Human TECHNOLOGY

ISSN: 1795-6889

https://ht.csr-pub.eu Volume 20(2), September 2024, 325–360

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN COMBATING ILLEGAL FINANCIAL OPERATIONS: BIBLIOMETRIC ANALYSIS

Serhiy Lyeonov
Silesian University of Technology
Sumy State University
Poland, Ukraine
ORCID 0000-0001-5639-3008

Veselin Draskovic
University of Social Sciences, Poland
ORCID 0000-0003-3968-422X

Zuzana Kubaščikova
University of Economics in Bratislava
Slovakia
ORCID 0000-0001-6739-1278

Veronika Fenyves
Faculty of Economics and Business, University of Debrecen, Debrecen, Hungary
ORCID 0000-0002-8737-0666

Abstract: *Money launderers and corrupt entities refine methods to evade detection, making artificial intelligence (AI) and machine learning (ML) essential for countering these threats. AI automates identity verification using diverse data sources, including government databases and social media, analysing client data more effectively than traditional methods. This study uses bibliometric analysis to examine AI and ML in anti-money laundering and anti-corruption efforts. A sample of 746 documents from 477 sources from Scopus shows a 14.33% annual growth rate and an average document age of 3.51 years, highlighting the field's actuality and rapid development. The research indicates significant international collaboration in documents. The main clusters of keywords relate to the implementation of AI and ML in (1) avoiding fraud and cybersecurity, (2) AML compliance, (3) promotion of transparency in combating corruption, etc. Addressing ethical concerns, privacy, and bias is crucial for the fair and effective use of AI and ML in this area.*

Keywords: *artificial intelligence, machine learning, anti-money laundering, anti-corruption efforts.*

DOI: https://doi.org/10.14254/1795-6889.2024.20-2.5

INTRODUCTION

The swift advancement of cutting-edge technologies like AI, blockchain, cloud computing, and machine/deep learning is driving economic processes into new realms where traditional linear models, finite frameworks, and strict hierarchies become obsolete. Instead, new relationships, connections, and interdependencies continually emerge, which is a hallmark of quantum economics. Holtfort and Horsch (2024) even state thatin recent years, quantum economics has been developing alongside behavioural and evolutionary economic theories, applying principles of quantum physics, such as wave-particle duality and uncertainty, to solve economic problems. The integration of AI and ML into financial security is not only vital for combating illegal financial activities but also holds transformative potential across various sectors, increasing the efficiency of employing human resources, changing the focus of their utilisation from a monotonous detecting to an analytical and controlling one.Numerous articles assert that AI and ML models and techniques provide greater accuracy, transparency, and security across various analytical fields. For example, empirical results from Awe and Dias (2022) indicate that autoregressive artificial neural networks model offers advanced prediction accuracy compared to the traditional method.

Kuzior et al. (2024) found that while the rapid advancement and widespread use of digital technologies enhance oversight of economic activities, they also introduce new challenges related to the rise of cybercrime. Yarovenko et al. (2023a) affirmed that leading nations like the USA, China, Germany, France, and others are both targets and perpetrators of cyberattacks. Moreover, Yarovenko et al. (2024) revealed that social and regulatory factors impact illicit practices in developed countries more than economic and digital factors. Barbu et al. (2024) investigated the trends in scientific collaboration on tax evasion and tax. Vasilyeva et al. (2021) utilized Data-Mining techniques to study the effects of digitalization and the COVID-19 pandemic on the selection of AML approaches. Polishchuk et al. (2019) created recommendations for implementing a cooperative model to enhance the effectiveness of code-based SMART contracts by reducing costs through the automation of manual processes and mitigating legal risks using distributed blockchain technology. Dobrovolska et al. (2021) investigated the evolution and current state of money circulation worldwide, and particularly in Ukraine, in conditions of digitalization and the development of blockchain technology and digital currency.

Governments and regulatory bodies worldwide are placing increasing importance in combating financial crimes. Complying with anti-money laundering (AML) regulations and other financial security measures is an escalating concern for financial institutions. AI and ML technologies aid in meeting these regulatory requirements by offering more accurate and timely detection of suspicious activities, ensuring adherence to laws and regulations, and helping avoid costly penalties. For example, in the mid-1980s, the US Customs Service's Financial Division began developing a system to analyse Currency Transaction Reports. The Financial Crimes Enforcement Network established by the Department of the Treasury then developed the Financial Artificial Intelligence System to identify suspicious patterns in the Currency Transaction Reports database. In 1991, the Advanced Research Projects Agency funded further development of AI systems for combating money laundering, focusing on issues linked to terrorism and illegal arms sales rather than drug trafficking.

Additionally, intelligence agencies are believed to use AI-based techniques for specific types of pattern recognition and analysis related to national security. In 1994, the US Senate formed a subcommittee to investigate the application of AI tools for identifying money laundering. The study found that an electronic funds transfer technology was being used to illegally move money from the US to financial institutions abroad. Consequently, the subcommittee recommended utilising AI in three main areas: acquisition, analysis, and utilisation of knowledge and data (Jensen, 1997).

Androniceanu (2023) indicated a noticeable improvement in management, increasing economic efficiency and social perception of state authorities and governance processes. Consequently, developing and implementing policies for using digital instruments and AI in public governance and state/municipal services leads to the dynamic development of a government. Fülöp et al. (2023) highlighted the ethical concerns related to AI in accounting. According to authors finding, while most accountants who took part in the interview had a basic knowledge of AI, only a few fully grasped the concept. Nonetheless, all participants agreed on the importance of AI ethics and the necessity of regulatory bodies to oversee ethical legislation concerning artificial intelligence. Drăcea et al. (2024) proposed that enhancing governance and human development can advance budget transparency, which ~~in turn~~ can further improve governance and contribute to greater human development by ensuring the efficient allocation of public resources while also considering political factors. Orlandić et al. (2024) suggested that combining robotic process automation with AI and ML improves operational productivity, reduces costs, and increases efficiency in the public sector. Kuanaliyev et al. (2024) highlighted the necessity of adapting the public administration system to digital transformation's emerging challenges and opportunities (including AI and ML). Waldman (2024) discussed the limitations of state-run healthcare systems and advocated for a shift to more technology (AI line predicting, processes for payment confirmation, medical error reviews, and clinical guidelines) and a human-oriented (patient-controlled) model, highlighting its necessity and feasibility. The article by Bozhenko et al. (2023a) reviewed the arguments and counterarguments in the scientific discussion on improving climate finance transparency. It identified data gathering, reporting systems, and accounting and management systems as the main challenges to the formation of an effective climate fund monitoring system. The study's relevance lies in revealing that the largest receivers of global climate finance are countries with high corruption risks, poor human rights protection~~s~~, and low trust in law enforcement and justice systems.

At the international level, the Financial Action Task Force (FATF, n.d.) has emphasized the challenges posed by cross-border money laundering and terrorist financing, intensified by the globalization of financial markets. Criminals and criminal networks exploit regulatory differences across jurisdictions to move illicit funds. AI and ML technologies are pivotal in analysing vast amounts of cross-border transaction data and identifying patterns that could signal illegal activities. AI and ML technologies address the complexities of transnational financial crimes by tracking the flow of funds across borders, detecting anomalies, and alerting authorities,. Beyond their immediate impact on financial security, AI and ML foster international collaboration and information sharing, which is essential for combating illegal activities in a globalized world. Organizations like Interpol and Europol leverage these technologies to enhance their data processing capabilities, significantly improving the detection and analysis of global criminal networks.

Corruption, Money Laundering in Modern Economy

Acar and Kara (2023) concluded that corruption significantly influences trade efficiency , especially in developing countries. The study by Gasimov et al. (2023) found that in non-EU post-Soviet countries, the effect of corruption on economic growth is less pronounced in energy-rich countries than in their energy-poor counterparts. Djouadi et al. (2024) suggested that corruption might encourage investment in these regions in specific contexts and economic environments, particularly if ineffective bureaucratic and stringent policies hinder investment activities (by simplifying processes like acquiring permits, licenses, and access to financing, creating a predictable business atmosphere).

The problem of overcoming corruption is especially significant for Ukraine, as this challenge is identified by the European Commission as the main one on our path to the EU, especially against the background of constant scandals with public procurement, army supplies and bribery. Kovbasyuk et al. (2024) highlighted the lack of significant progress in combating corruption, the lack of transparency in many public administration mechanisms, and the exposed corruption schemes involving the allocation of international military and humanitarian aid and public defence procurement. That threatens the support of international donors and partners, damages Ukraine's reputation globally, hinders its progress towards EU membership, and considerably affects the conclusions of external allies. Bozhenko et al. (2023b) stated that 89% of Ukrainians see corruption as the second biggest challenge to the country's stability after the full-scale war. The findings suggest that while Ukrainian society believes it can tackle corruption, there is limited active engagement, with only revolutionary actions considered in critical situations.

Maile and Vyas-Doorgapersad (2023) specifically investigated the institutional causes of human misconduct within South Africa's public service sector. Kaya (2023) empirically demonstrated and theoretically validated that government behaviour in times of economic or financial crises influences the extent and frequency of bribery in Eastern Europe and Central Asia. Bartulovic et al. (2023) found that corruption assists money laundering, while money laundering, in turn, reinforces corruption. Promoting and improving transparency within the anti-money laundering system is essential, as greater transparency reduces the potential for corruption among all stakeholders involved.

The article by Utkina (2023) investigated the current role of financial monitoring in fighting and avoiding money laundering and corruption. The author argued that with the expansion of blockchain technology, the financial monitoring environment would undergo significant changes, leading to more efficient and successful strategies for preventing and addressing money laundering and corruption. Kuzior et al. (2022) used quantile regressions to study the impact of digitalization on economic transformations. It was found that the level of digital development, influenced by national cybersecurity and ease of doing business, affects countries' susceptibility to fraudulent schemes for legalizing criminal income. The studies by Zámek and Zakharkina (2024), Asare and Samusevych (2023), and Kozhushko (2023) aimed to use bibliometric analysis to identify trends and investigation areas concentrating on the effects of digitalization and transparency on national defence. The research explored how these factors could enhance transparency and combat corruption while presenting challenges to cybersecurity due to the greater availability of information, focusing on financial fraud, tax

instruments, and economic security. It summarised the content and conceptual aspects of research on the digitalization of the economy.

AI and ML in Prevention Financial Crimes

Beyond enhancing research and development, improving staff's education, and fostering their personal development, AI and ML's ability to process vast datasets and identify patterns has implications for financial security. For example, phishing attacks, synthetic identity fraud, business email compromise, and other threats exploiting human mistakes and vulnerabilities are increasingly complex and challenging to detect using traditional methods. Staiger (2023), a content specialist of the Association of Certified Fraud Examiners, noted that technology-enabled schemes, such as deepfakes and social engineering, using AI-generated voice and video for impersonating executives and manipulating financial transactions, are challenging to detect and prevent with conventional techniques. Thus, AI and ML applications in detecting sophisticated cybercrimes contribute significantly to ensuring not just financial integrity but also the overall resilience of digital systems.

AI and ML technologies have significantly improved the capability to detect illegal activities in real time by analysing vast datasets for unusual patterns, which helps avoid human-related mistakes. For instance, major financial institutions now use ML algorithms to observe transaction data in real time, flagging suspicious activities that deviate from a customer's usual behaviour. According to a white paper by Deloitte and UOB (2020), these systems have reduced the incidence of false positives, increasing the accuracy and speed of detecting genuine fraud attempts. One of the critical improvements in AI and ML is the development of adaptive learning models that can evolve with changing patterns of financial crime. These models can learn from new data or even mine the data about customer patterns from social media, open data or internal bases, etc., and update themselves to identify emerging threats more effectively.

A publication by McKinsey & Company's experts underscores how AI and ML technologies have significantly reduced false positives in anti-money laundering (AML) systems. Traditional monitoring methods often generate an overwhelming number of false alerts, requiring extensive human resources to review and resolve. By integrating AI and ML, banks, insurance companies, and other financial institutions can more precisely identify genuine suspicious activities. This improvement lowers the costs associated with manual investigations involving human resources and allows institutions to allocate their resources more effectively, ultimately decreasing operational expenses on their staff (Doppalapudi et al., 2022). Čejka et al. (2023) demonstrated effective screen change recognition with minimum incorrect negatives and adequate mistaken positives, highlighting the potential for increased automation in examining. The study suggested that these technologies could promote user-centric innovations across different industries.

Furthermore, FOCAL (2023) suggested that AI and ML systems can automate fraud detection, enabling real-time monitoring of financial transactions through analysing vast datasets to detect patterns indicative of fraud, such as unusual transaction volumes or atypical human spending behaviours. Financial institutions adopting these technologies have reported substantial reductions in the time and cost associated with fraud detection and investigation, offering a competitive advantage in a tightly regulated industry. Lăzăroiu et al. (2023) studied how crowdfunding and blockchain fintech operations leverage AI algorithms, cloud

computing, deep and machine learning, augmented and virtual reality, and big data analytics in mobile payment transactions. According to the authors' findings, these technologies enhance the speed and accuracy of detecting suspicious transactions. Lei et al. (2024) explored China's implementation of the Digital Currency Electronic Payment (DCEP) project that challenges the existing framework for monetary crimes and includes a new form of legal tender covering contracts, transactions, identity information, and much more. DCEP is designed to resolve several emerging challenges, such as expanding the range of legal interests impacted by criminal activities, redeveloping the components of monetary crimes, diminishing criminal law's preventive role, and complexities in distinguishing between concurrent crimes. Botoc et al. (2024) argued that Big Data had significantly revolutionised the fintech industry, allowing companies to enhance decision-making, analyse customer behaviour, and create innovative products like personalised investment portfolios, risk-based pricing, and fraud detection solutions. Roba and Moulay (2024) explored the risks that banks encounter and the strategies for managing these risks, employing the artificial neural network model for various classification and discrimination tasks among institutions. Druva Kumar and Senthil Kumar (2024) noted that the contemporary insurance industry integrates advanced technologies like AI and ML and focuses on appearing tendencies such as digital changes and a customer-centric approach.

As AI and ML evolve, their integration into global efforts against financial crimes promotes international collaboration, improving communication and cooperation between institutions, authorities, and nations. Therefore, this technological advancementextends beyond the security domain, contributing to a more transparent and trustworthy global financial system. The commitment to implementing AI and ML in financial operations underscores their importance in shaping a secure, equitable, and progressive future. Dabija and Vătămănescu (2023) argued that AI had become embedded in our daily lives, transforming industries such as healthcare, finance, and transportation. Bilan et al. (2022) shared a similar perspective, exploring the interaction between AI from one side and management, change, culture in organisation, and organizational development from another side. Some research, for example, an article by Piotrowski and Orzeszko (2023), provided suggestions on the exploitation of AI technologies in finance with a focus on the ethical side of using such tools by banks. Durica et al. (2023) sought to innovate in predicting financial distress by developing individual models and ensembles, utilising ML techniques. The study by Abid et al. (2024) is unique in that it introduced AI and technological competence as moderating factors in achieving the advantages of implementing personnel service. In the paper by Pouabe et al. (2023), the managerial impact of decision-making is demonstrated using various data and two artificial neural network techniques in analysing the company's operations. Sahnouni and Benghebrid (2023) advocated for organisations to find a cost-effective and accurate system that reduces the influence of individual human prejudices during evaluations by adopting an innovative approach, improving objectivity, especially in complex systems. Skrynnyk and Lyeonov (2023) discussed that Big Data, Blockchain, and AI have similar applications in financial control and accounting in governmental authorities and commerce enterprises. They noted similarities in technical specifications like cryptocurrency, but differences in specific areas such as social networking problems in public services.

AI and Chellenges of Human Behavior and Data Sensivity

Managing sensitive human and financial data is a significant concern when using AI and ML to combat illegal financial operations. Guaranteeing data privacy and security while retaining the efficiency of these systems is a critical challenge. The paper by Höller et al. (2023) explored public awareness regarding unethical artificial intelligence and the actions that can be taken to counteract it (mitigation measures). The empirical findings indicated that an individual's awareness of improvement is induced by their self-efficacy, whereas trust in the algorithmic platform is of no significant influence. The most suggested mitigation measures include laws and regulations, algorithm audits, and education and training. Sheliemina (2024) argued that the application of AI in medicine comes with risks concerning ethics and data privacy, issues with the quality of data applied for learning procedures, and the need to protect against cyber threats. Additionally, there is a concern that medical costs may increase due to the extensive testing and validation required for new technologies. Dobrovolska et al. (2024) emphasised that the expansion of health digital databases and sites containing data on patients, hospitals, and medications, along with the increased use of remote access tools in healthcare, the rapid growth of telemedicine, especially during the COVID-19 pandemic, and the advancement of big data-driven cure technologies, such as computational oncology, necessitate robust cybersecurity measures. It is essential for clinics to safeguard the personal information, and for hospitals and health insurance companies to safeguardthe financial information, , guard patient records against cyberattacks, and guarantee fastened data exchange within the public health sector.

Behavioural analytics, powered by AI, can detect unusual behaviours that may indicate illegal activities. This includes the analysis of transaction patterns, frequency, and volume, which can reveal money laundering attempts or the financing of illegal operations. Oe and Yamaoka (2023) measured the effects of individuals' behaviour and interactions in the digital environment on altering personal behavioural models in the real world. Yarovenko et al. (2023b) proposed an approach to modelling the potential actions of insider cyber swindlers in banks. The study revealed that potential insider cybercriminals in banks are primarily interested in obtaining clients' personal financial information, accessing their online banking profiles, and acquiring their phone data. Ballester et al. (2023) examined how followers' behavioural engagement impacts word of mouth and the intention to participate in an activity, focusing on the moderating role of consumers' attitudes towards using unique tags in posts. The study's research model was tested using a sample of followers from the social media accounts managed by the establishment. Urbonavičius and Degutis (2023) argue that digitalization shapes various economic behaviors that occur online or combine online and offline activities. Their findings reveal an indirect effect of the willingness to disclose personal data and shed light on how privacy risks influence decisions related to online and offline behaviors.

Continued research and innovation in this field are crucial for enhancing the effectiveness and fairness of AI and ML systems in financial security. Addressing these investigational gaps through more comprehensive and inclusive bibliometric analyses can provide a clearer picture of the current landscape and future directions in implementing AI and ML to combat illegal financial operations. It will also ensure that the research community and industry practitioners are better equipped to tackle the complex challenges of financial crimes in a rapidly evolving digital landscape.

METHODS

To better understand the scope of issues, both explored and underexplored, identified in the literature review, it is also recommended to perform a bibliometric analysis of publications in artificial intelligence and machine learning in combating illegal financial operations. Considering this, we formulated several key research questions:

RQ 1: Is there an increasing research interest in applying AI and ML to combat illegal financial activities?

RQ 2: What are the main findings and trends in research focusing on AI and ML's function in addressing illegal financial operations?

RQ 3: Has there been a shift in research focus towards a more detailed examination of specific factors influencing the use of AI and ML in combating illegal financial activities?

When detailing the research methodology, it is vital to focus on three primary sections: data collection, cleaning, and analysis.

Data Collection

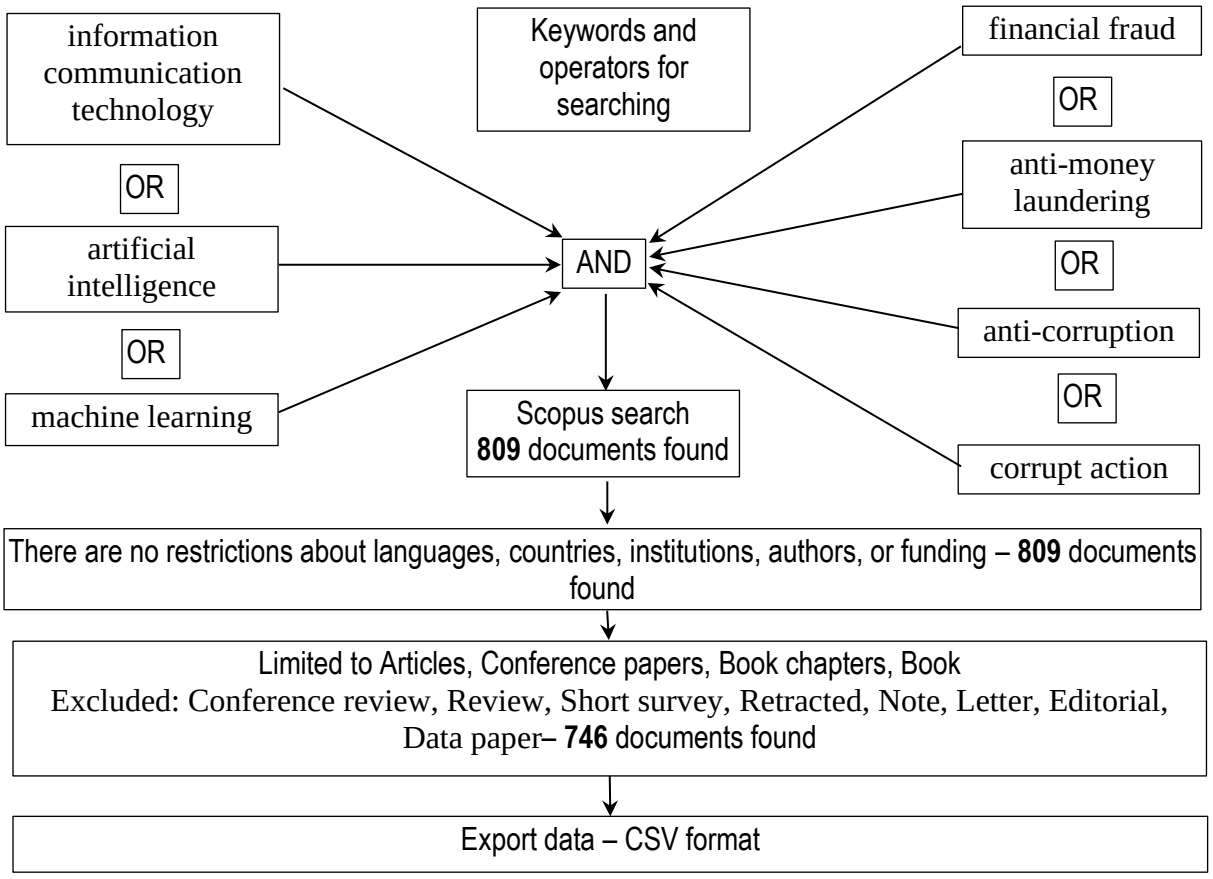


Figure 1. Data collection for searching in Scopus database documents with a focus on AI and ML's role in addressing illegal financial operations

Source: developed by the authors

Figure 1 is proposed to illustrate the data collection process, which utilises the Scopus database. Scopus is chosen for its extensive and comprehensive content coverage and its user-friendly interface, which includes individual profiles for authors, institutions, and journals. Its reliable impact indicators are less prone to manipulation and are obtainable for all sources (journals, proceedings of conferences, books etc.) in various scientific areas. Scopus stands out for its transparency and public accessibility, offering access free of charge to multiple metrics (Pranckutė, 2021). It also provides the convenience of accessing content through a single database, thus avoiding confusion and access limitations. Furthermore, Scopus enables operators to take search results in several formats, such as CSV, Bibtex, and Excel.

Data cleaning

The following keywords were excluded because they reference not precisely to the area of research but more to the characteristics of the sample for investigation (countries or their groups, or they pertain directly to the research methodology and reporting of results), that is not relevant to our objectives. Therefore, it was decided to exclude next keywords: logistic regression, xgboost, based, study, de, review, paper, research, results, authors, author, ieee, proposed.

The words listed below were recognised as synonyms, enabling their metadata to be combined during the analysis:

- information and communication technologies, information and communication technology, ICT, information technology;
- machine learning, machine-learning;
- machine learning algorithms, machine learning methods, machine learning techniques, machine learning models, learning algorithms;
- blockchain, blockchain;
- investment, investments;
- neural network, neural-networks, neural networks, neural-network;
- anti-money laundering, anti-money laundering (AML), AML;
- system, systems;
- technology, technologies;
- method, methods;
- algorithm, algorithms.

Data analysis

This investigation uses Biblioshiny and Excel to analyse and present gathered data from Scopus databases. Data from Scopus was first imported into Biblioshiny, and then each result was individually exported to Excel. As a result, 746 publications were analysed using bibliometric methods. Complete evidence about the quality of different metadata of the sample of documents with a focus on AI and ML in combating illegal financial operations and on the next stage used for the bibliometric investigation is presented in Table 1.

Table 1. Completeness of bibliographic metadata [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Metadata	Description	Missing Counts	Missing %	Status
AB	Abstract	0	0.00	Excellent
AU	Author	0	0.00	Excellent
DT	Document Type	0	0.00	Excellent
SO	Journal	0	0.00	Excellent
LA	Language	0	0.00	Excellent
PY	Publication Year	0	0.00	Excellent
TI	Title	0	0.00	Excellent
TC	Total Citation	0	0.00	Excellent
C1	Affiliation	5	0.67	Good
CR	Cited References	16	2.14	Good
DI	DOI	75	10.05	Acceptable
DE	Keywords	94	12.60	Acceptable
ID	Keywords Plus	254	34.05	Poor
RP	Corresponding Author	272	36.46	Poor
WC	Science Categories	746	100.00	Completely missing

The sample documents were selected from publications released between 1991 and the first half of 2024 (Table 2). According to Biblioshiny, these publications featured 2103 unique authors, including 85 single authors. These 85 authors published 89 single documents. Also, on average, more than three authors cooperated in research (indicator Co-Authors per Document is 3.31). Interestingly, almost half of all documents (49.06%) are conference papers.

Table 2. Descriptive Statistics of the Sample Publications [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	1991:2024
Sources (Journals, Books, etc)	477
Documents	746
Annual Growth Rate %	14,33
Document Average Age	3,51
Average citations per doc	12,98
References	24133
DOCUMENT CONTENTS	
Keywords Plus (ID)	2893
Author's Keywords (DE)	1749
AUTHORS	
Authors	2103
Authors of single-authored docs	85
AUTHORS COLLABORATION	
Single-authored docs	89
Co-Authors per Doc	3,31
International co-authorships %	18,23
DOCUMENT TYPES	
article	315
book	6
book chapter	59
conference paper	366

RESULTS

Over the entire period 1991-2024 (it should be noted that for the year 2024, only the publications of the first half of the year are included) on AI and ML in combating illegal financial operations, it is possible to state that there is a growing number of publications with an annual growth rate of 14.33% (Table 2). At the same time, a significant part of the publications is dated in recent years, and the average age of the document is 3.51 years (Table 2). Analysis of the dynamics of publications allows us to distinguish the following three periods:

1) 1991-2002 - the periodic appearance of publications and the initial appearance of interest of scientists in the issues of AI and ML in combating illegal financial operation, although interest in the development and promotion in the practical plane was observed as early as the late 1980s, as mentioned earlier, FinCEN was instituted by the Department of the Treasury in 1988-89. Furthermore, the lack of scientific publications is surprising.

2) 2003-2015 – variable publication activity of authors in this topic with a growing trend, which has the form of an exponential equation $y = 1{,}3804e^{0{,}1532x}$, the coefficient of determination approaches 0.7 ($R^2 = 0.6797$), so we can assert about the high level of reliability of the obtained equation describing the trend (Figure 1).

3) 2015-2024 – rapid growth, which is described by the equation of the polynomial trend of the second-degree $y = 2{,}9286x^2 - 2{,}0952x + 9$, the coefficient of determination of the trend $R^2 = 0.9936$, which indicates the almost 100% reliability of the obtained forecast trend for 2024- 2026. According to this forecast, further rapid growth in scientists' publication activity on the analysed topic is expected. In 2026, the number of publications will reach the mark of 340 documents (Figure 1).

The oldest publication on AI and ML in combating illegal financial operations is an article by Sherizen (1991), which explored the influence of Unification '92 on information safety. While considerable effort had been concentrated on developing the assessment measures for information technology security by experts, further crucial yet indirect decisions about information security were being made. The outlined decisions regarding Unification '92 could be critical in shaping information defence after 1992. The author mentioned that numerous EC directives and outcomes, some not explicitly labelled as information security, will significantly influence the protections that will be feasible and required. The major categories of these include decisions related to the following: (1) to technical part (computer and communications technologies); (2) to legal resolutions and the definition in legislation of financial errors, crimes, and disputes; (3) to political and public policies related to the overall economy and the regulatory restrictions imposed on financial services operations, services, and products. The author also provided examples of these categories from critical European information services, auditing standards and constraints, anti-money laundering controlling systems, open boundaries, and electronic data intersection.

The following article on the subject under investigation appeared only in 1995. The article by Goldberg and Senator (1995) explained that databases often struggle to identify entities of interest accurately. To address this, two operations – consolidation and link formation – were proposed as crucial components for Knowledge Discovery in Databases (KDD) systems, complementing traditional machine learning practises that use clustering based on similarity. Merging and linkage arrangement can be efficiently implemented as index formation in

interactive catalogue organisation systems. An operational KDD system utilises these techniques to detect possible money laundering behaviours within a database of significant money operations.

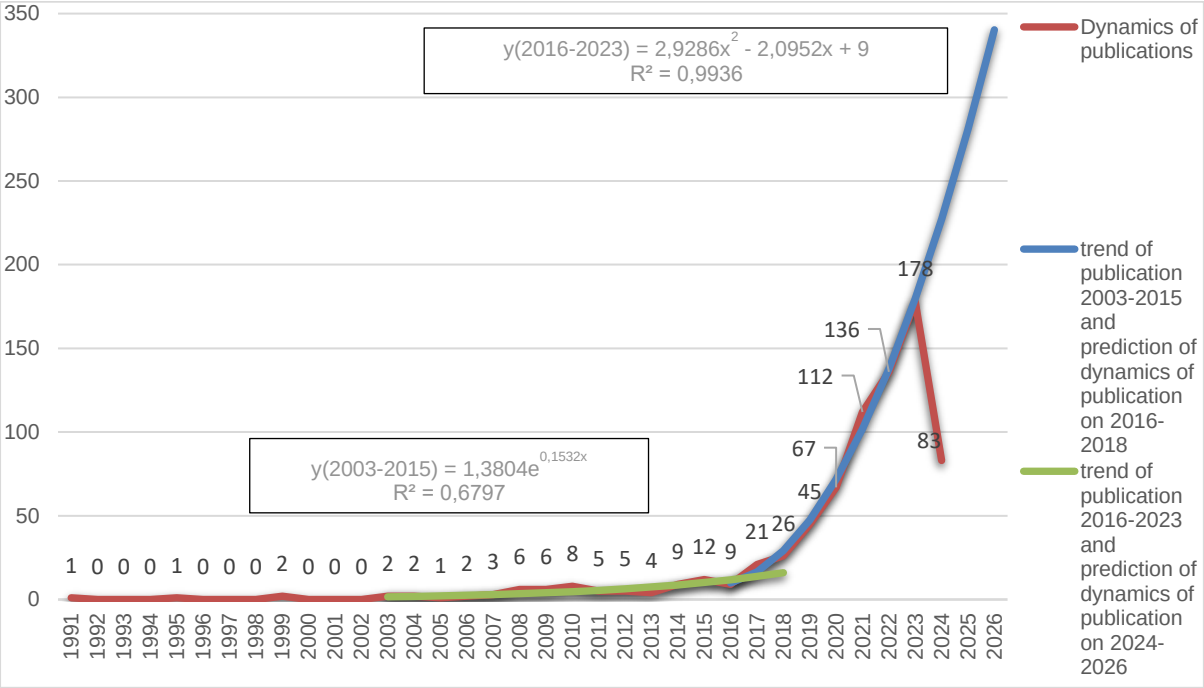


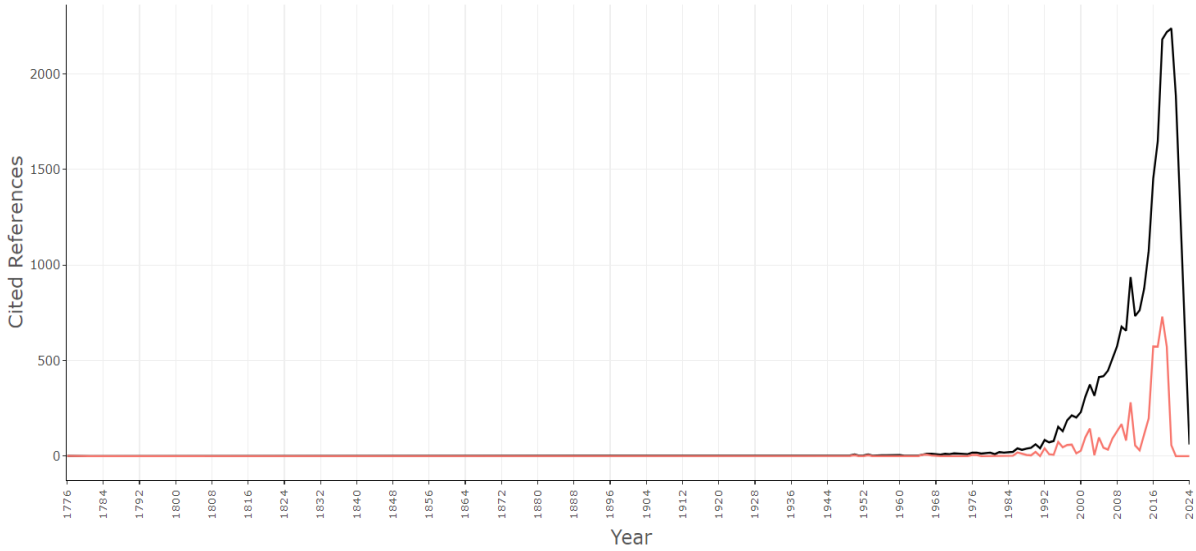
Figure 1. Dynamics and the trends of publication on the topic of AI and ML in combating illegal financial operations.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)].

The most cited reference among publications on AI and ML in combating illegal financial operations is Randhawa et al. (2018), which explored using machine learning algorithms to detect credit card fraud. The study began with standard models and then introduced hybrid methods, including AdaBoost and majority voting techniques. The effectiveness of these models was evaluated using a publicly available credit card dataset, followed by testing on a real-world dataset from a financial institution. To further assess the robustness of the algorithms, noise was introduced to the data samples. The experimental results indicated that the majority voting method performs exceptionally well, achieving high accuracy in detecting fraudulent transactions. This reference had 21 local (among a sample of publications) citations.

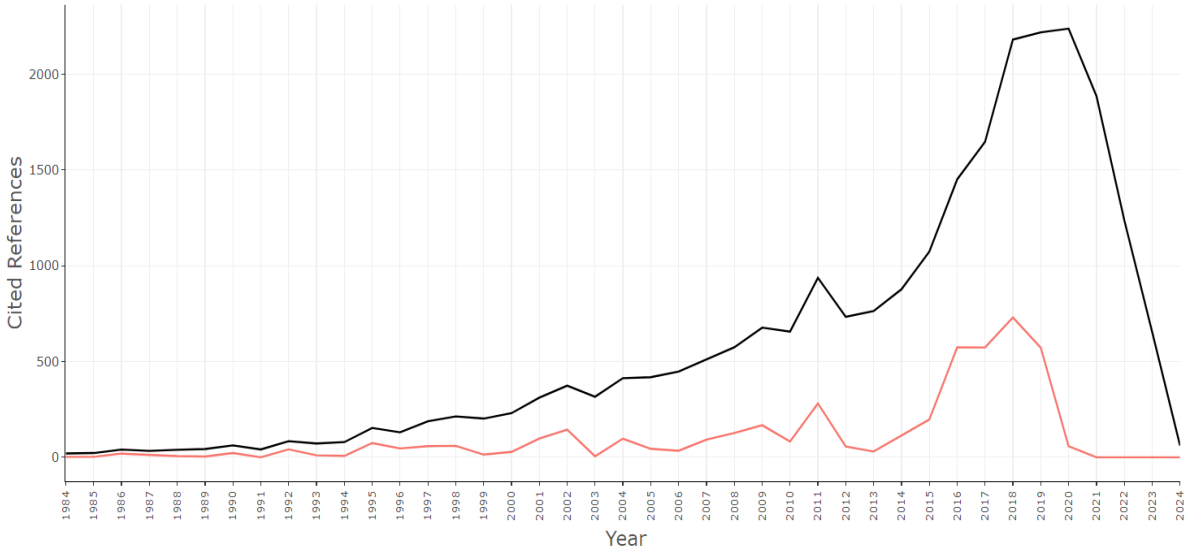
On the second position (20 local citations) is the article by Bhattacharyya et al. (2011), which equivalenced the efficacy of different procedures, including support vector machines, random forests, and logistic regression, in identifying fraudulent transactions to advance the detection, control, and prosecution of credit card fraud by evaluating and recommending the most effective data mining approaches. Using real transaction data from an international credit card operation, the authors also aimed to determine which methods provide the best effectiveness, considering accuracy and reliability.

Biblioshiny App allows for the building of reference spectroscopy to understand the peaks of a citation and to analyse their connection with events in that period. Figure 2 presents such

spectroscopy for the sample of publications on AI and ML in combating illegal financial operations.



a) whole period



b) 1984-2024

Figure 2. Spectroscopy for the sample of publications on the topic of AI and ML in combating illegal financial operations (Black – Number of cited references per year; Red – Deviation from the 5-year median)

[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Among 2103 authors in our sample (Table 2), the most productive author focusing on AI and ML in combating illegal financial operations is Jingyu Li, a researcher from the School of Mechatronics Engineering of the Beijing Institute of Technology (Beijing, China). The other most productive authors (that published five or more articles) and the indicator of their fractionalised articles are presented in Figure 3.

Lotka's law is a rough inverse-square law, stating that the number of authors publishing specific articles is fixed to the number of authors publishing just one article. According to Lotka's law, as the amount of published articles rises, the frequency of authors producing that many publications decreases.

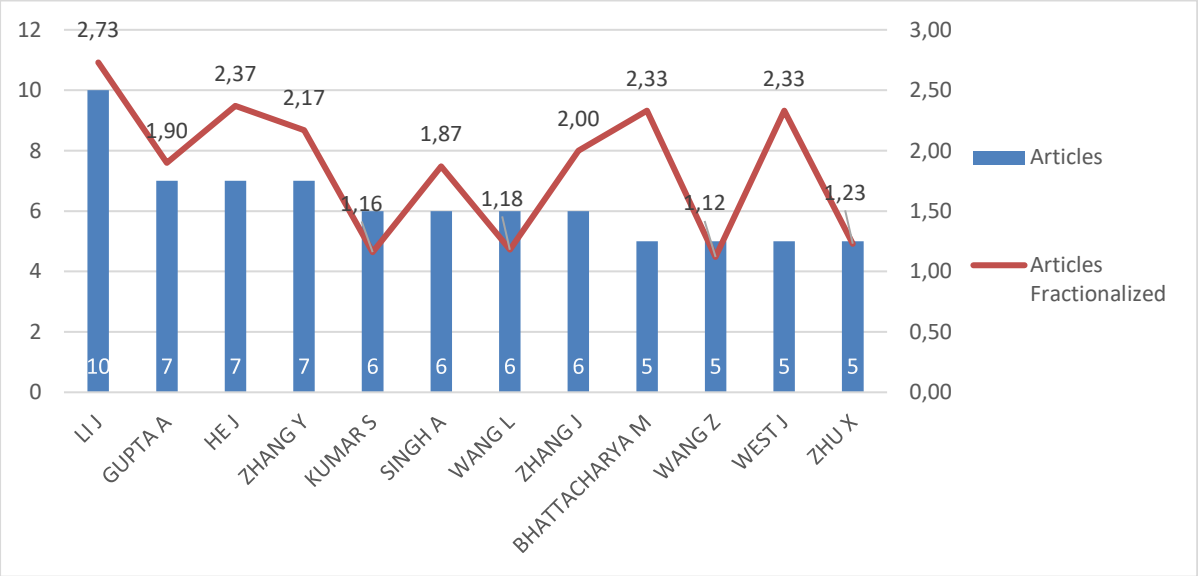


Figure 3. The most productive authors (that published five or more articles) and the indicator of their fractionalised articles.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

In our case, there is only 1 (0.14% of all authors) author (Li J.) that published ten articles on the topic of AI and ML in combating illegal financial operations, three authors (Guptaa A., He J., and Zhang Y. – 0.14% from 2103 authors) published seven articles, two groups of 4 authors each (0.02% of all authors) published 6 and 5 articles, respectively, 45 authors (2.1%) published four articles, 144 authors (6.8%) have two articles in their portfolio.

Table 3. Authors' local impact [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Element	H_Index (Hirsch index)	G_Index	M_Index (H_Index/namber of year from first publication)	TC (Total Citations)	NP (Number of Publica-tions)	PY_Start Start Year of Publica-tions
He J.	6	7	0,353	128	7	2008
Singh A.	5	6	0,833	59	6	2019
Bhattacharya M.	4	5	0,4	64	5	2015
Gupta A.	4	7	1	62	7	2021
Jain A.	4	4	0,667	64	4	2019
Li J.	4	7	0,4	59	10	2015
West J.	4	5	0,4	64	5	2015
Chen Y.	3	4	0,6	19	4	2020
Gao S.	3	3	0,158	75	3	2006
Garcia-Bedoya O.	3	3	0,6	29	3	2020

Other 1880 (89.4%) authors have published only one article. We provide an analysis of the authors' local impact by calculating the indexes, including the H-index, G-index, and M-index, that characterised different sides of the citation of their articles (Table 3). He J. is the most influential author with the highest H-index, G-index, M-index, and total citations. Singh A. has the highest M-index (0,833) because this author started his scientific activity much later than He J (2019 against 2008).

Biblioshiny App allows the creation of a Sankey Plot by selecting three main meta-data fields. If we choose the top references, authors, and keywords, we can build the Graf by focusing on top authors, their intellectual roots (references), and research content (keywords).

The most cited «roots» among the top 12 authors are the following: Randhawa et al. (2018), Bartoletti et al. (2018), Bhattacharyya et al. (2011), Chen et al. (2018), Kirkos at al. (2007), Nakamoto (2008) were cited three times, others were cited once (Figure 3).

Almost all the top authors cited references from the top group. Still, two authors, Bhattacharyya M. and Zhang Y., did not refer to articles from the top group of references. This is explained by the fact that the articles of such author, Bhattacharyya M., are explanations because his research was included in the top group of references. However, the work of Zhang and Trubey (2018) is included among the top 30 references for the analysed topic (Figure 4). Regarding keywords, it is impossible to identify preferences among the top 20 authors (Figure 4).

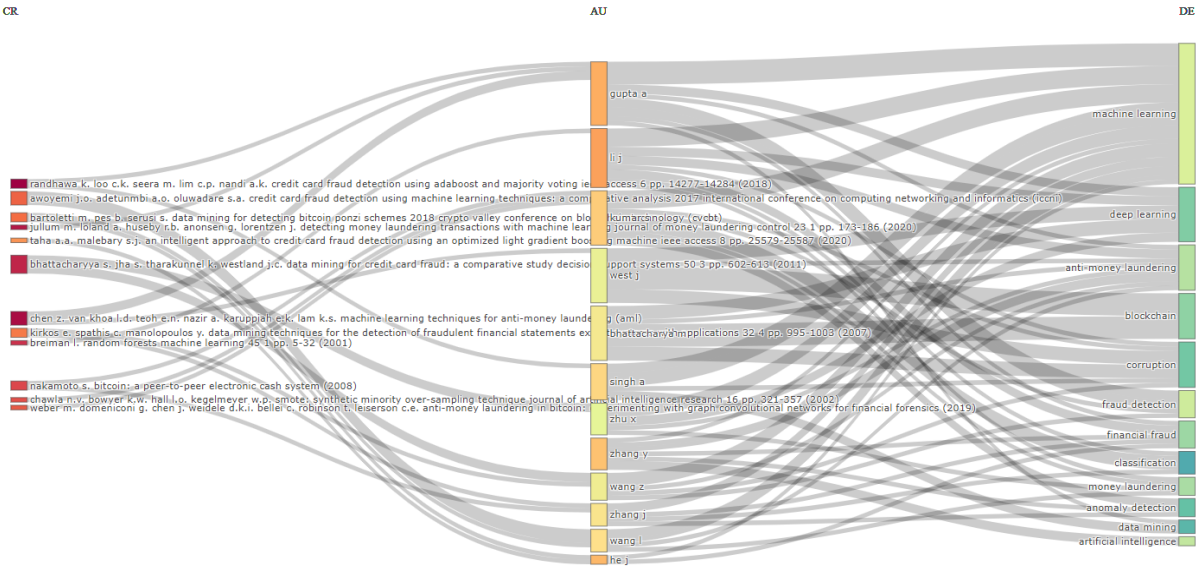


Figure 4. The three-field plot «References – Authors – Keywords" focuses on AI and ML in combating illegal financial operations.

[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

According to Table 2, international co-authorships are 18.23%, which means that almost one of the fifth articles is a collaborative investigation. Table 3 presents statistics on the output of scientists from various countries, measured by the number of publications. Only authors from top countries such as Canada, Bangladesh, and Brazil published single-country publications; others have worked in solid international cooperation. The highest level of MCP_Ratio is linked with the United Arab Emirates. The undisputed leader in the number of publications is China (12.9% of publications), and the top 5 countries also include India, the USA, the United

Kingdom, and Italy. The top 5 countries account for 32.7% of all publications. The top 23 countries (5 or more publications) account for almost 50% of publications (Table 4).

Table 4. Corresponding Authors's Countries (affiliated authors published five or more articles) and their affiliated author's publication activity characteristics. [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Country	Number of the articles	Single Country Publications	Multiple Country Publications	Ratio of publications within the sample	Multiple Country Publications / total number of publications by country
China	96	75	21	0,129	0,219
India	77	71	6	0,103	0,078
USA	29	22	7	0,039	0,241
United Kingdom	24	17	7	0,032	0,292
Italy	18	11	7	0,024	0,389
Australia	14	11	3	0,019	0,214
Malaysia	10	8	2	0,013	0,2
Canada	9	9	0	0,012	0
Germany	8	6	2	0,011	0,25
Korea	8	7	1	0,011	0,125
Poland	8	7	1	0,011	0,125
Saudi Arabia	8	5	3	0,011	0,375
Spain	7	6	1	0,009	0,143
Greece	6	5	1	0,008	0,167
Morocco	6	5	1	0,008	0,167
Turkey	6	5	1	0,008	0,167
United Arab Emirates	6	2	4	0,008	0,667
Austria	5	2	3	0,007	0,6
Bangladesh	5	5	0	0,007	0
Brazil	5	5	0	0,007	0
Colombia	5	3	2	0,007	0,4
Netherlands	5	3	2	0,007	0,4
PortugalP	5	5	0	0,007	0

Biblioshiny allows the building of countries' collaboration networks. In the red cluster, India is leading with the Betweenness indicator (198.176). Interestingly, authors from other countries of the red cluster cooperate actively with authors from other clusters. The closest connection in the blue cluster is observed between the authors of the USA and the UK (Betweenness is equal to 176.704 and 103.844, and the closeness of both countries is equal to 0.15). The authors of these countries are also closely connected with China (Betweenness is 96.539, and closeness is 0.13). The authors of the only country of the turquoise cluster are related to the USA. Similarly, authors from Indonesia (grey cluster) and Mexico (orange cluster) are linked by co-publications with authors from Malaysia. It should be noted that the authors of the purple cluster (Ukraine and Kazakhstan) and the brown cluster (Cyprus and Iran)

have joint publications exclusively among themselves and are not connected by joint publications with authors from other countries (Figure 5).

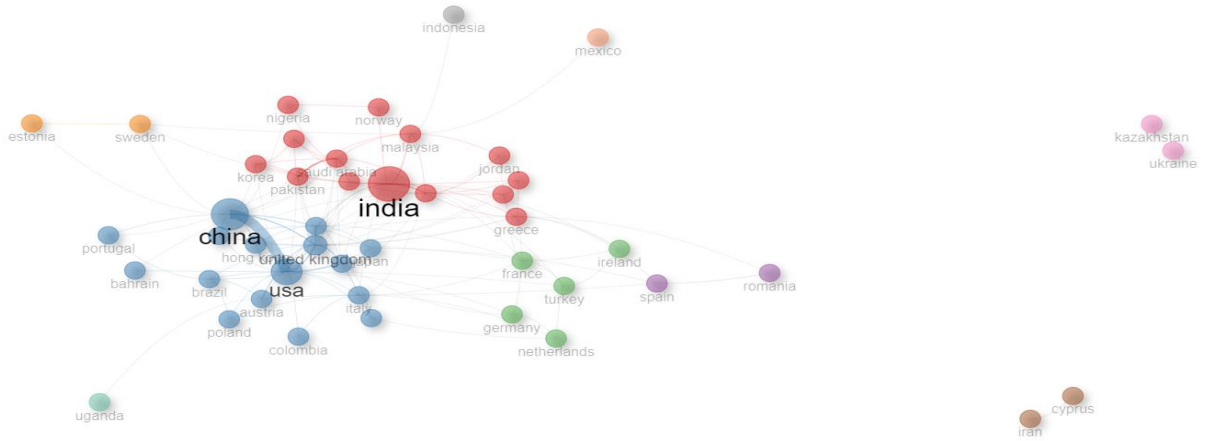


Figure 5. Collaboration network of the countries
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Biblioshiny allows the building of Sankey Plot based on the top countries, affiliated institutions, and authors (Figure 6). We can state that most institutes cooperated with authors from several countries. So, Politecnico di Milano employed authors from Italy, the USA, and the UK. Although there are institutions affiliated with authors from only one country, for example, Sun Yat-Sen University is linked only with authors from China. Just some top 20 institutions collaborated with authors from the top 12 list (those with five or more publications). Only Hunan University of Finance and Economics, Sun Yat-Sen University, University of Electronic Science and Technology of China, and Tongji University have experience in employing such authors (Figure 6).

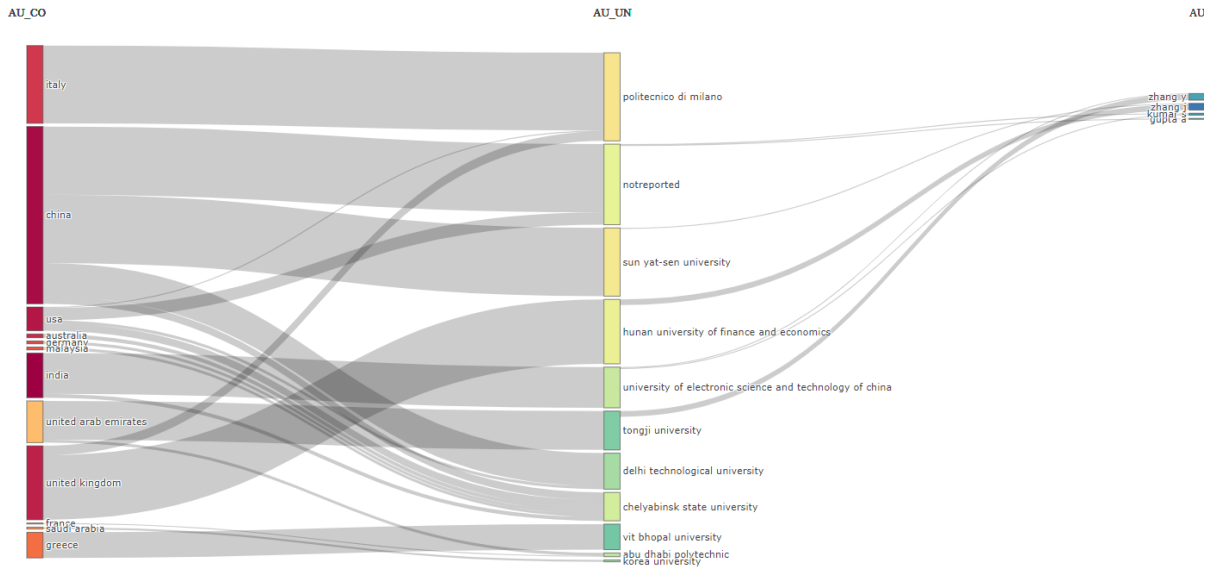


Figure 6. Three-field plot «Countries – Institutions – Authors».
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

From our sample of 477 sources (Table 2), the top 15 sources are mostly conference papers. Table 5 presents the top 15 sources in the sample of publications focusing on AI and ML in combating illegal financial operations.

Table 5. The top 15 most relevant sources [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Sources	Articles
ACM International Conference Proceeding Series	23
Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	20
IEEE Access	19
Lecture Notes in Networks and Systems	17
Procedia Computer Science	14
Communications in Computer and Information Science	13
Journal of Money Laundering Control	13
Advances in Intelligent Systems and Computing	12
CEUR Workshop Proceedings	12
Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining	8
AIP Conference Proceedings	7
Expert Systems with Applications	7
Journal of Financial Crime	6
Lecture Notes in Electrical Engineering	6
Proceedings - 2022 IEEE International Conference on Big Data, Big Data 2022	5

Bradford's law states that consecutive zones of journals with the same number of articles on a particular topic create a simple geometric series. The three categories or «zones» of journals are (1) journals that provide the weightiest insights into the topic, which include 35 items in this case; (2) sources that make occasional but noteworthy contributions, totalling 196 items; and (3) journals with minimal impact, which comprise 246 items. Figure 7 represents the core zone of the sources according to Bradford's law, which published documents focusing on AI and ML in combating illegal financial operations.

Table 6 provides critical data for evaluating the local impact of journals. Notably, our sample's journal, «“IEEE Access»” (a multidisciplinary, all-electronic archival journal), got the highest level of all metrics, including the H-index, G-index, and M-index. Interestingly, IEEE Access does not get the most significant total citations (TC), relinquishing the leading position to the journal Expert Systems with Applications. The last one is also ahead of the Journal of Money Laundering Control (third H-index) and the ACM International Conference Proceeding Series (fourth H-index) by the indicator M-index. However, they have higher H-indexes and G-indexes.

Investigation of source activity over time shows that such publications as Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) began to publish individual articles on the topic with a focus on AI and ML in combating illegal financial operations as early as the 1990s. Still, most sources

began to publish articles much later in the 2020s actively. During this period, a rapid increase in publication activity on the analysed topic was observed in all the top 9 sources (Figure 8).

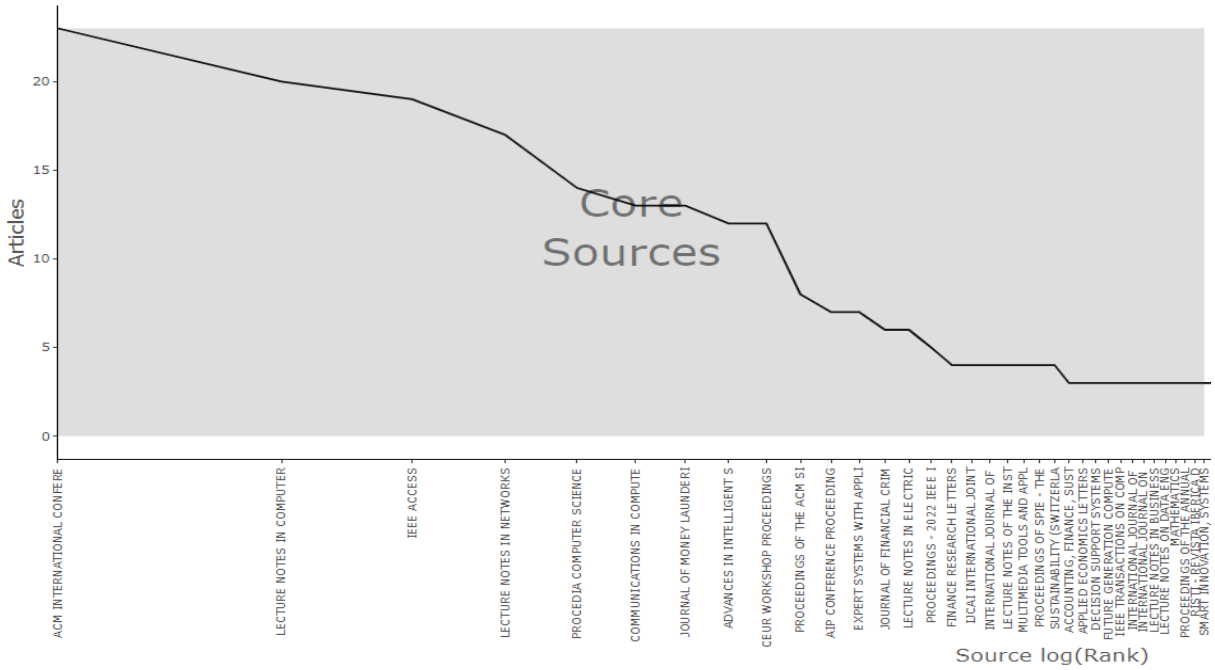


Figure 7. Core sources by Bradford's law
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Table 6. Local impact of top 10 sources in the sample of the documents with a focus on AI and ML in combating illegal financial operations [Source: developed by the authors (based on the Scopus database using the Biblioshiny App).]

Element	H_Index	G_Inex	M_Index	TC	NP	PY_start
IEEE Access	10	17	1,429	298	19	2018
Procedia Computer Science	9	14	1	232	14	2016
Journal of Money Laundering Control	7	13	0,389	245	13	2007
ACM International Conference Proceeding Series	6	14	0,462	206	23	2012
Expert Systems with Applications	6	7	0,75	437	7	2017
Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	6	11	0,231	135	20	1999
Advances in Intelligent Systems and Computing	4	8	0,571	68	12	2018
Communications in Computer and Information Science	4	6	0,571	48	13	2018
Journal of Financial Crime	4	6	0,667	65	6	2019
CEUR Workshop Proceedings	3	6	0,375	44	12	2017

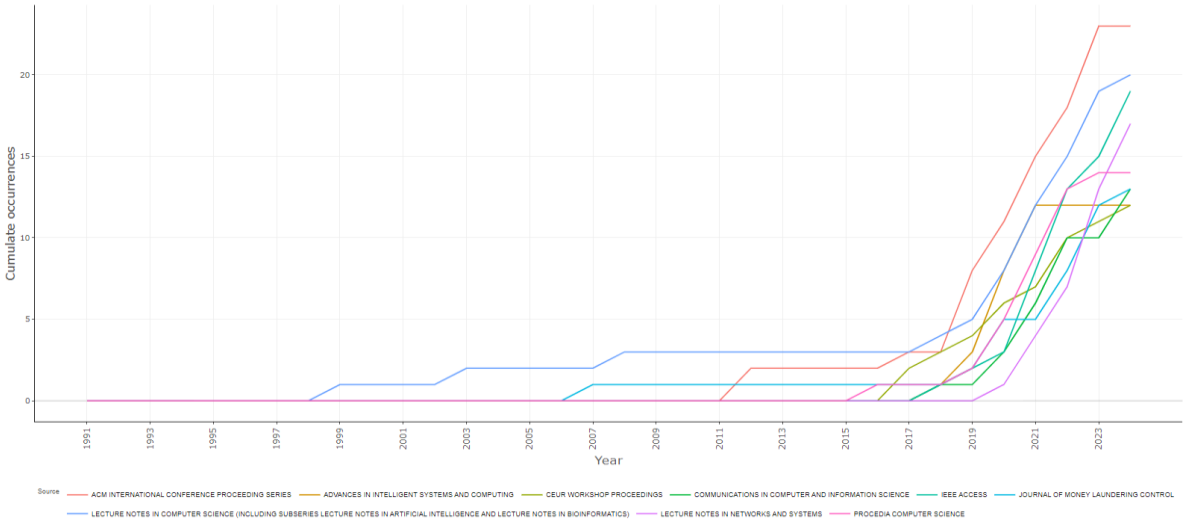


Figure 8. Top 9 sources' production over time.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Sankey plot based on the top sources, authors, and keywords (Figure 9) allows us to state that half of the top 20 sources published the authors' documents from the group's top 20. Most top authors published in Procedia Computer Science (5 from 20) (Figure 9). Also among the top 20 authors were the popular the ACM International Conference Proceeding Series (3 from 20 authors published in this source), the Journal of Money Laundering Control (3 from 20), the Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (3 from 20), etc. As for keywords, we cannot divide sources into specialisations according to keywords (Figure 9).

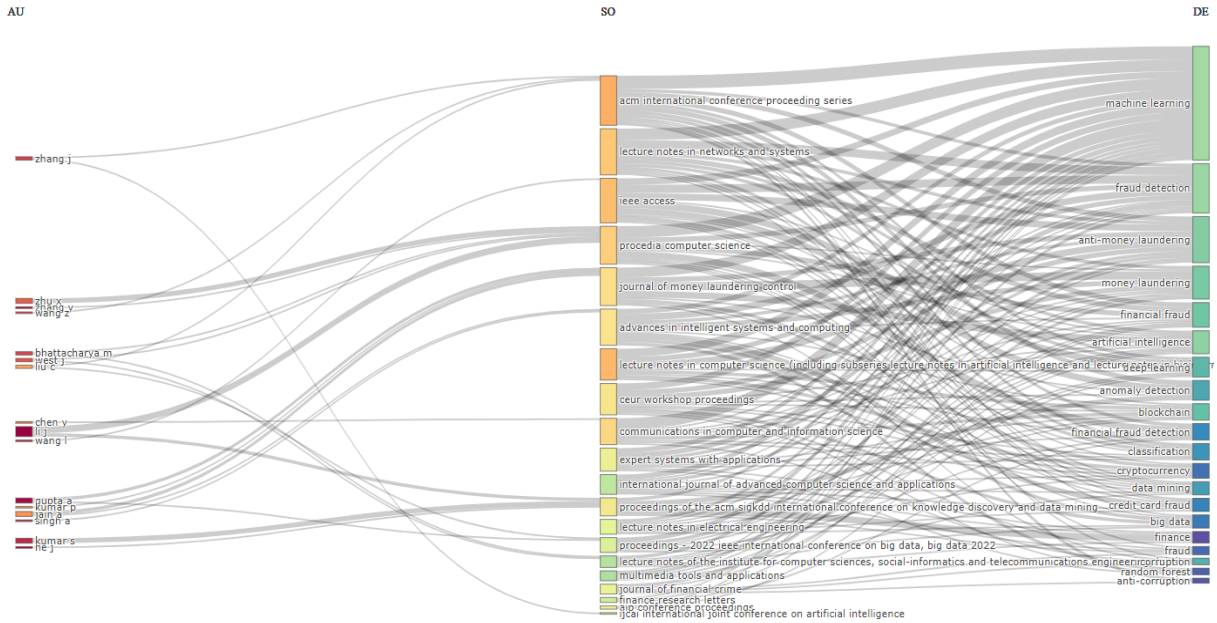


Figure 7. Three-field plot “Authors – Sources – Keywords» of publication with focus on AI and ML in combating illegal financial operations.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

As can be observed in Figure 8, documents are characterised by low citation rates for almost the entire period. Only 2010 differs by meaningful indexes MeanTCperArt and MeanTCperYear owing to the paper by Bertot et al. (2010), which has 1591 citations and specifies such a significant variation of 2010 compared to other years. Also, it should be noted that Andersen (2009) and Shim & Eom (2009) (282 and 127 citations, respectively) provided the second indicator of average citations per article in 2009 (MeanTCperArt = 77.00). Publications by Awoyemi et al. (2017) and Hajek & Henriques (2017) (344 and 173 citations) provided a MeanTCperArt of 50.9 in 2017 despite the significantly higher number of articles published that year (Figure 8).

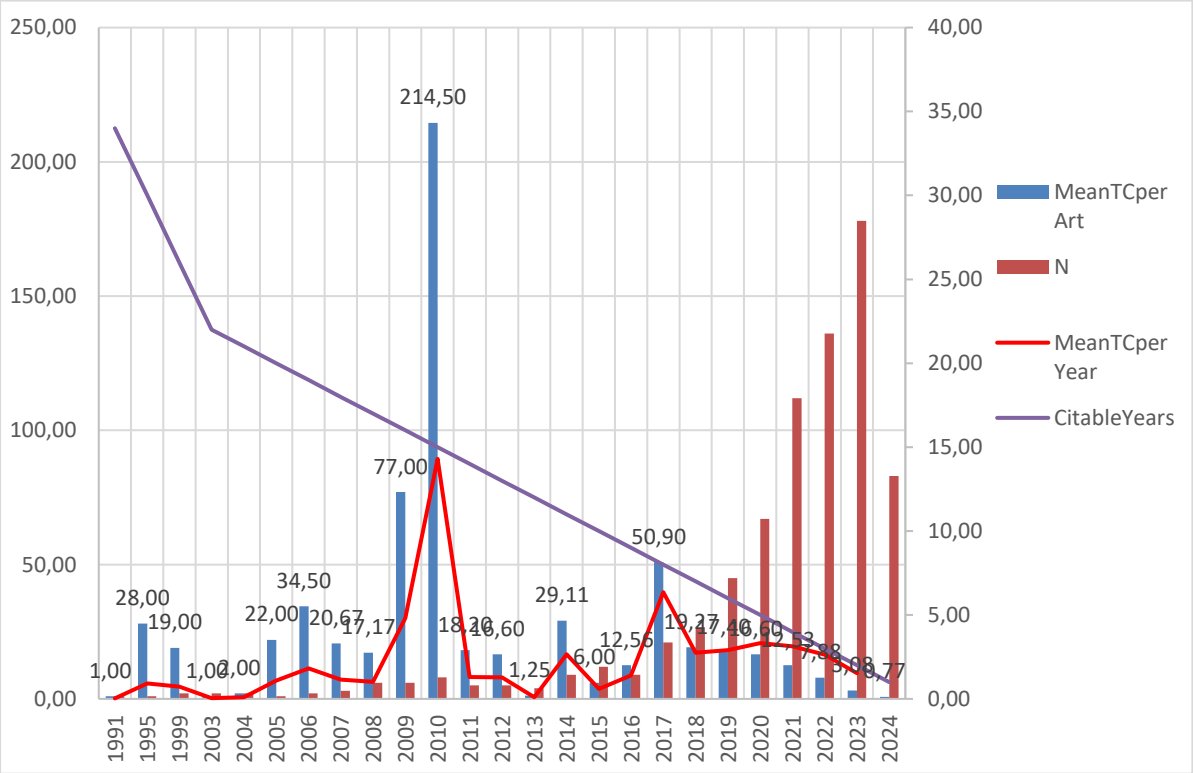


Figure 8. Average Citations Per Year of publications focusing on AI and ML in combating illegal financial operations.

[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Citations in global measure indicate a document's influence across the bibliographic database, often attracting many citations from various research areas. In contrast, local citations count how frequently a paper was cited by other research within a particular investigated set (Biblioshiny Tutorial, n.d.). Tables 7 and 8 list the top 10 most globally and locally cited documents in our sample, respectively, along with their citation characteristics. The article by Bertot et al. (2010) is the most cited paper globally. This paper examined how information and communication technologies (ICTs), including e-government and social media, could be leveraged to promote transparency and combat corruption within societies, how they could facilitate greater openness in government operations, making information more accessible to the public and enabling citizens to hold their governments accountable. The authors highlighted

Tables 7. Most Global Cited Documents [Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Paper	Author (s)	Source	Year	DOI	TC	TC p. Y.	NTC
We are using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies.	Bertot, J. C., Jaeger, P. T., Grimes, J. M.	Government Information Quarterly, 27(3), 264–271.	2010	10.1016/j.giq. 2010.03.001	1591	106,07	7,42
Credit card fraud detection using machine learning techniques: A comparative analysis	Awoyemi J.O., Adetunmbi A.O., Oluwadare S.A.	2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 2017, pp. 1-9	2017	10.1109/ICCNI. 2017.8123782	344	43,00	6,76
E-Government as an anti-corruption strategy.	Andersen, T. B.	Information Economics and Policy, 21(3), 201–210.	2009	10.1016/ j.infoecopol. 2008.11.003	282	17,63	3,66
E-Government, Internet Adoption, and Corruption: An Empirical Investigation	Elbahnasawy, N. G.	World Development, 57, 114–126	2014	10.1016/ j.worlddev. 2013.12.005	221	20,09	7,59
Mining corporate annual reports for intelligent detection of financial statement fraud – A comparative study of machine learning methods	Hajek, P., Henriques, R.	Knowledge-Based Systems, 128, 139–152	2017	10.1016 / j.knosys. 2017.05.001	173	21,63	3,40
Cross-domain analysis of ML and DL: Evaluating their impact in diverse domains.	Khetani V., Gandhi Y., Bhattacharya S., Ajani S.N., Limkar S.	International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.	2023	https://ijisae.org/ index.php/ IJISAE/article/ view/2951	149	74,50	48,31
Detection of illicit accounts over the Ethereum blockchain	Farrugia, S., Ellul, J., Azzopardi, G.	Expert Systems with Applications, 150, 113318.	2020	10.1016/j.eswa. 2020.113318	144	28,80	8,68
Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection	Itoo, F., Meenakshi, Singh, S.	International Journal of Information Technology, **13**, 1503–1511	2020	10.1007/ s41870-020-00430-y	132	33,00	10,54
Using social network analysis to prevent money laundering	Fronzetti Colladon, A., Remondi, E.	Expert Systems with Applications, 67, 49–58.	2017	10.1016/ j.eswa. 2016.09.029	129	16,13	2,53
Anti-corruption effects of information communication and technology (ICT) and social capital	Shim, D. C., Eom, T. H.	International Review of Administrative Sciences, 75(1), 99–116.	2009	10.1177/ 00208523 08099508	127	7,94	1,65

Note: **TC** – total citation**, TC p. Y.** – total citation per year**, NTC** – normalized total citation

Tables 8. Most Local Cited Documents [Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Document	Author (s)	Source	DOI	Year	LC	GC	LC/GC Ratio (%)	NLC	NGC
Detecting money laundering transactions with machine learning	Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., Lorentzen, J.	*Journal of Money Laundering Control*, *23*(1), 173–186.	10.1108/ JMLC-07-2019-0055	2020	28	75	37,33	19,54	4,52
Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies	Bertot, J. C., Jaeger, P. T., Grimes, J. M.	*Government Information Quarterly*, *27*(3), 264–271.	10.1016/ j.giq. 2010.03.001	2010	17	1591	1,07	5,67	7,42
Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective	Canhoto, A. I.	*Journal of Business Research,* 131, 441-452	10.1016/ j.jbusres. 2020.10.012	2021	16	73	21,92	21,08	5,83
Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection	Zhang, Y., Trubey, P.	*Computational Economics*, *54*(3), 1043–1063.	10.1007/ s10614-018-9864-z	2019	16	49	32,65	14,69	2,82
Credit card fraud detection using machine learning techniques: A comparative analysis	Awoyemi J.O., Adetunmbi A.O., Oluwadare S.A.	*2017 International Conference on Computing Networking and Informatics (ICCNI)*, Lagos, Nigeria, 2017, pp. 1-9	10.1109/ ICCNI. 2017.8123782	2017	16	344	4,65	7,30	6,76
Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering	Alkhalili, M., Qutqut, M. H., Almasalha, F.	*IEEE Access*, *9*, 18481–18496.	10.1109/ ACCESS. 2021.3052313	2021	15	35	42,86	19,76	2,79
Mining corporate annual reports for intelligent detection of financial statement fraud – A comparative study of machine learning methods	Hajek, P., Henriques, R.	*Knowledge-Based Systems*, *128*, 139–152.	10.1016/ j.knosys. 2017.05.001	2017	13	173	7,51	5,93	3,40
Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain. In	Alarab I., Prakoonwit S., Ikbal Nacer M.	Proceedings of the 2020 5th International Conference on Machine Learning Technologies (ICMLT '20), 23–27.	10.1145/ 3409073. 3409080	2020	12	65	18,46	8,38	3,92
Comparative Analysis Using Supervised Learning Methods for Anti-Money Laundering in Bitcoin.	Alarab I., Prakoonwit S., Ikbal Nacer M.	Proceedings of the 2020 5th ICMLT '20, 11–17.	10.1145/ 3409073. 3409078	2020	12	46	26,09	8,38	2,77
Performance of machine learning techniques in the detection of financial fraud	Sadgali, I., Sael, N., Benabbou, F.	*Procedia Computer Science*, *148*, 45–54.	10.1016/ j.procs. 2019.01.007	2019	11	77	14,29	10,10	4,43

Note: **Y.** – year of publication, **LC** – local citations**, GC** – global citations**, NLC** – normalised local citations, **NGC** – normalised global citations

the importance of e-government initiatives, which use digital tools to streamline government processes, enhance service delivery, and provide transparent access to government information. Social media platforms were discussed as powerful tools for fostering dialogue between governments and citizens, encouraging public participation, and disseminating information widely and quickly. The authors argued that ICTs could effectively reduce corruption by increasing the visibility of government activities, providing mechanisms for reporting and tracking corruption, and fostering a culture of accountability. The article also addressed the challenges associated with implementing ICT-based transparency initiatives, such as the digital divide, privacy concerns, and the need for effective policies and regulations.

The second in this rank is the paper by Awoyemi et al. (2017), which evaluated the performance of three techniques – naïve Bayes, k-nearest neighbour, and logistic regression – on credit card fraud dataset (284,807 transactions from European cardholders). A mixed approach of under-sampling and over-sampling was applied to the compromised data to address the data imbalance. These techniques were tested on raw and pre-processed data, and the implementation was done in Python. The results indicated optimal accuracy rates of 97.92% for naïve Bayes, 97.69% for k-NN, and 54.86% for logistic regression. Comparative results revealed that the k-nearest neighbour beats both naïve Bayes and logistic regression.

Interestingly, the article by Bertot et al. (2010) ranks second in the ranking of the most locally cited documents. The most locally cited document is the article by Jullum et al. (2020), which explored the application of machine learning techniques to identify money laundering activities. The authors discussed developing and implementing machine learning simulations designed to detect suspicious financial transactions that may indicate money laundering. They analysed the effectiveness of these models using real transaction data, highlighting their potential to improve the detection of illicit financial activities. The study emphasised the importance of advanced data analysis and machine learning in developing the capabilities of financial institutions and regulatory bodies to combat money laundering.

Words that frequently co-occur within a document and form a connection within a network are commonly called a co-words network. Found network construction helps discover the themes within an investigating topic, identifying key and emerging subtopics, referred to as the research border. It also assists in monitoring the progression of issues over time (Biblioshiny Tutorial, n.d.).

According to Table 1, Keywords (Author) have only 12.60 losses and have been acceptable for analysis. The unifying theme of the keywords of the most significant red cluster (including 20 keywords, Figure 9) is the application of advanced computational techniques and algorithms, particularly in artificial intelligence and machine learning, to identify and avoid fraudulent operations across various financial and cybersecurity contexts. These keywords reflect the interdisciplinary approaches to improve the accuracy, efficiency, and transparency of identifying and mitigating fraud in digital and financial environments.

The authors' keywords of the green cluster are dedicated to using artificial intelligence and machine learning to identify, prevent, and manage financial crimes such as money laundering and fraud. These keywords reflect the integration of sophisticated data analysis and algorithmic techniques within the finance and banking sectors to enhance transaction monitoring, ensure regulatory compliance, and combat financial crime (Figure 9). The connecting theme of the keywords of the yellow cluster (blockchain, cryptocurrency, bitcoin, cybercrime, fintech, security, Ethereum – Figure 9) is the intersection of advanced digital financial technologies

and cybersecurity. These terms are all related to the use and impact of blockchain technology and cryptocurrencies in the financial technology (fintech) industry, highlighting concerns about security and the potential for cybercrime within these emerging financial systems. The blue cluster (Figure 9) is connected to applying advanced analytical and computational techniques to detect and avoid fraudulent activities in financial transactions, particularly credit card fraud. These terms emphasise using data mining and computational intelligence methods to improve the accuracy and increase the efficiency of fraud detection systems through effective feature selection and analysis.

The unifying theme of the keywords of the violet cluster is the employment of digital technologies and platforms to promote transparency and combat corruption. These terms highlight how information and communication technologies (ICT) and social media can be leveraged to increase accountability, provide greater access to information, and foster public engagement to reduce corruption. Keywords corruption and technology occupied two separate clusters (purpure and brown).

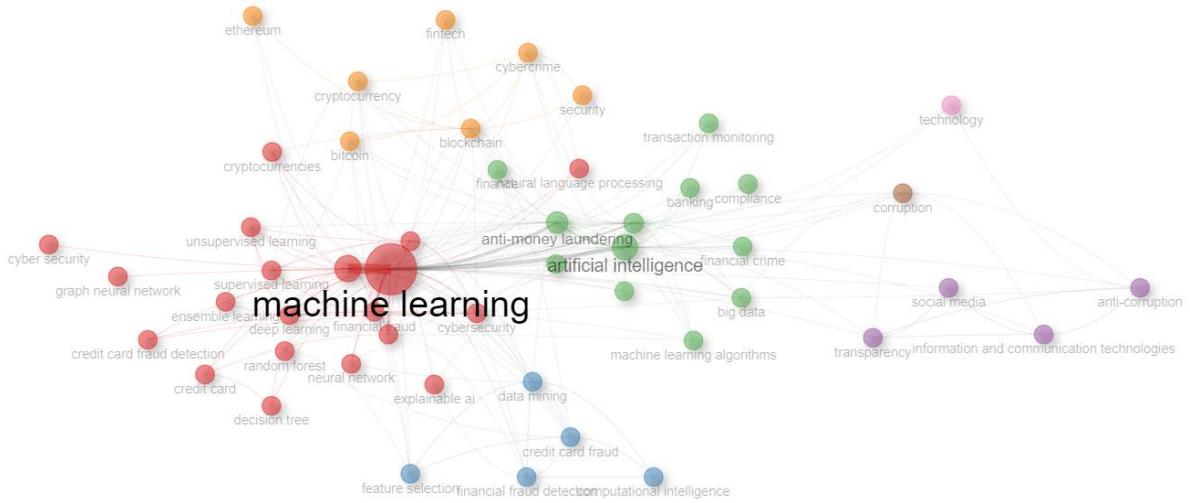


Figure 9. Co-occurrence author's keywords network.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

As for keywords plus, the construction of the co-occurrence network identifies only two clusters:

1. The subtopics of the red cluster collectively emphasise the integration of machine learning and advanced data analysis techniques in combating financial crime and improving the security and integrity of financial systems. They also could be divided into subgroups: (1) the use of machine learning, deep learning, neural networks, support vector machines, decision trees, random forests, and nearest neighbour search in building predictive models for fraud detection; (2) techniques specifically targeting the detection and prevention of financial fraud, including credit card fraud and fraudulent transactions in commerce and investment; (3) employing data mining and feature extraction methods to analyse large datasets for identifying patterns and anomalies indicative of fraud; (4) protecting financial transactions and systems from cybercrime and ensuring network security to prevent unauthorised access and fraud; (5) leveraging ICT to enhance fraud detection systems and

improve decision-making processes related to financial crime prevention; (6) applying machine learning in financial sectors to safeguard investments, forecast risks, and minimise losses due to fraudulent activities; (7) using e-learning platforms and managing large datasets to train and refine fraud detection models and systems.

2. The keywords of the red cluster are centred around the integration of AI, machine learning, blockchain, and big data analytics in enhancing the detection and prevention of money laundering within financial systems. This cluster also includes some subthemes:
    - Utilising AI, supervised learning, anomaly detection, convolutional neural networks, and graph neural networks to develop models for identifying suspicious activities and patterns indicative of money laundering.
    - Employing blockchain technology and cryptocurrencies such as bitcoin to understand and mitigate money laundering risks in decentralised financial systems.
    - Implementing AML measures and practices to prevent and detect money laundering activities within financial institutions.
    - Leveraging big data analytics to process and analyse large financial transaction volumes to identify unusual behaviour and potential laundering activities.
    - Conducting risk assessments and monitoring financial institutions to ensure compliance with AML regulations and effectively manage financial transaction risks.
    - Addressing challenges and developing solutions for detecting laundering activities involving electronic money and digital currencies.

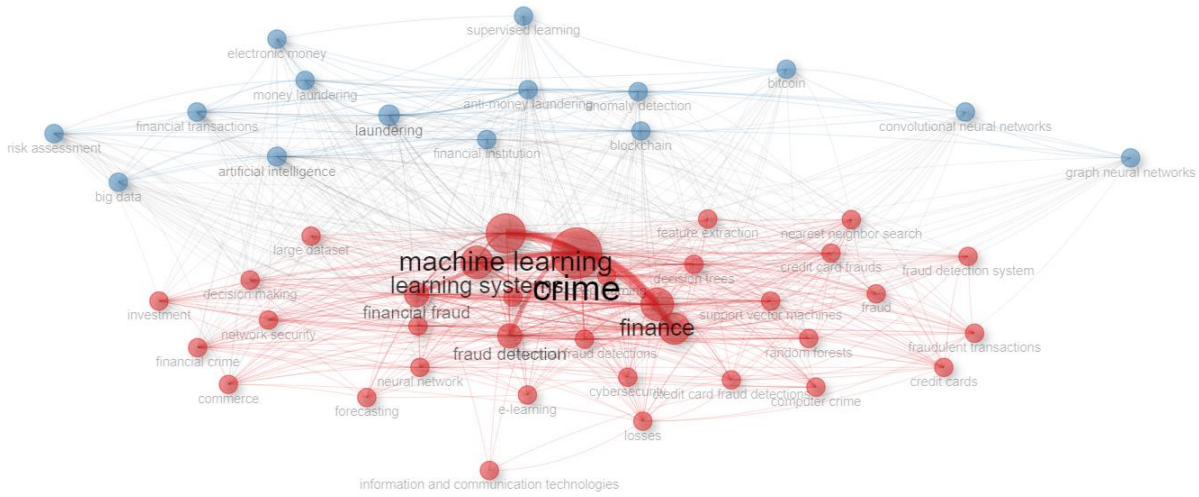


Figure 9. Co-occurrence keywords plus network.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Figure 10 presents the different keywords from the list of Titles and abstracts.

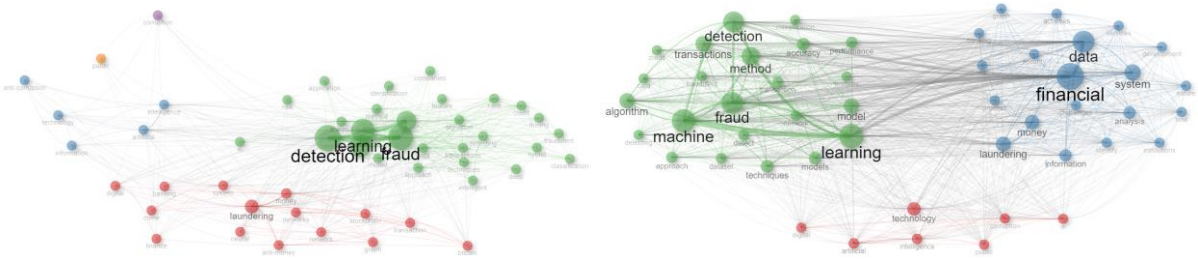


Figure 10. Co-occurrence keywords from the list of Titles and Abstract network.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

Notably, keywords from numerous clusters and investigating sub-themes are intently joined, reflecting a trend toward merging in academic research. The Biblioshiny app helps identify the most relevant and progressed paper types and track their movements over time by assessing their growing relevance and development levels. An alluvial diagram in Figure 12 visualises the evolution of themes in the scholarly literature on AI and ML in combating illegal financial operations. Like a flowchart, this diagram successfully demonstrates the change and revolution of themes within the investigating sample over time (Aria & Cuccurullo, 2017). Longitudinal analyses of documents stress topics' joining, convergence, or deviation over time (Aria & Cuccurullo, 2020).

The moment was chosen by the detected bifurcation points of the trend change in the number of publications presented in Figure 1. These are the years 2003 and 2015. The few publications of the early period of 1991-2003 are mainly devoted to applying artificial intelligence in combating illegal financial operations. Interestingly, they were transformed into the Crime sub-topic in the following period of 2004-2015. From 2004 to 2015, new sub-topics appeared: ICT, decision-making, computer crime, government data processing, and data security (Figure 11).

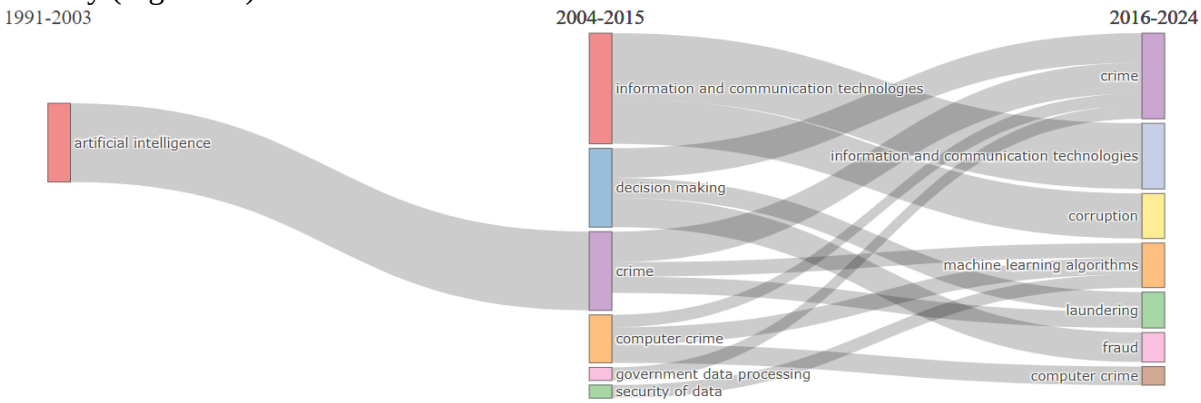
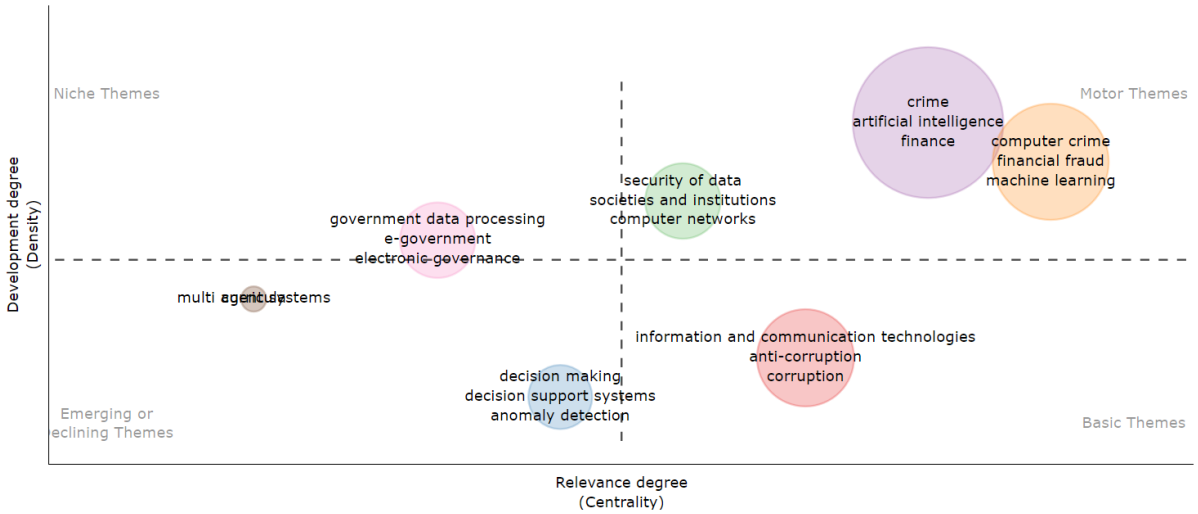


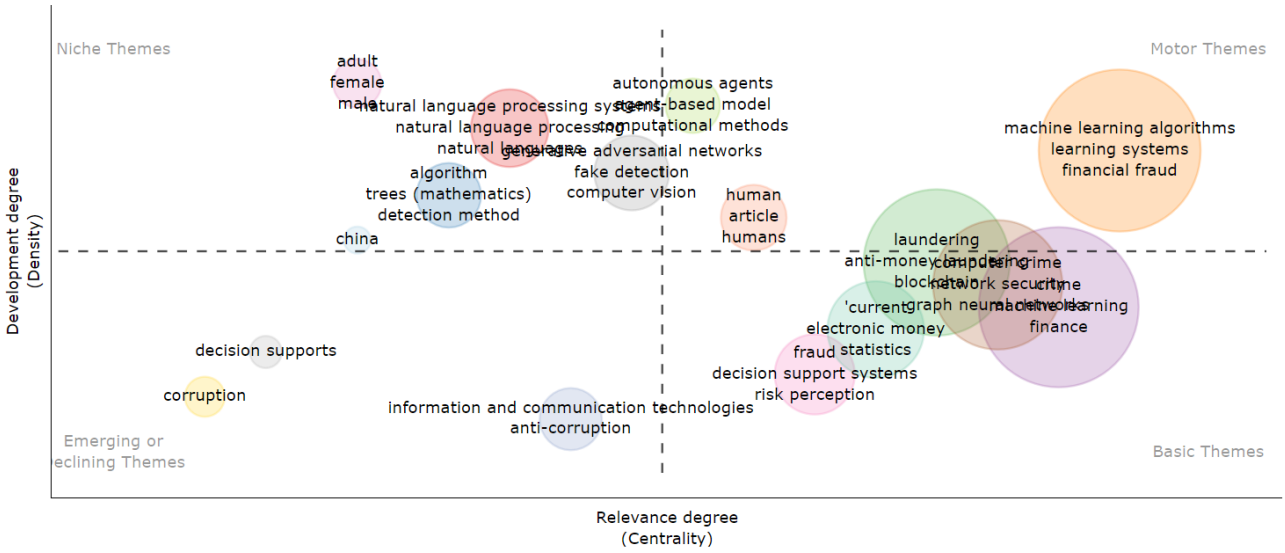
Figure 11. A Longitudinal Thematic Map Analysis in a sample of publications with a focus on AI and ML in combating illegal financial operations
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

However, these subtopics will transform in the next period. A group of studies focused on corruption research stood out from the sub-topic of ICT. Studies with the keywords machine learning algorithms and laundering stood out from the crime subtopic. Subtheme Decision-making was separated into subtopics, such as fraud, and it partially joined the subtopics of laundering and crime. Part of the research in the subtopics of Computer crime also migrated to

the subtopics of Crime and Machine learning algorithms. The last-mentioned sub-topic also included research from 2004-2015 with a sub-topic like the security of data, which means that more and more studies are investigating the use of machine learning in cybersecurity, detecting suspicious operations and criminal crimes, including cybercrime (Figure 11).



a) 2003-2015



b) 2016-2024

Figure 12. Mapping of relevance degree and development degree of subtopic in documents with a focus on AI and ML in combating illegal financial operations

[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

The bibliophile clustering algorithm for the keywords' network enables the identification of different themes within a sample of publications. Each theme or cluster can be depicted on a specific plot called a Thematic map (Cobo et al., 2011). Centrality measures the relevance of a theme, while density measures its level of development. This framework allows us to categorise themes into the following quadrants:

- Highly developed and isolated themes (Niche).

- Emerging or declining themes.
- Motor themes.
- Basic and transversal themes.

In our case, it is interesting to investigate the location of subtopics in the «Degrees of compliance-development» matrix in the time frames of 2003-2015 and 2016-2024. The results are presented in Figure 12. The main topics in 2003-2015 included ICT, anti-corruption, and corruption. Special topics were state data processing, e-government, and e-governance. It should be noted that the ICT, anti-corruption, and corruption sub-topics have moved in 2016-2024 into the quadrant of declining topics. Such subtopics as Machine learning algorithms, Learning systems, and Financial fraud are Motor themes. The location of other subtopics in the «Degrees of compliance-development» matrix is presented in Figure 12 a, b.

The closeness between keywords indicates shared content: keywords are tight to each other because a significant ratio of articles discusses them; they are situated at a distance when only an insignificant segment of articles uses these keywords. The basis of the map characterises the mean location of all column profiles, thus marking the centre of the investigated sample, which indicates common and widely split topics (Cuccurullo et al., 2016). Clusters are identified through hierarchical clustering (Figure 13). Fractals of keywords are grouped around separate subtopics: (1) Machine learning and its application in determining fraudulent transactions; (2) the use of big data and data mining in the determination of financial fraud in the financial and commercial spheres; (3) credit card fraud detection; (4) AI in the detection of financial and computer crimes; (5) use of neural networks and blockchain technologies in the detection of abnormal activity; (6) AML; (7) using nearest neighbour search and random forest methods; and (8) Bitcoin.

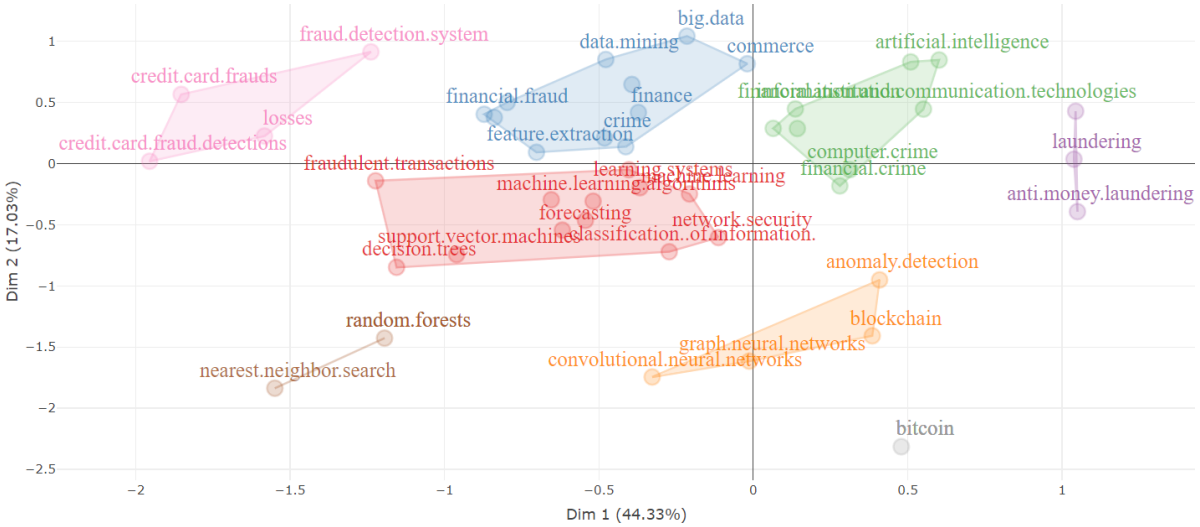


Figure 12. Multiple correspondence analysis.
[Source: developed by the authors (based on the Scopus database using the Biblioshiny App)]

CONCLUSIONS

The relevance of Artificial Intelligence (AI) and Machine Learning (ML) in combating illegal financial activities is increasingly evident in today's financial and technological landscape. Implementing advanced AI and ML systems demonstrates a solid commitment to security and transparency, which can enhance customer confidence and strengthen the institution's reputation. As financial crimes become more sophisticated and regulatory pressures increase, the role of AI and ML in ensuring financial security is more critical than ever. These technologies provide sophisticated, efficient, and practical solutions for detecting and preventing financial crimes, making them indispensable tools for financial institutions worldwide. A comprehensive and inclusive bibliometric analysis can shed light on the state of the art and possible future vectors of AI and ML applications in this field, equipping researchers and practitioners to report the complex challenges financial crimes pose in a rapidly evolving digital environment.

The analysis covers publications from 1991 to the first half of 2024, involving 2103 unique authors, including 85 who authored single-author documents. The average number of co-authors per document is 3.31, and 49.06% are conference papers. There has been a steady growth in publications, with an annual growth rate of 14.33%. Notably, a significant number of these publications are recent, with an average document age of 3.51 years.

From 1991 to 2002, publications on AI and ML in combating illegal financial operations appeared sporadically, marking the initial interest in the field. The period from 2003 to 2015 saw a rise in publication activity, with a trend resembling exponential growth. The period from 2015 to 2024 experienced rapid growth, explained by a polynomial trend of the second degree. These findings affirm the growing research interest in this area, especially from 2003 onwards.

The most cited publication in this domain is by Randhawa et al. (2018), which explores the use of machine learning algorithms for credit card fraud detection. Jingyu Li, a researcher from the Beijing Institute of Technology, emerged as the most productive author, contributing significantly to the literature. According to Lotka's law, as the number of publications rises, the frequency of authors contributing to many documents decreases, with only one author (Li J.) publishing ten articles. In contrast, most authors have published only one article.

International collaboration is evident, with 18.23% of publications involving co-authorship across countries. This shows strong international cooperation in the research field, with Canada, Bangladesh, and Brazil primarily publishing single-country papers. The United Arab Emirates exhibits the highest MCP ratio. China leads in the number of publications, followed by India, the USA, the United Kingdom, and Italy, collectively accounting for 32.7% of the publications.

According to Bradford's law, journals are divided into three categories: core journals (35 items), significant contributors (196 items), and less influential journals (246 items). Key sources, such as Lecture Notes in Computer Science, began publishing relevant articles in the 1990s, with a noticeable increase in publications from the 2020s.

Citation rates are generally low, with a notable spike in 2010 due to the highly cited work by Bertot et al. (2010). The primary cluster of keywords focuses on using advanced computational techniques, particularly AI and ML, to detect and prevent fraud in various financial and cybersecurity contexts.

The analysis segmented the timeline into distinct periods based on publication trends: 1991-2003 (early AI applications in combating illegal financial operations), 2004-2015 (emergence of new subtopics like ICT, decision-making, computer crime, government data processing, and data security), and 2016-2024 (expansion into big data, neural networks, blockchain technologies, and AML). Key subtopics include machine learning for fraud detection, big data and data mining for financial fraud, credit card fraud detection, AI in financial and computer crime detection, and neural networks and blockchain technologies.

While this study offers valuable scholarly insights, it has several limitations. Relying solely on the Scopus database may have led to the exclusion of other relevant studies. Additionally, the review was limited to journal articles, books, chapters, and conference papers, leaving out other potential sources of knowledge. Furthermore, the findings were based on the authors' specific set of keywords, highlighting the need for validation through empirical methods like expert interviews and surveys.

IMPLICATIONS FOR RESEARCH, APPLICATION, OR POLICY

Integrating artificial intelligence (AI) and machine learning (ML) in combating illegal financial activities offers significant advancements in detection and prevention, which are essential for both research and policy development. Research implications include the need for further exploration of ethical concerns, privacy, and bias in AI/ML applications and the development of more sophisticated algorithms. Application-wise, financial institutions should adopt AI/ML technologies to enhance compliance with anti-money laundering regulations and reduce operational costs through automated fraud detection. Policymakers must address the regulatory challenges posed by the cross-border nature of financial crimes and promote international collaboration to utilise AI/ML tools effectively.

REFERENCES

Abid, U., Faisal, M., Al-Esmael B., *Farooq Z.H*. (2024). Exploring the moderating role of technological competence and artificial intelligence in green HRM. *Polish Journal of Management Studies,* 29(2), 7-22. https://doi.org/10.17512/pjms.2024.29.2.01.

Acar, A. Z., & Kara, K. (2023). Identifying the effects of corruption perception on the relationship between international trade and logistics performance in developing countries. *Business, Management and Economics Engineering*, *21*(1), 63–83. https://doi.org/10.3846/bmee.2023.18676

Andersen, T. B. (2009). E-Government as an anti-corruption strategy. *Information Economics and Policy*, *21*(3), 201–210. https://doi.org/10.1016/j.infoecopol.2008.11.003

Androniceanu, A. (2023). The new trends of digital transformation and artificial intelligence in public administration. *Administratie si Management Public*, 40, 147- 155. DOI: https://doi.org/10.24818/amp/2023.40-09

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959-975. https://doi.org/10.1016/j.joi.2017.08.007

Aria, M., & Cuccurullo, C. (2020). *Biblioshiny: Bibliometrix for No Coders*. https://bibliometrix.org/biblioshiny/biblioshiny1.html

Asare, K., Samusevych, Y. (2023). Exploring Financial Fraud, Tax Tools, and Economic Security Research: Comprehensive Bibliometric Analysis. *Financial Markets, Institutions and Risks, 7*(3), 136-146. https://doi.org/10.61093/fmir.7(3).136-146.2023

Awe, O. O., & Dias, R. (2022). Comparative Analysis of ARIMA and Artificial Neural Network Techniques for Forecasting Non-Stationary Agricultural Output Time Series. *Agris on-line Papers in Economics and Informatics*, *14*(4), 3–9. https://doi.org/10.7160/aol.2022.140401

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis. *2017 International Conference on Computing Networking and Informatics (ICCNI)*. https://doi.org/10.1109/iccni.2017.8123782

Ballester, E., Rubio, N., & Ruiz, C. (2023). Emojis and Users' Brand Engagement in Instagram. The Case of Eco-Friendly Restaurants. *Journal of Tourism and Services*, *14*(27), 64–88. https://doi.org/10.29036/jots.v14i27.514

Barbu, L., Horobeț, A., Belaşcu, L., & Ilie, A. G. (2024). Approaches to tax evasion: a bibliometric and mapping analysis of Web of Science indexed studies. *Journal of Business Economics and Management*, *25*(1), 1–20. https://doi.org/10.3846/jbem.2024.20691

Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. https://doi.org/10.1109/cvcbt.2018.00014

Bartulovic, M., Aljinovic, N., Piplica, D. (2023), Determining the Relationship Between Corruption and Money Laundering, *Montenegrin Journal of Economics*, 19(2), 109-118. 10.14254/1800-5845/2023.19-2.9

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, *27*(3), 264–271. https://doi.org/10.1016/j.giq.2010.03.001

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

Biblioshiny Tutorial. (n.d.) Tutorial. Available at https://bibliometrix.org/biblioshiny/biblioshiny2.html

Bilan, S., Šuleř, P., Skrynnyk, O., Krajňáková, E., & Vasilyeva, T. (2022). Systematic bibliometric review of artificial intelligence technology in organizational management, development, change and culture. *Business: Theory and Practice*, *23*(1), 1–13. https://doi.org/10.3846/btp.2022.13204

Botoc F.C., Khaled M.D., Milos L.R., Bilti R.S. *(2024).* The role of big data in the fintech industry: a bibliometric analysis. *Transformations in Business & Economics*. 22(3A), 60A, 853-868. http://www.transformations.knf.vu.lt/60a

Bozhenko, V. Buriak, A., Bozhenko, A. & Roienko, O. (2023a). Transparency and Corruption Prevention in Financing Climate Action. *Financial Markets, Institutions and Risks, 7*(2), 88-94. https://doi.org/10.21272/fmir.7(2).88-94.2023

Bozhenko, A., Krawczyk, D., Hałuszko, K. & Ozarenko, V. (2023b). Data-Mining Modeling of Corruption Perception Patterns Based on Association Rules. *Business Ethics and Leadership, 7*(4), 181-189. https://doi.org/10.61093/bel.7(4).181-189.2023

Čejka, M., Masner, J., Jarolímek, J., Benda, P., Prokop, M., Šimek, P., & Šimek, P. (2023). UX and Machine Learning – Preprocessing of Audiovisual Data Using Computer Vision to Recognize UI Elements. *Agris on-line Papers in Economics and Informatics*, *15*(3), 35–44. https://doi.org/10.7160/aol.2023.150304

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, *57*(2), 245–285. https://doi.org/10.1007/s10115-017-1144-z

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of aresearch field: A practical application to the fuzzy sets theory field. *Journal of Informetrics*, 5(1), 146-166. https://doi.org/10.1016/j.joi.2010.10.002

Dabija, D. C., & Vătămănescu , E.-M. (2023). Artificial intelligence: The future is already here. *Oeconomia Copernicana*, *14*(4), 1053–1056. https://doi.org/10.24136/oc.2023.031

Deloitte, United Overseas Bank (UOB) (2020). Advanced analytics and innovation in Financial Crime Compliance: The future is now. White paper. Available at https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sg-fas-advanced-analytics-innovation-in-financial-crime-compliance.pdf

Djouadi, I., Zakane, A., & Abdellaoui, O. (2024). Corruption and Economic Growth Nexus: Empirical Evidence From Dynamic Threshold Panel Data. *Business Ethics and Leadership, 8*(2), 49-62. https://doi.org/10.61093/bel.8(2).49-62.2024

Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024). Health Security and Cybersecurity: Analysis of Interdependencies. *Health Economics and Management Review, 5*(2), 84-103. https://doi.org/10.61093/hem.2024.2-06

Dobrovolska, O., Marhasova, V., Momot, O., Borysova, L., Kozii, N., & Chyzhyshyn, O. (2021). Evolution and Current State of Money Circulation in Ukraine and the World. *Studies of Applied Economics, 39*(5). https://doi.org/10.25115/eea.v39i5.5042

Doppalapudi PK, Kumar P., Murphy A., Werner S., Zhang S., Rougeaux C., StearnsR. (2022). The fight against money laundering: Machine learning is a game changer. McKinsey & Company. Available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer#/

Drăcea, R. M., Pirtea, M. G., Cristea, M., Noja, G. G., & Ciobanu, L. (2024). Budget Transparency and Good Governance for Human Development and Citizens' Well-Being. New Empirical Evidence from the European Union. *Engineering Economics*, *35*(3), 328–347. https://doi.org/10.5755/j01.ee.35.3.34024

Druva Kumar K. S., Senthil Kumar J. P. (2024). Efficiency assessment and trends in the insurance industry: A bibliometric analysis of DEA application. *Insurance Markets and Companies*, *15*(1), 83-98. doi:10.21511/ins.15(1).2024.07

Durica, M., Frnda, J., & Svabova, L. (2023). Artificial neural network and decision tree-based modelling of non-prosperity of companies. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *18*(4), 1105–1131. https://doi.org/10.24136/eq.2023.035

European Union Agency for Law Enforcement Cooperation (Europol) (2019) Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement. https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

Financial Action Task Force web site (FATF). (n.d.) https://www.fatf-gafi.org/

FOCAL (2023). Fraud Detection with Machine Learning & Artificial Intelligence in 2024. Available at https://www.getfocal.ai/blog/fraud-detection-with-machine-learning

Fülöp, M. T., Topor, D. I., Ionescu, C. A., Cifuentes-Faura, J., & Măgdaș, N. (2023). Ethical concerns associated with artificial intelligence in the accounting profession: a curse or a blessing? Journal of Business Economics and Management, 24(2), 387–404. https://doi.org/10.3846/jbem.2023.19251

Gasimov, I., Jabiyev, F., & Asgarzade, G. (2023). Institutional quality and economic growth in the non-EU post-Soviet countries: Does energy abundance matter?. *Economics and Sociology*, 16(2), 139-147. doi:10.14254/2071- 789X.2023/16-2/9

Goldberg H. G., Senator T.E. (1995). Restructuring Databases for Knowledge Discovery by Consolidation and Link Formation. *KDD 1995 - Proceedings of the 1st International Conference on Knowledge Discovery and Data Mining* Pages 136 – 141.Code 192333. https://cdn.aaai.org/Symposia/Fall/1998/FS-98-01/FS98-01-008.pdf

Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud – A comparative study of machine learning methods. *Knowledge-Based Systems*, *128*, 139–152. https://doi.org/10.1016/j.knosys.2017.05.001

Höller, S., Dilger, T., Spiess, T., Ploder, C., & Bernsteiner, R. (2023). Awareness of Unethical Artificial Intelligence and its Mitigation Measures. *European Journal of Interdisciplinary Studies*, *15*(2), 67–89. https://doi.org/10.24818/ejis.2023.17

Holtfort, T., Horsch, A. (2024). Quantum Economics: A Systematic Literature Review. *SocioEconomic Challenges*, *8*(1), 62-77. https://doi.org/10.61093/sec.8(1).62-77.2024

Jensen, D. (1997) Prospective Assessment of AI Technologies for Fraud Detection: A Case Study. AAAI Workshop on AI Approaches to Fraud Detection and Risk Management, 34-38. https://cdn.aaai.org/Workshops/1997/WS-97-07/WS97-07-007.pdf

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173–186. https://doi.org/10.1108/jmlc-07-2019-0055

Kaya, H.D. (2023). The global crisis, government contracts, licensing and corruption. *SocioEconomic Challenges, 7*(4), 1-7. https://doi.org/10.61093/sec.7(4).1-7.2023

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data Mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995–1003. https://doi.org/10.1016/j.eswa.2006.02.016

Kovbasyuk, L., Vakulenko, Y., Ivanets, I., Bozhenko, V., & Kharchenko, D. (2024). Forecast of Corruption: From Ethical to Pragmatic Considerations. *Business Ethics and Leadership, 8*(2), 184-199. https://doi.org/10.61093/bel.8(2).184-199.2024

Kozhushko, I. (2023). Transformation of Financial Services Industry in Conditions of Digitalization of Economy. *Financial Markets, Institutions and Risks, 7*(4), 189-200. https://doi.org/10.61093/fmir.7(4).189-200.2023

Kuanaliyev, A., Taubayev, A., Kunyazov, Y., Ernazarov, T., Mussipova, L., Saduakassova, A. (2024), Digital and Economic Transformation in the Public Administration System, *Montenegrin Journal of Economics*, 20(3), 63-78. 10.14254/1800-5845/2024.20-3.5

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, 17(2), 220- 239. doi:10.14254/2071-8330.2024/17-2/12

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4), 195. https://doi.org/10.3390/joitmc8040195

Lăzăroiu, G., Bogdan, M., Geamănu, M., Hurloiu, L., Luminița, L., & Ștefănescu, R. (2023). Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management. *Oeconomia Copernicana*, *14*(3), 707–730. https://doi.org/10.24136/oc.2023.021

Lei Y., Haiping X., Boyan S. (2024). Digital currency electronic payment in china: economic characteristics, regulatory dilemma and legislative governance path. *Transformations in Business & Economics*, 23(1), (61), 86-105. http://www.transformations.knf.vu.lt/61/article/digi

Maile, K.V., & Vyas-Doorgapersad, S. (2023). Misconduct Impeding Good Governance in The South African Public Service. *Business Ethics and Leadership, 7*(2), 9-17. https://doi.org/10.21272/bel.7(2).9-17.2023

Nakamoto S. (2008). Bitcoin: a Peer-To-Peer Electronic Cash System. Available at https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

Oe, H., Yamaoka, Y. (2023). The impact of the digital environment on eco-friendly behavioural change towards nature: Exploring the concept of forest bathing without forest. *SocioEconomic Challenges, 7*(3), 76-93. https://doi.org/10.61093/sec.7(3).76-93.2023

Orlandić, M., Đukić, T., and Mladenović, M. (2024). Upcoming digital transformation and artificial intelligence trends in the public sector. *Administratie si Management Public*, 42, 45-59. https://doi.org/10.24818/amp/2024.42-03

Piotrowski, D., & Orzeszko, W. (2023). Artificial intelligence and customers' intention to use robo-advisory in banking services. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, 18(4), 967–1007. https://doi.org/10.24136/eq.2023.031

Polishchuk Y., Ivashchenko A., Dyba O. (2019). SMART-Contracts via Blockchain as the Innovation Tool for SMEs Development. *Ikonomicheski Izsledvania*, 28 (6), 39-53.

Pouabe, P., Pretorius, J., Pretorius L., et al. (2023). Decision-making based on machine learning techniques: a case study. *Polish Journal of Management Studies*, 28(1), 240-262. https://doi.org/10.17512/pjms.2023.28.1.14.

Pranckutė R. (2021). Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. *Publications*. 9(1):12. https://doi.org/10.3390/publications9010012

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access*, *6*, 14277–14284. https://doi.org/10.1109/access.2018.2806420

Roba, M., & Moulay, O. K. (2024). Risk Management in Using Artificial Neural Networks. *SocioEconomic Challenges*, *8*(2), 302-313. https://doi.org/10.61093/sec.8(2).302-313.2024

Sahnouni, M., & Benghebrid, R. (2023). Competency Assessment Based on Fuzzy Logic and Artificial Intelligence Mechanism: A Study of Competency Assessment Document for the Algerian SEROR Company. *Business Ethics and Leadership, 7*(4), 159-170. https://doi.org/10.61093/bel.7(4).159-170.2023

Sheliemina, N. (2024). The Use of Artificial Intelligence in Medical Diagnostics: Opportunities, Prospects and Risks. *Health Economics and Management Review*, *5*(2), 104-124. https://doi.org/10.61093/hem.2024.2-07

Sherizen, S. (1991). European unification '92 impacts on information security. *Computers & Security*, *10*(7), 601–610. https://doi.org/10.1016/0167-4048(91)90117-v

Shim, D. C., & Eom, T. H. (2009). Anticorruption effects of information communication and technology (ICT) and social capital. *International Review of Administrative Sciences*, *75*(1), 99-116. https://doi.org/10.1177/0020852308099508

Skrynnyk, O., & Lyeonov, S. (2023). Emerging trends and research focal points of information technologies for financial control and accounting at the state and corporate level: Bibliometric research and visualization. *Accounting and Financial Control*, *4*(1), 49–62. https://doi.org/10.21511/afc.04(1).2023.05

Staiger A. (2023). AI's Double-Edged Sword: How Fraudsters are Weaponizing Intelligence. Association of Certified Fraud Examiners Insights Blog. Available at https://www.acfe.com/acfe-insights-blog/blog-detail?s=how-fraudsters-are-weaponizing-artificial-intelligence

United Nations Office on Drugs and Crime (UNODC) (n.d.) Money Laundering. Available at https://www.unodc.org/unodc/en/money-laundering/overview.html

Urbonavičius, S., & Degutis, M. (2023). Technology-Driven Economic Behaviours: The Role of Willingness to Disclose Personal Data in Online Buying and Webrooming. *Engineering Economics*, *34*(5), 568–578. https://doi.org/10.5755/j01.ee.34.5.34782

U.S. Congress, Office of Technology Assessment, (OTA) (1995) Information Technologies for Control of Money Laundering, OTA-ITC-630 (Washington, DC: U.S. Government Printing Office, September 1995). https://ota.fas.org/reports/9529.pdf

Utkina, M. (2023). Leveraging Blockchain Technology for Enhancing Financial Monitoring: Main Challenges and Opportunities. *European Journal of Interdisciplinary Studies*, *15*(2), 134–151. https://doi.org/10.24818/ejis.2023.21

Vasilyeva, T., Ziółko, A., Kuzmenko, O., Kapinos, A., & Humenna, Y. (2021). Impact of digitalization and the COVID-19 pandemic on the AML scenario: Data mining analysis for good governance. *Economics and Sociology*, *14*(4), 326–354. https://doi.org/10.14254/2071-789x.2021/14-4/19

Waldman, D. (2024). Replace government healthcare with patient-controlled health care. *Health Economics and Management Review*, *5*(1), 80-89. https://doi.org/10.61093/hem.2024.1-06

Yarovenko, H., Lopatka, A., Vasilyeva, T., & Vida, I. (2023a). Socio-economic profiles of countries - cybercrime victims. *Economics and Sociology*, 16(2), 167-194. doi:10.14254/2071-789X.2023/16-2/11

Yarovenko, H., Kuzior, A. & Raputa, A. (2023b). The Modeling of the Probable Behaviour of Insider Cyber Fraudsters in Banks. *Financial Markets, Institutions and Risks, 7*(4), 155-167. https://doi.org/10.61093/fmir.7(4).155-167.2023

Yarovenko, H., Vasilyeva, T., Ustinovichius, L., & Remsei, S. (2024). Illicit practices: Experience of developed countries. Journal of International Studies, 17(2), 146-177. doi:10.14254/2071-8330.2024/17-2/8

Zhang, Y., & Trubey, P. (2018). Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *Computational Economics, 54*(3), 1043–1063. https://doi.org/10.1007/s10614-018-9864-z

Zámek, D., Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. *Financial Markets, Institutions and Risks, 8*(1), 173-188. https://doi.org/10.61093/fmir.8(1).173-188.2024

Authors' Note

This article was supported by the Ministry of Education and Science of Ukraine (project No. 0123U101945 - National security of Ukraine through prevention of financial fraud and money laundering: war and post-war challenges) and APVV agency (APVV-16-0602 Enhancement of the relevance of the accounting data in the SR – from expenses to value). This paper supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by the University of Debrecen Program for Scientific Publication.

All correspondence should be addressed to
Lyeonov Serhiy
Silesian University of Technology, Poland
Sumy State University, Ukraine
Akademicka, 2A, 44-100, Gliwice, Poland
Serhiy.Lyeonov@polsl.pl

Human Technology
ISSN 1795-6889
https://ht.csr-pub.eu