industry on social media platforms using an innovative approach.	(Thi et al. 2020)
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)

(*Continued*)

Table 4. (Continued).

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 compares 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)

(*Continued*)

Table 4. (Continued).

S.No	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.	Multi feature behaviour approximation algorithm (MFBAA)	A unique MFBAA approach has been developed in this paper to boost performance. The multi-feature behavior approximation method keeps track of each transaction made by distinct users and their behaviors while servicing access status, services, etc.	(Jayasree and Balan 2017)
28.	Bitmap Index-based Decision Tree (BIDT)	The BIDT approach is proposed in this study to assess the adaptation risk in money laundering.	(Jayasree and Balan 2017)
29.	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)

would be hijacked and manipulated by a network of rogue nodes to conduct fraud (Jayasree and Balan 2017). This is particularly true when new kinds of crime, such as cybercrime or new technologies in conventional organized crime, are related to existing information, concepts, and theories in the subject. It's important to consider what the use of technology means for organized criminal groups as they form and grow (Kruisbergen et al. 2019).

Different hybrid AML based systems are now available, however not all deal with actual money and virtual currency. In addition, they frequently issue false-positive alarms, are not connected to other related financial foundations, and rely heavily on the expertise of the analysts (Sobh 2020). It's easy to present an image of the existing international AML standard and its responsibilities (Goldbarsht 2020). International organizations play a critical role in driving worldwide adoption of AML legislation (Maguchu 2018). A global policy framework implementing complicated anti-money laundering

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 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.	(Chen and Han 2021)
6.	CoDetect	In this research, CoDetect is proposed, a novel fraud detection system that can identify financial fraud using both network and feature information.	(Huang et al. 2018)
7.	Graph Computing	The use of graph computing ideas in AI 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.	(Kurshan, Shen, and Yu 2020)
8.	Machine learning	These papers propose an intelligent two-phase strategy for spotting suspicious ML accounts from transaction data based on data analysis techniques and machine learning.	(Alkhalili, Qutqut, and Almasalha 2021; Canhoto 2021; Chen et al. 2018; Choi and Lee 2018; Domashova and Mikhailina 2021; Plachouras and Leidner 2015; Tai and Kan 2019)
9.	Digital forensics	This article discusses a new sub-discipline of digital forensics called Fintech, which deals with financial technology.	(Nikkel 2020)
10.	Economic analysis	This article adds to the economic understanding of illegal operations and money laundering.	(Loayza, Villa, and Misas 2019)
11.	Sensitivity analysis	Sensitivity analysis investigates this impact by looking at specific interdictions for network disruptions.	(Shen et al. 2021)

(*Continued*)

Table 5. (Continued).

S.No	List of various components that determine ML	Description	References
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	(Hong et al. 2017)
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.	(Choi and Lee 2018)
14.	Sampling schemes	This research delves into machine learning and sampling strategies to ML detection and unusual event categorization in general.	(Zhang and Trubey 2019)
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.	(Jayantilal, Jorge, and Ferreira 2017)
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.	(Desmond, Salmon, and Lacey 2021)
17.	Gravity model	The classic gravity model that we give can explain Trade-Based ML flows over the earth.	(Ferwerda et al. 2013)

regulations provides comfort and security, but it does not protect us against criminality (Pol 2020). As traditional financial services systems change, technology is ushering in a significant shift from human-centered to computer-driven financial services. The progressive change to a computer and data-driven financial system and the fast rise of the financial technology (FinTech) sector are example of industry (Truby, Brown, and Dahdal 2020). A corrupt dictatorship's control over both political and economic concerns is strengthened by access to global financial sectors and the availability of offshore markets, which give the regime a sense of invulnerability both locally and worldwide (Marat 2015).

What Are the Economical and Social Impacts of Money Laundering on Society?

For decades, ML has been a worldwide issue that has posed a severe threat to society. Governments, regulatory agencies, and financial institutions are all fighting to outcome this issue, yet billions of dollars in government funds continue to make the news. Money launderers, in particular, hunt for ways to conceal their

wealth, which is the fundamental element of the process. As a result, the majority of emerging nations have traits and qualities that money launderers find appealing to carry out their crime. This has an effect on these nations' political, societal, and economic aspects. Understanding these emerging nations' economic, social environments and political are crucial to the fight against money laundering. The united nation office on drugs and crime (UNODC) assess that ML accounts for 2 to 5% of world GDP, or $800 billion to $2 trillion per year, and is one of the most severe threats to the world economy and security. To identify suspicious activity, financial sectors have begun to use AI and machine learning technology to automate data and time-intensive processes (Kute et al. 2021). The aim of this question is to analyze the social and economic impacts of ML on society and briefly discuss it in Table 6.

Limitations

By examining the methods utilized, this research paper has summarized the 112 most pertinent publications for ensuring protection and security measures to the system in the organization. Furthermore, this SLR work has extracted enriched information about different types of security threats, their influence on economic organizations. Also, this SLR work presented a new research direction by bridging the gaps in the extant and deemed to open new gates for the development of efficient AI-based risk mitigation and high security and authenticity ensuring systems. Besides these critical advantages, some of the cons that prevailed with this SLR work are listed below:

- Only four online research libraries were chosen for collections and article downloads. Our primary objective was to identify just those libraries that had been thoroughly investigated and evaluated by the majority of researchers.
- This SLR analysis has been ongoing for 15 years, yet new papers in AI and money laundering are released every day.
- Only published material is considered for evaluation and analysis. For valuation and analytical purposes, no work-in-progress or work conduct simulation in the experimental labs is done.
- The papers are gathered by specified search terms, phrases and keywords. As a result, if an article does not have a synonym that matches the keywords, it is skipped throughout the article collection process.

Future Research Directions

According to the analysis of the research questions utilized the majority of the chosen papers did not investigate the potential bias of researchers and effect of results, and there were few comments regarding the limits of the

Table 6. Social and economic impacts of Money Laundering.

S.No	Type of impacts	Description	References
1.	E-Bank	Researchers devised a fraud detection method based on data mining hybrids to address the issue.E-Banks contributed to the IEEE-CIS fraud dataset, which is large enough to build a decent classifier.	(Sarma et al. 2020; Song 2020)
2.	Investment Bank	In this paper, researchers describe the technique as a tool and some preliminary experimental findings using actual transaction datasets to deduct the money laundering activities in the investment bank.	(Le Khac, Markos, and Kechadi 2010)
3.	Financial Fraud	The empirical study shows that our approach may be used to detect financial fraud. It uses cutting-edge feature representation approaches in financial systems to better describe users and logs of various sorts.	(Choi and Lee 2018; Dhaya and Ravi 2021; Huang et al. 2018; Kunlin 2018; Plachouras and Leidner 2015; Pourhabibi et al. 2020; Singla 2021)
4.	Commercial Bank	This research article demonstrates the decision tree's efficacy in creating AML rules from client profiles. Anti-money laundering systems at China's small and midsize commercial banks are desperately needed.	(Wang and Yang 2007)
5.	Financial Institute	The paper's primary goal is to identify and evaluate a substantial shift in dealing with money laundering schemes occurring in various nations and assess the risk factor connected with them in the recent past. The research will also examine how the UAE can combat money laundering by developing an AML regime and how special AML units are formed for the above goal.	(Bashir et al. 2020; Gowin et al. 2021; Hong et al. 2017; Kshetri 2021; Lawlor-Forsyth and Michelle Gallant 2018; Lee 2020; Marat 2015; Picard and Pieretti 2011; Xie et al. 2010)
6.	Financial Transaction	A unique feature develop on the base of time-frequency analysis that leverages 2-D demonstrations is presented. Random forest is used as a machine learning approach, while virtual annealing is used for hyper-parameter tuning.	(Chen et al. 2018; Ketenci et al. 2021; Sobh 2020)
7.	Bitcoin	This article focuses on the first comprehensive overview of anti-money laundering (AML) potential and constraints in Bitcoin, a decentralized cryptographic currency gaining popularity.	(Butler 2019; Campbell-Verduyn 2018; Fletcher, Larkin, and Corbet 2021; Möser, Böhme, and Breuker 2013; Stokes 2012)
8.	Counter financing of terrorism (CFT)	The study proposes a method for automating new criminal cases for ML and CFT, which are based on ML/CFT typologies but are not exact replicas.	(Al-Rashidi 2021; Canhoto 2021; Domashova and Mikhailina 2021; Fletcher, Larkin, and Corbet 2021; Omar, Johari, and Sathye 2015; Plachouras and Leidner 2015; Plaksiy, Nikiforov, and Miloslavskaya 2018; Rudner 2010; Shehu 2012)
9.	Cryptocurrencies	The nexus of anti-money laundering efforts and the issues posed by cryptocurrency are discussed in this article.	(Haffke, Fromberger, and Zimmermann 2020; Mabunda 2018)

(*Continued*)

Table 6. (Continued).

S.No	Type of impacts	Description	References
10.	Financial Crime	This article explore the overview of the most recent changes in financial crimes scene and analyzes the challenges that present and emerging graph solutions face in terms of implementation. We suggest that the application needs and implementation obstacles give crucial information for creating effective solutions.	(Kurshan, Shen, and Yu 2020; Watkins et al. 2003)
11.	E-Learning	A study of how e-Learning technologies are employed in banks of UAE is presented in this research. This research focuses on the variables that may have slowed the adoption of such technology.	(Al Hammadi, Zualkernan, and Ahmed 2007)
12.	Fintech	Fintech is being introduced due to society's digital revolution for payments, cash transfers, and other financial activities.	(Nikkel 2020)
13.	Regulatory technology (RegTech)	This study intends to demonstrate the influence of implementing RegTech advances in banks on money laundering prevention efficacy.	(Lee 2020; Turki et al. 2020)
14.	Economy	The article presents endogenously rising violence, the economic gain provided by unlawful money may recruit more criminal departments to the neighborhood or fracture the dominating criminal departments.	(Romero 2020)
15.	Governance	Consequently, the paper presents a framework for security governance: a comprehensive security concept, transnational security spaces, public-private partnership, multi-nodal control, and multi-purpose rationalization.	(Jakobi 2018)
16.	Treasury	The potential of RegTech and the benefits of implementing it into a Smart Treasury department are explored in this article.	(Von Solms 2021)
17.	Anti-money Laundering	This study reviews the existing literature on AI based technology for AML. Researchers examine current AI approaches for AML and propose a framework that implement advanced natural language processing and DL techniques to help develop next-generation AML solutions.	(Han et al. 2020; Maguchu 2018)
18.	Asset recovery	The research findings show that the asset recovery focus has been effective. On the other hand, Respondents expressed concern about conflict and inconsistency in the application of the law, particularly among the police and the courts.	(Sittlington and Harvey 2018)

methodologies and instruments employed in the examined studies. The study is seen to be a good resource for anybody interested in anti-money laundering research utilizing information technology and will help spark fresh interests in the sector, even if it cannot be considered to be thorough. The primary study

publications were sourced from only four separate most peer-reviewed online digital repositories. For analysis and evaluation, 112 relevant publications, including articles, book portions, conference papers, and survey work, were found. The research will aid companies and practitioners by describing the many consequences of ML on our society and economy, as well as integrating AI in financial institutions. The Institutions can adopt an AI risk mitigation plan to improve the efficiency and security of financial companies. It will identify numerous threats before they arise. This comprehensive analysis of current research will help as knowledge for academics and researchers interested in creating safe and secure AML systems for the financial sector in the future. The assumption of this SLR work is that it will foster a strong relationship between the community and the AML system in the face of new research trends. Future research is advised to broaden the scope of this study by manually searching the references of the articles chosen in this review, as well as in pertinent journals, books, surveys and conferences, using the snowball technique.

Conclusion and Discussion

Over the decade, global interest in the phenomenon of money laundering has grown, and it has become a crime. However, most of the research has emphasized money laundering from the standpoint of industrialized nations. As a result, international legislation, policies, and opinion have all been constructed with developed country requirements as their primary focus to combat money laundering. As technology up degrades by the day, many entities or individuals to generate various other channels and provide platforms to transfer dirty money and illegal foreign exchange. ML has long been regarded as a huge danger to the world's economy and financial system. It erodes public confidence in the financial system and puts financial industries and the overall financial system's soundness and stability at risk. Most governments have taken efforts to minimize the occurrence of ML in response to the threat it poses to the worldwide financial system and national economies. Consequently, the expansion of AI applications in the financial sectors is experiencing major difficulties in terms of money laundering and fraudulent activities.

Financial organizations and banking sectors are spending a huge budget to secure their system. AI can play a vital role in controlling ML/CTF. Technology adoption and AI application need to collaborate with each sector nationwide. By using different features and techniques of AI like ANN, machine learning, deep learning, and intelligent robotics, etc., in the existing system to counter the risk of ML/CTF. Organizations need to develop an AI-based AML system to secure money from laundering. It is necessary to check an ongoing process by the government and regulatory bodies to monitor at

each level to maintain sustainable economic growth. Anti-money laundering legislation is supposed to improve financial sectors and the worldwide financial system's reputations, as well as customer confidence and trust. AI technology promotes fast development in the financial sector by assessing and investigating the possible hazards of money laundering at financial companies and institutions. It has shown extraordinary abilities in a multitude of fields, including the financial and regulatory sectors

Globally, FATF plays a significant role in minimizing the risk of ML/CTF. Various countries have committed to submitting different reports to FATF authorities to justify their efforts against AML/CTF. Similarly, the FATF is quite explicit about the revenue and expenditures of some organizations that are being abused in the name of charitable endeavor, such charity. However, the government must have a strong desire and determination to follow through with this instead of unfreezing them as it formerly did. After these precautionary measures by the government and regulatory authorities of various countries still, there are alternative networks adopted by the people to transfer illegal foreign exchange remittance that operates outside of banking channels. This paper aims to examine the existing situation from various perspectives and bring up future research paths to conduct the study and construct high levels of authenticity and security in the financial sector by utilizing AI. In order to resolve this issue, SLR is conducted to analyze for high security, authentication, and safety the most suitable articles accumulated from online peer-reviewed digital libraries.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported by the Qatar National Library [QUHI-CBE-21/22-1].

ORCID

Habib Ullah Khan http://orcid.org/0000-0001-8373-2781

References

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.

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.

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.

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

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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).

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

Keele, S. 2007. *Guidelines for performing systematic literature reviews in software engineering*. UK: Citeseer.

Ketenci, U. G., T. Kurt, S. Önal, C. Erbil, S. Aktürkoğlu, 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.

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.

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

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.

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).

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.

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

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.

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).

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.

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

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

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.

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.

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.

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.

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

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).

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

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.

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.

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.

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.

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.

Möser, M., R. Böhme, and D. Breuker. 2013. An inquiry into money laundering tools in the Bitcoin ecosystem. Paper read at 2013 APWG eCrime researchers summit.

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.

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

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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.

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

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

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

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).

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.

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.

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

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.

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.

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.

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.

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

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).

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

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

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.

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.

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.

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

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.

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.

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.

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

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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