Artificial Intelligence applied to the prevention and detection of banking fraud: from bibliometric analysis to investigation*

Fèmi José DJAMBOUTOU[1,*,†] and Pélagie HOUNGUE[2,†]

[1] *Ecole Doctorale des Sciences de l'Ingénieur, Université d'Abomey-Calavi, Abomey-Calavi, Benin*
[2] *Institut de Mathématiques et de Sciences Physiques (IMSP), Dangbo, Benin*

Abstract

Banking transaction security is a major challenge for financial world. Traditional solutions that combat banking fraud rely on physical and IT security measures, as well as identity verification and transaction monitoring procedures. These traditional methods have shown their limitations beside technological advancements and the emergence of more sophisticated attack techniques. The obsolescence of traditional anti-fraud techniques has led to the development of new approaches based on Artificial Intelligence (AI). The application of AI to fraud detection is nowadays a revolution in the banking sector. Despite this, there is no recent and comprehensive bibliometric analysis study to assess and map scientific production in this field of research. The objective of this paper is to establish a quantitative assessment of scientific production in order to facilitate the search for relevant bibliographic references. To achieve this, the Web of Science (WoS) and Scopus databases were used due to their completeness and high impact factor. A query based on the search string: (Bank fraud AND artificial intelligence) or (Bank fraud AND Deep learning) or (Bank fraud AND machine learning) allowed the extraction of 102 documents from Scopus and 135 documents from WoS. The PRISMA method was used to select the documents of interest for the study.

The study showed that scientific production in this field experienced significant growth since 2018. China, India, and the United States clearly dominate scientific production, leaving African countries behind. Finally, our investigation shows that supervised learning, unsupervised learning, and reinforcement learning are the AI technologies traditionally deployed in the fight against banking fraud.

Keywords

Bank fraud, artificial intelligence, deep learning, machine learning

1. Introduction

The United Nations Office on Drugs and Crime (UNODC) estimates that $2 trillion of criminal money passes through the banking system each year [1]. The majority of crimes are committed through failures in computer systems [2,3]. Indeed, as these technologies are developed and made available to banking institutions, the means to circumvent them are built in parallel. Thus, the banking sector is constantly plagued by cybercrime offenses. The scientific community has not remained insensitive to this growing threat, which increasingly weighs on the profitability of banking institutions. Several researchers or groups of researchers have set themselves the objective of waging a rearguard action against this scourge, which is increasingly giving sleepless nights to the world of finance in general and the banking sector in particular. This is when different technologies, including AI, are being used to counter this rapidly growing scourge. Researchers are engaging in this new trend and are directing research themes towards the application of AI to banking fraud [4]. However, it is difficult to assess the effectiveness of existing approaches, identify emerging approaches and understand the issues and challenges associated with the implementation

* *CITA 2025: International Conference of Information and Communication Technologies of the National Academy of Sciences, Arts and Letters of Benin, 26-28 June 2025, Cotonou, Benin*
[1,*] Corresponding author.
[†] These authors contributed equally.
djamboutoujose@gmail.com (F. J. DJAMBOUTOU); pelagie.houngue@imsp-uac.org (P. HOUNGUE)
0009-0003-4315-3576 (F. J. DJAMBOUTOU); 0000-0001-8138-2079 (P. HOUNGUE)

of the technology. A bibliometric analysis would help maping recent research and highlight the gaps in the scientific literature in the field. In this perspective, this paper attempts to answer the following research questions:

- What is the volume of scientific publications in the field of AI applied to banking fraud between 2015 and 2025?
- How does scientific production evolve over time?
- What are the most important scientific journals?
- Who are the most productive authors in this field of research?
- What is the state of construction of collaboration networks between researchers?
- What are the most influential contributions in this field?
- What is the geographical distribution of the authors and research institutions involved?
- What AI technologies are commonly deployed in the fight against banking fraud?
- What is the state of scientific production in African context?

These are all questions whose answers will provide a clear idea of the evolution of scientific activity and AI technologies that underpin our field of research. The present contribution therefore aims to conduct a bibliometric analysis study highlighting scientific productivity, the main research actors in this field, the main sources as well as other important factors such as geographical distribution and collaborative links between researchers or research institutions on this subject. To carry out the study, an inventory was made through the literature review section. Then the research methodology was clearly explained, highlighting the means and strategies implemented to obtain the results. The results of the research are presented and then discussed. In addition, the limitations of the bibliometric analysis are described in section 5. Finally, the conclusion and perspectives close the study.

2. State of the art

This research work has antecedents that are important to know in order to situate itself in the scientific literature. Although there is no study identical to the one discussed here, efforts at bibliometric analysis have been made by some authors. This is the case of Oke et al. who worked on the role of AI in financial services. The data were collected from the Web of Science publication database and analyzed with CiteSpace and VOSViewer software. Their study takes into account documents published between 1989 and 2023 [4]. The results show a growing interest among scientists in the application of AI to financial services [5]. However, the study only partially addresses the application of AI to the detection of banking fraud. In addition, their work is limited to articles published up to 2023. The study is no longer relevant because a bibliometric analysis study constantly needs updating. Furthermore, it would have been more interesting to use several complementary databases to conduct the study.

Similarly, Jawad Isbai et al. conducted a bibliometric analysis study in 2024, highlighting the evolution of scientific production in the field of digital transformation in the banking sector [6]. Scopus and Web of Science served as sources of information. The documents considered for the study were published in the period from 2015 to 2024. This is, of course, a recent bibliometric analysis study relating to the banking sector. However, it does not address the security aspect of banking data or the applications of AI. In addition, the article was written as part of economic research, unlike our research framework, which is purely computer science.

Finally, Jean-Pierre Manuana-nseka published a document on the theme "from bibliometrics to cybermetrics" in 2010 [7]. In this work, the author made significant contributions to the quantitative evaluation of a website based on its metadata. Once again, the study does not concern artificial intelligence, nor the security field, much less the banking sector. Even if this study had the same research objectives as ours, it would no longer be relevant.

In short, in a logic of consolidating existing knowledge, the authors have highlighted emerging trends and proposed research opportunities [8]. However, it is clear that the previous work found has not specifically focused on the application of AI to the detection of banking fraud. The gap is obvious and it is important to fill it by providing a complete and recent bibliometric analysis study. Indeed, our research topic fundamentally deals with the use of AI to solve banking fraud problems. In order to achieve this ultimate objective, a rigorous and reproducible research methodology was implemented.

3. Research methodology

The methodology implemented in this study includes three major stages: the choice of information sources, the analysis of extracted documents and the generation of graphics.

3.1. Choosing databases

The aim of this article is to measure the level of development of scientific activity in the field of AI applied to banking fraud [6]. To achieve this, the WoS, Scopus and Google Scolar databases were targeted to serve as sources of information. The final choice is made on the Scopus and WoS platforms due to their high impact factor and completeness. Scopus is a multidisciplinary database of bibliographic references. It covers more than 49 million records including commercial publications, open-access journals and a series of books [9]. Scopus is the current most comprehensive panel of scientific publication in the world. In fact, WoS and Scopus are two complementary publication databases. Only 2/3 of their contents are common and 1/3 of the documents are found in only one of the two databases [9] as shown in Figure 1. Exploiting the complementary strength of Scopus and WoS gives a certain robustness to the research methodology and guarantees the exhaustiveness of the results.

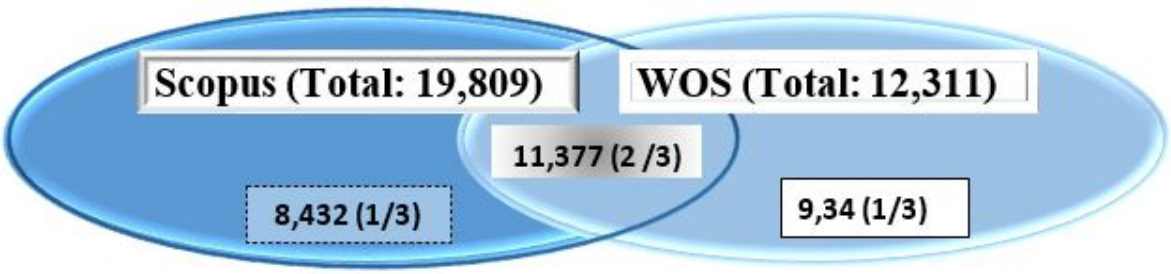

Figure 1: Illustration of the complementarity between Scopus and WoS

3.2. PRISMA method for document analysis

The search string "(Bank fraud AND artificial intelligence) or (Bank fraud AND Deep learning) or (Bank fraud AND machine learning)" was defined and then submitted to the search bar of each of the Scopus and WoS platforms, on May 1, 2025. The collected documents were published in the period 2015-2025. The PRISMA 2020 (Preferred Reporting Item for Systematic Review and Meta-Analysis) method was used to select the documents included in this analysis as shown in Figure 2. A total of 102 and 135 articles under Scopus and WoS respectively were selected to conduct the study.

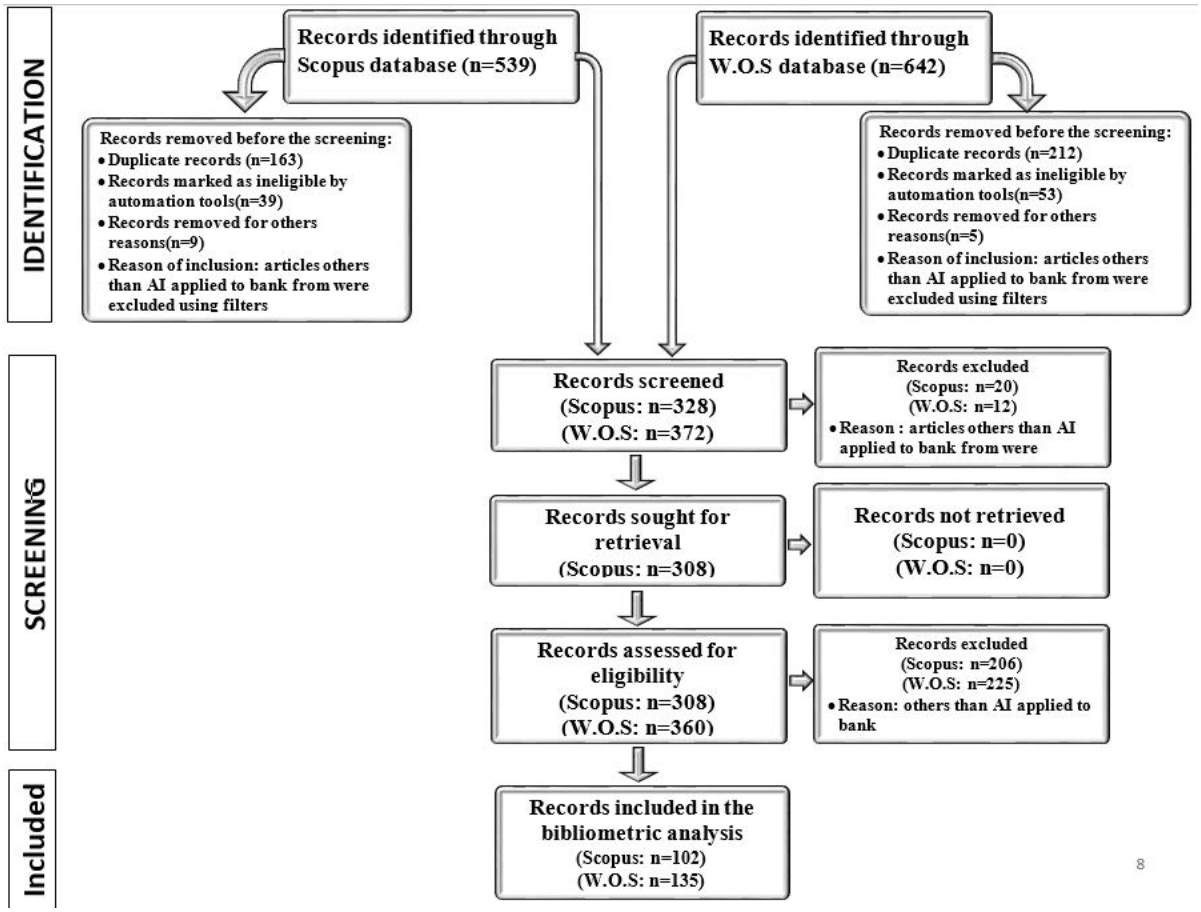

Figure 2: Illustration of the complementarity between Scopus and WoS

3.3. Chart Generation Tools

VOSViewer, Excel and Bibliometrix tools were used to generate graphs.

4. Results of the bibliometric study

The purpose of this section is to present the results of the bibliometric analysis. This will involve developing graphs from statistical data collected on the Scopus and WoS platforms. Comments and analyses of the graphs will follow in order to identify information that can facilitate the search for relevant bibliographic references and identify the dominant schools of thought in the field of AI applied to banking fraud. A survey is then conducted to identify common AI technologies applied to banking fraud.

4.1. Variation in annual scientific production

This subsection aims to assess the level of interest of the scientific community in this specific research area. This will allow researchers and sponsors to understand trends in the sector and guide research themes accordingly. Figure 3 shows the evolution of annual scientific production in the field of AI applied to banking fraud. The data used to develop the graphs come from the Scopus and WoS publication databases.

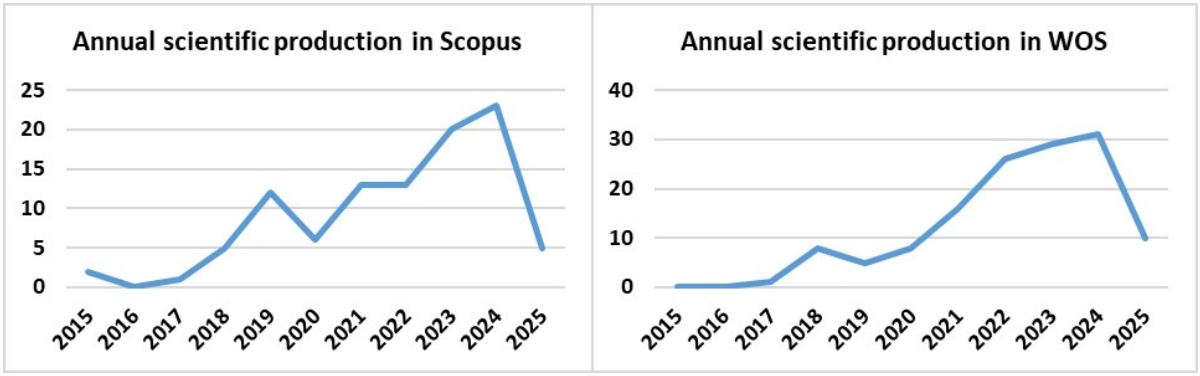

Figure 3: Annual scientific production in Scopus and W.O.

Analysis of the graphs highlights a significant evolution in the interest that scientists have in the field of AI applied to banking fraud. Both graphs reveal low publication activity before 2017. This means that the period 2015 to 2017 corresponds to an exploratory phase where AI technologies were just beginning to be considered in this field of application. From 2018 onwards, a notable growth is observed with a progressive peak culminating in 2024. There are 23 publications for Scopus and 31 for Web of Science. This demonstrates an increased enthusiasm from the scientific community. This dynamic can be explained by several factors such as the technological maturity of AI methods, the exponential increase in digital fraud linked to the digitalization of banking services and the regulatory incentives for financial institutions to strengthen security systems. The slight decline in 2020 in the Scopus publication database could be attributed to the disruptions caused by the COVID-19 pandemic, which affected research activities and editorial processes. Finally, the apparent drop in 2025 in both databases is likely related to the partial nature of the data available for that year at the time of the analysis. It therefore does not necessarily reflect a real decrease in scientific activity in this field during the period

It should be noted that the articles selected for the study come from sufficiently reliable sources to guarantee a certain credibility to our document. It would therefore be interesting to discover the most influential sources in our field of research.

4.2. Most relevant sources

Sources, also called journals, represent a category of key players in scientific production. They disseminate verified information that advances research in many fields. For example, the scientific articles selected as part of this bibliometric analysis study went through a rigorous validation process before their dissemination and archiving. Figure 4 presents the most influential sources in the world of AI applied to bank fraud, included in WoS and Scopus.

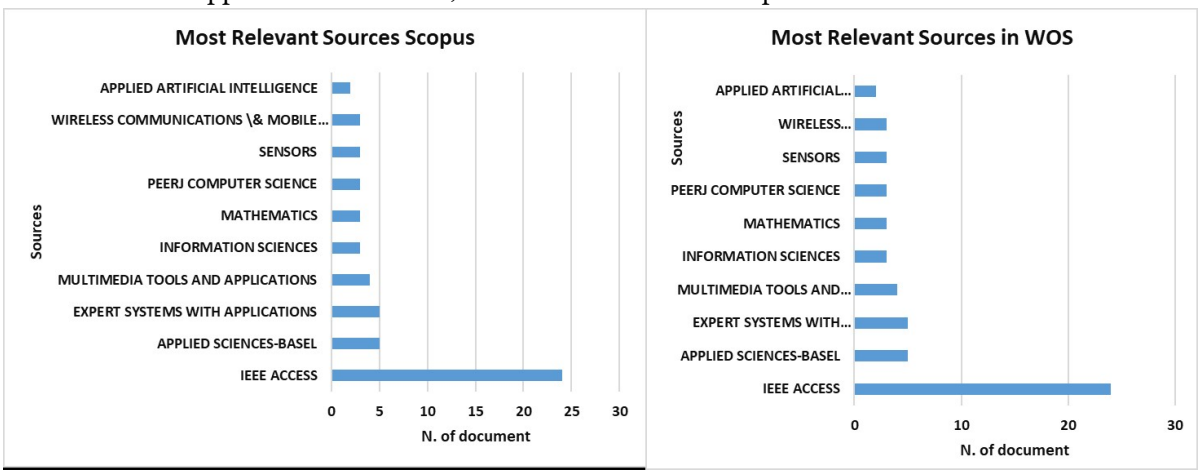

Figure 4: Most relevant sources

From the graphs, the journal "IEEE Access" stands out with nearly 25 documents published in each of the databases considered, far surpassing other sources. This supremacy of "IEEE Access" can be explained by its inclusive editorial policy, its interdisciplinary orientation as well as its responsiveness in terms of publication. These values seem particularly attractive to researchers working on emerging technological issues such as machine learning algorithms applied to financial cybersecurity. In addition, "IEEE Access" is an open access journal, promoting the international visibility of work, particularly from African countries, where access to paid publications can be a major obstacle.

Other identified sources such as "Expert Systems with Applications", "Multimedia Tools and Applications" or "Information Sciences" are quantitatively less represented with publications varying between 3 and 6 documents. This confirms the technical and algorithmic dimension of the research field, with an orientation towards intelligent systems, complex signal processing and information security. The relative stability of these journals in both databases demonstrates a consensus on their relevance for the scientific community working at the interface of AI and finance.

The low representation of publications in certain sources such as "Applied Artificial Intelligence" or "PeerJ Computer Science" can be attributed to the thematic specificity of these journals or to more selective editorial criteria. Furthermore, the limited volume of articles in African journals or those focused on local banking issues reflects an imbalance in the international visibility of African research on financial fraud. This observation highlights the need to strengthen the structuring of regional journals, encourage publications in international collaboration and broaden access to high-level scientific dissemination channels.

Finally, the convergence of source profiles between Scopus and WoS indicates a progressive standardization of publication channels in this field of research. This result can also be interpreted as a possible underrepresentation of contextual perspectives, particularly African ones, in major general journals. This raises a strategic challenge, which is to promote scientific production anchored in local realities while meeting the demands of international research.

4.3. Most relevant affiliation

Affiliations are the research institutes or universities to which the authors belong. Their role is crucial in scientific research because they help contextualize research, demonstrate the legitimacy of the authors, and facilitate knowledge dissemination. A few, including some in Africa, have distinguished themselves for their contribution to the application of AI to bank fraud. Figure 5 presents the trends.

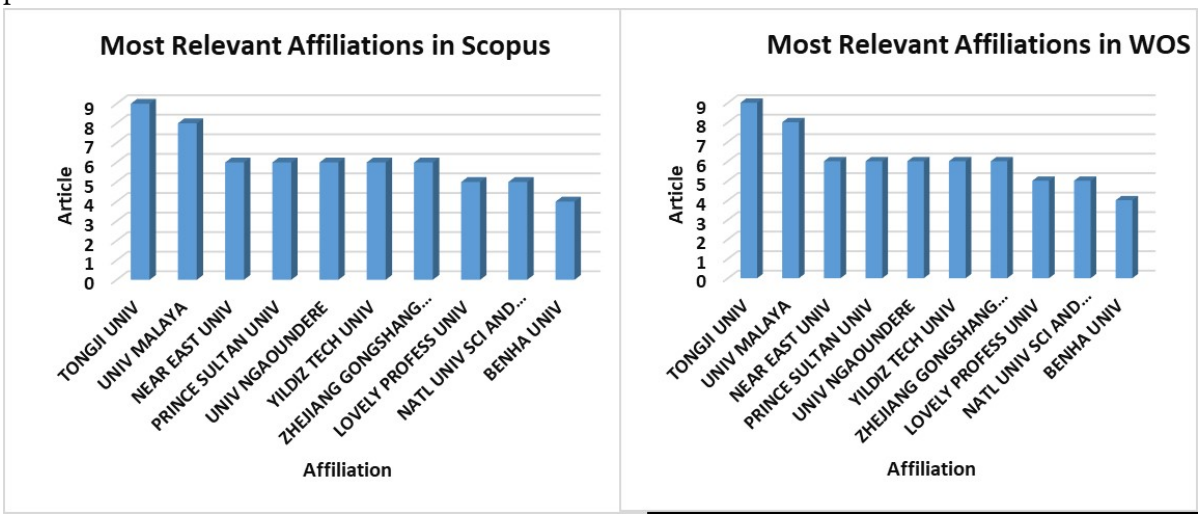

Figure 5: Most relevant affiliation

The two graphs, developed using information from the Scopus and WoS databases, show a notable convergence in the most active institutional affiliations in the field of research related to the application of AI to the detection and prevention of banking fraud. "Tongji University" and "University of Malaya" consistently occupy the top positions in both corpora. This reflects a consolidated research strategy and regular scientific production. Despite this consistency, subtle differences in the order of affiliations suggest disparities in documentary coverage, indexing criteria, or editorial policies specific to each database. The representation of African institutions remains marginal, with the exception of a few isolated cases such as the University of Ngaoundéré. This highlights a persistent underrepresentation of African research in high-impact international databases. This situation can be explained by various structural factors, including insufficient research funding, poor accessibility to indexed journals, and a lack of incentive policies for scientific promotion. In contrast, Asian and Middle Eastern institutions are demonstrating growing dynamism, often supported by proactive public policies in digital transformation. In this context, it is becoming imperative for African institutions to strengthen their integration into international research networks and develop mechanisms that promote publication in indexed journals. This could increase their scientific visibility, and they will be able to contribute significantly to this strategic area. It is now time to talk about authors, the linchpins of scientific production.

4.4. Most relevant author

Indeed, beyond simply counting publications, the h-index constitutes a relevant bibliometric indicator for assessing the productivity and scientific impact of authors in a given field. In the context of the application of AI to the prevention and detection of banking fraud, the analysis of the most prolific authors in the WoS and Scopus databases invites a more nuanced reading based on this index. Figure 6 presents the trends.

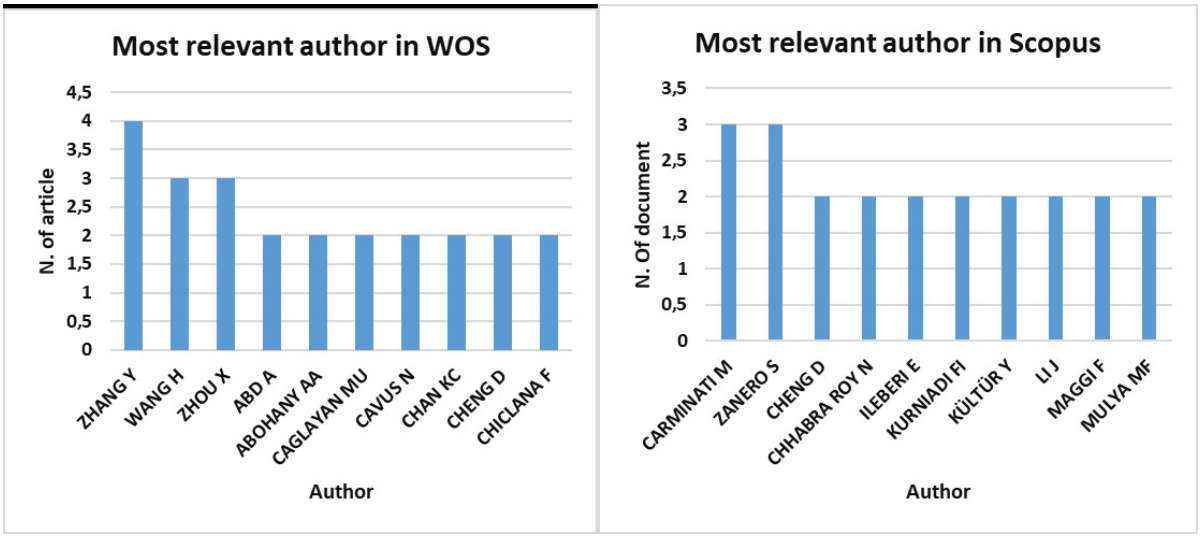

Figure 6: Most relevant author

The WoS publication database shows that authors ZHANG Y, WANG H, and ZHOU X are the most quantitatively productive authors. However, their true influence in the field cannot be fully measured without considering the quality and impact of their publications. An author with 3 or 4 articles may have only a low h-index if their publications are rarely cited. Conversely, a less prolific researcher in terms of the number of documents may exert a major influence on the literature thanks to fundamental, highly cited contributions. This reasoning also applies to Scopus, where CARMINATI M and ZANERO S occupy the top positions in terms of volume, but where the h-index could reveal other more influential authors due to the relevance of their work.

In the African context, this qualitative dimension is particularly crucial. Many researchers on the continent, although not well represented in volume rankings, could nevertheless gain greater visibility and recognition if they focus their efforts on local and innovative issues likely to generate significant academic impact. Moreover, in an environment marked by limited resources, it is more realistic to aim for strategic productivity based on publications with high citation potential, rather than a race for volume, which is difficult to sustain.

In short, the h-index shifts the focus from purely quantitative logic to an assessment of actual scientific impact. For African countries, where R&D investment remains low, this approach can inspire a targeted editorial strategy aimed at producing quality research on the continent's specific challenges, including the architecture of informal banking systems, cybersecurity in mobile services, or the adaptation of AI algorithms to local constraints. This would not only strengthen the h-index of African researchers, but also enrich the international literature with perspectives that are still underrepresented.

4.5. Most relevant country

States contribute to the development of scientific knowledge through funding, regulation, and the definition of research policies. They encourage research actors to explore the shadow areas of knowledge and provide them with the necessary infrastructure. This is true because countries with high productivity in the field of AI are strongly supported by their governments, as shown in Figure 7.

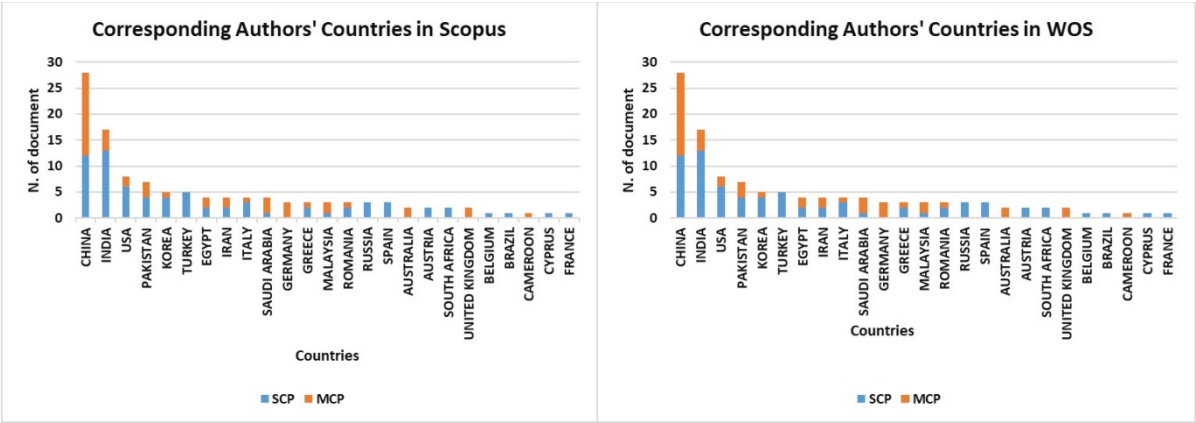

Figure 7: Most relevant country

Analysis of the Scopus and WoS databases reveals contrasting dynamics. China, India, and the United States clearly dominate scientific production. Scopus presents much higher volumes than WoS. This is explained by a broader coverage of local journals, particularly Asian ones. In China and India, publications are predominantly national (SCP). The United States and European countries favor more international collaborations (MCP), especially visible in WoS.

African countries remain in the background. However, South Africa, Cameroon, and Nigeria appear tentatively in Scopus. This visibility is due to the indexing of regional journals. Scopus places greater emphasis on the scientific output of countries in the Global South. WoS, more selective, reflects high-impact research.

African countries must strengthen their research capacities. International partnerships are essential. Investing in AI applied to banking cybersecurity is a strategic priority. Scopus provides an inclusive vision. WoS imposes a requirement for excellence. These two approaches complement each other when evaluating global research. However, one question nags at the mind: what technologies do perpetrators typically use to combat banking fraud?

5. Machine learning in the fight against banking fraud: an investigation

The objective of the section is to structure the AI technologies commonly deployed to tackle fraud in the banking sector. Note that the same technologies are used in insurance and many other fields [10, 11]. The categorization of the different techniques, as discussed here, comes from a thorough understanding of the scientific documents dealing with the application of AI to banking fraud. The main approaches identified in the arsenal of the fight against banking fraud are four (04): (I) supervised learning [12]; (II) unsupervised learning; (III) reinforcement learning, without forgetting the (IV) hybrid techniques [13, 14, 15]. The set of the above categories is known as "Machine Learning" [14, 17, 18]. Each technology being itself composed of sub-technologies or algorithms as shown in figure 8.

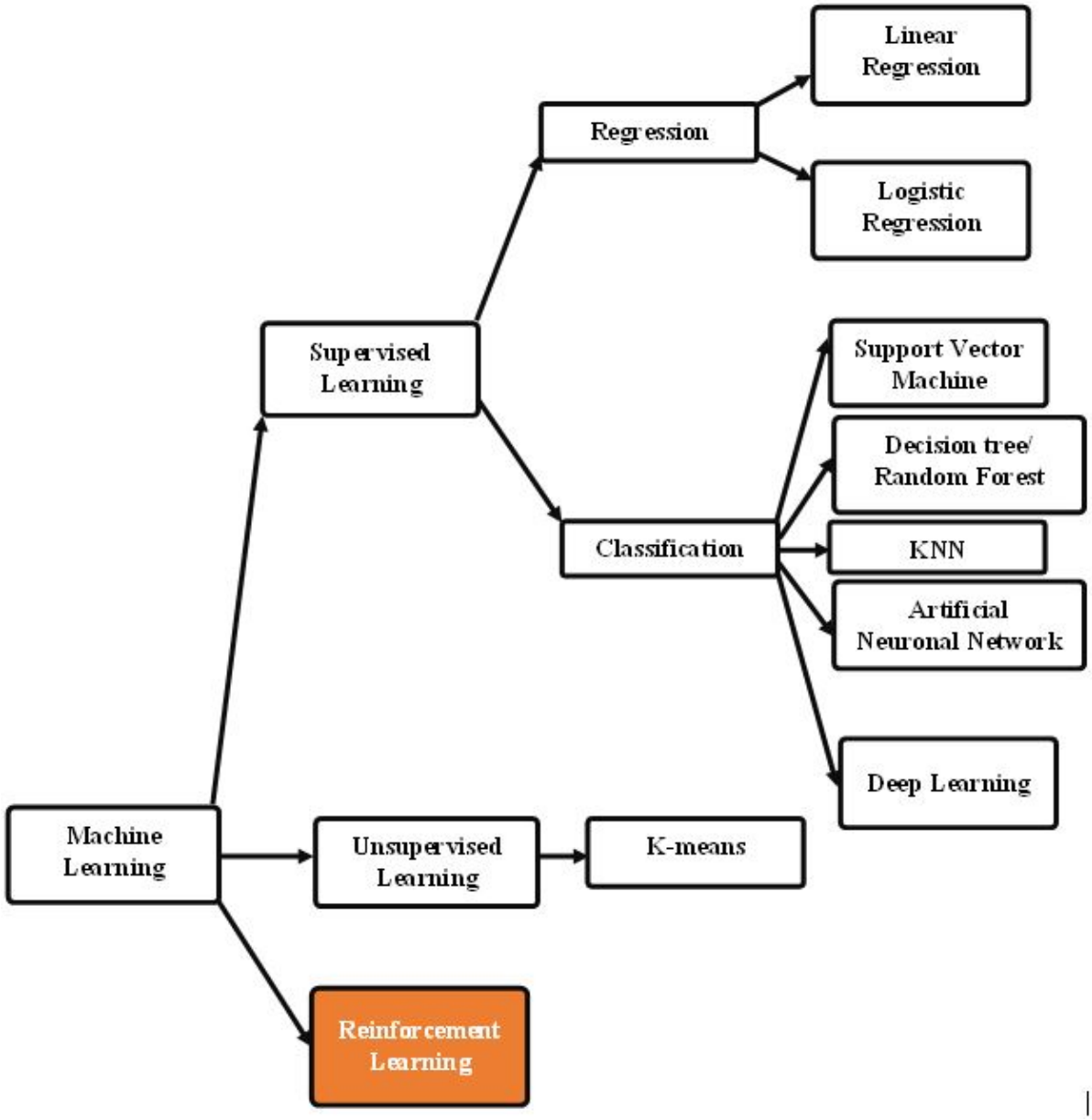

Figure 8: Technologies commonly deployed to tackle fraud in the banking sector

From the observation of Figure 8, we get an idea of the scope of use of certain algorithms through the red or white markers. Red symbolizes rarely used technologies while green represents regularly used algorithms. It is important to emphasize that the algorithms are chosen according to the cases.

For example, reinforcement learning is used for real-time detection systems [18, 19] while “artificial neural networks” are used to model complex relationships between variables [20].

5.1. Supervised learning: modeling fraud from historical data

Supervised learning remains one of the most widely used approaches in banking fraud detection systems due to its ability to efficiently exploit labeled transaction histories. This approach is based on the assumption that fraud patterns can be learned from past examples [21] and then generalized to new data. It mobilizes a range of classical or advanced algorithms such as logistic regression, decision trees, random forests, support vector machines (SVM), as well as deep learning architectures such as convolutional neural networks (CNN) or recurrent neural networks (LSTM) [22].

In a banking environment, these models can predict the probability of a fraudulent transaction occurring based on variables such as amount, merchant type, geolocation, time, or historical customer behavior. For example, systems based on neural networks have been successfully used to identify unusual transactional sequences in massive datasets, such as those of online banks [23].

This approach finds a direct parallel in the insurance field where supervised models are used to analyze claims and identify deviant behavior. A study by Ming et al. (2024) shows that machine learning models are effective in analyzing risks in the insurance sector [7], especially when they are associated with socio-demographic characteristics or past histories.

Despite their effectiveness, supervised approaches suffer from a low ability to detect new or rare frauds, especially due to class imbalance. This phenomenon is called “class imbalance” [24, 25, 26].

5.2. Unsupervised learning: detecting the unknown through anomaly analysis

Supervised learning is based on history, while unsupervised learning is used in contexts where fraud is not yet labeled. It is also used for cases of fraud evolving rapidly and unpredictably. It is based on the detection of anomalies, defined as statistically atypical observations compared to normal behavior. Methods such as autoencoders, Isolation Forest, singular value decomposition (SVD) or clustering techniques (DBSCAN, K-means) are frequently used [27].

In banking, these models are able to identify transactions that deviate from the usual profiles of a user or customer segment. For example, the use of autoencoders allows typical transactions to be reconstructed with a low error rate, while frauds generate a higher reconstruction error, signaling suspicious behavior [28].

Despite their interest, these methods have several limitations which are: difficult interpretation, the results can be unstable depending on the chosen parameters and false positives are frequent. Nevertheless, they play a crucial role in hybrid systems, by feeding detection pipelines with weak or unanticipated signals [29].

5.3. Reinforcement learning: an adaptive strategy for fraud prevention

Reinforcement learning (RL) opens a new dimension in fraud detection, by considering this task as a sequential process of decision optimization. An AI agent interacts with the environment (e.g., a transaction stream), receives positive or negative rewards depending on the actions taken (accept, reject, alert, block), and adjusts its strategy to maximize its long-term effectiveness [27].

This approach is particularly useful for modeling complex scenarios, where decisions must take into account the global context and future consequences. In the banking case, an RL agent can learn to dynamically adjust detection thresholds according to the customer risk level, the saturation of the control service or the alert history. Huang et al. (2021) propose a Deep Q-Networks-based framework to prioritize human investigations on the most critical cases, maximizing the return on verification efforts [13].

In the insurance field, RL can also be used to optimize reimbursement or expert request policies, taking into account policyholder histories, management costs and latent fraud risk [28].

However, there are many obstacles. Learning requires numerous trials, the reward function is difficult to calibrate, and simulated environments must be close to reality. Furthermore, the transparency of the agent's decisions remains a major concern for institutions subject to regulatory constraints.

5.4. Towards hybrid approaches: combining approaches for resilient detection

To circumvent the natural limitations of the three approaches mentioned in the previous sections, a strong trend is emerging towards hybrid architectures that take advantage of the complementarity of paradigms. In these systems, unsupervised models are used to detect anomalies or pre-filter data while supervised models intervene to classify and refine predictions [34]. Reinforcement learning optimizes responses based on feedback and the intervention context [29].

For example, an effective combination may rely on an autoencoder that flags an anomaly, an SVM classifier that validates the suspicion by comparing with known frauds, and an RL agent that decides whether to block, monitor, or forward to a human analyst. A recent study by Xu et al. (2021) shows that such combinations achieve significant improvements in recall and precision, while reducing the cognitive load on supervisory teams [31].

6. Discussion

The study showed that scientific production in this field experienced significant growth from 2018 onwards. The journal "IEEE Access" caught our attention with nearly 25 documents published in each of the databases considered, far surpassing other sources. In terms of affiliation, "Tongji University" and "University of Malaya" consistently occupy the top positions in both corpora. China, India, and the United States clearly dominate scientific production. African countries remain behind. However, South Africa, Cameroon, and Nigeria appear timidly in Scopus. The WoS publication database shows that authors ZHANG Y, WANG H, and ZHOU X are the most quantitatively productive authors. Our investigation into the field of AI applied to banking fraud shows that supervised learning, unsupervised learning, and reinforcement learning are the AI technologies traditionally deployed in the fight against banking fraud.

According to Jean-Pierre Buigues [35], Asia has taken a dominant place in the global trade of high technologies. Indeed, the present study confirms this state of affairs by positioning India and China at the top of the list of sponsorship and scientific production. The significant volume of research in India and the substantial financial resources deployed by China indicate a strategic desire of these countries to influence the standards and practices of the industry on an international scale. To understand the reasons behind this part of the world's enthusiasm for high technologies, particularly Artificial Intelligence, it is important to go back in history [36]. Indeed, the whole of Asia was under the economic and military domination of the West for several decades. High technologies, particularly artificial intelligence, then appear as an opportunity to take revenge and free themselves from Western domination. Thus, Iran and North Korea are leading the arms race; Japan and South Korea are fond of electronics and mechanics. All these countries intend to exploit high technology to the fullest to regain their status in the community of nations. We understand from this that the sub-field of AI applied to the detection and prevention of banking fraud is simply benefiting from this part of the world's enthusiasm for high technology. This specific area of research therefore receives no special attention [37].

Furthermore, the 2019-2020 period was marked by a decline in scientific production in the field studied. This state of affairs is justified by the reign of the COVID-19 pandemic, which was a painful ordeal for all humanity. Confinement, social distancing, and mandatory wearing of masks are all measures that contributed to the drop in positive indicators in all fields of activity, including the field of scientific production studied in this article.

One particular aspect caught our attention during the analysis of documents, authors, and sources. This is the low participation of African authors in scientific production in the field of AI applied to banking fraud. Yet, the phenomenon is present there and claims thousands of victims

both within the continent and beyond. In our opinion, the problem is structural, and it is important that scientists and politicians on the continent agree to find solutions to follow in the footsteps of Asians who are making considerable efforts in this field of research.

7. Limits of the study

This study was based on reliable and carefully selected data. However, it has limitations related to the fact that only the Scopus and WoS platforms were used to conduct the study. It would still have been interesting to conduct a comparative study taking into account more than two databases such as Google Scholar or IEEE Xplore. Similarly, a bibliometric study is only quantitative in nature. Qualitative measurement requires a more in-depth analysis of the scientific productions studied. Also, the investigation conduct in Section 5 is not complete. It is limited by the lack of details on commonly used technologies and related methodologies. That will be the subject of a future study.

8. Challenges

The application of AI to banking fraud presents numerous challenges. The most important of these challenges is addressing the almost complete lack of contributions from African countries in this research area, despite the omnipresence of the phenomenon on the continent. Additionally, there is the low visibility of African researchers in international databases. More importantly, it is urgent to develop AI technologies capable of detecting rare or emerging fraud while minimizing false positives. Finally, enforcing international collaborations and investments in research on banking cybersecurity could advance research in this field.

9. Conclusion and future work

Writing scientific documents of a certain scope in a field of research requires a first interest in a bibliometric analysis study. This allows the researcher to understand the trends, identify the dominant schools of thought and the resource people in this specific field of research. This article is positioned as a preliminary step to a systematic literature review in the field of AI applied to solving banking fraud problems.

At the end of the study, we concluded that scientific production in this field has experienced significant growth since 2018. The journal "IEEE Access" caught our attention with nearly 25 documents published in each of the databases considered, far surpassing the other sources. In terms of affiliation, "Tongji University" and "University of Malaya" consistently occupy the top positions in both corpora. China, India, and the United States clearly dominate scientific production. African countries remain behind. However, South Africa, Cameroon, and Nigeria appear timidly in Scopus. The WoS publication database shows that authors ZHANG Y, WANG H, and ZHOU X are the most productive authors in quantitative terms. Our investigation into the field of AI applied to banking fraud shows that supervised learning, unsupervised learning and reinforcement learning are the AI technologies traditionally deployed in the fight against banking fraud.

In our future research, we will initially conduct a qualitative analysis of the studied documents. This will be a systematic literature review aimed at exploring specific AI technologies applied to banking fraud and their adaptation to the local context, particularly in Africa. Additionally, further research will complement the project and will consider the promotion of African publications in international journals to increase their visibility and impact. Furthermore, hybrid systems combining supervised, unsupervised, and reinforcement learning will be proposed for a more robust fraud detection.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] United Nations Office on Drugs and Crime, "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes", 2011, Available online: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf (2011)

[2] S. Kumar et al., "Exploitation of Machine Learning Algorithms for Detecting Financial Crimes Based on Customers' Behavior", SUSTAINABILITY, vol. 14, no . 21. MDPI, ST ALBAN-ANLAGE 66, CH-4052 BASEL, SWITZERLAND, November 2022. doi: 10.3390/su142113875.

[3] J. Nicholls, A. Kuppa, and N.-A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," IEEE ACCESS , vol. 9. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC, 445 HOES LANE, PISCATAWAY, NJ 08855-4141 USA, p. 163965–163986, 2021. doi: 10.1109/ACCESS.2021.3134076.

[4] OA Oke and N. Cavus, "The Role of AI in Financial Services: A Bibliometric Analysis," JOURNAL OF COMPUTER INFORMATION SYSTEMS. TAYLOR \& FRANCIS INC, 530 WALNUT STREET, STE 850, PHILADELPHIA, PA 19106 USA, January 18, 2024. doi: 10.1080/08874417.2024.2304545.

[5] G. Logeswari, S. Bose, and T. Anitha, "An Intrusion Detection System for SDN Using Machine Learning," IN TEL LIGENT AUTOMATION AND SOFT COMPUTING , vol. 35, no . 1. TECH SCIENCE PRESS, 871 CORONADO CENTER DR, SUTE 200, HENDERSON, NV 89052 USA, p. 867-880, 2023. doi: 10.32604/iasc.2023.026769.

[6] J. Isbai and D. Helmi, "Digital transformation and banking performance: a bibliometric and systematic review of the literature", Dossiers de Recherches en Économie et Gestion, vol. 12, no. 2, pp. 123–146, July 2024. DOI: 10.34874/IMIST.PRSM/doreg-v12i2.48655. [Online]. Available at: https://revues.imist.ma/index.php/DOREG/article/ view /48655.

[7] JP Manuana-nseka. "De la bibliometrie a la cybermetrie". Revue de biologie. 2010:79. Avalaible at :https://scholar.google.com/scholar?q=related:DyGuK6U4ZG8J:scholar. google.com/scioq=hl=enas-sdt=0,5 d=gs-qabs t=1750449386133 u=23p3DdyGuK6U4 ZG8J.

[8] S. Moro, P. Cortez, and P. Rita, "Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation", Expert Syst. Appl. , flight. 42, no . 3, p. 1314–1324, 2015, doi: 10.1016/j.eswa.2014.09.024.

[9] AA Chadegani, H. Salehi, M. Md Yunus, H. Farhadi, M. Fooladi, M. Farhadi, and NA Ebrahim, "A Comparison between Two Main Academic Literature Collections: Web of Science and Scopus Databases," Asian Social Science, vol. 9, no. 5, pp. 18–26, Apr. 2013. [Online]. Available at: https://doi.org/10.5539/ass.v9n5p18

[10] P. Kate, V. Ravi, and A. Gangwar, "FinGAN: Chaotic generative adversarial network for analytical customer relationship management in banking and insurance," NEURAL COMPUTING \& APPLICATIONS , vol. 35, no . 8, SI. SPRINGER LONDON LTD, 236 GRAYS INN RD, 6TH FLOOR, LONDON WC1X 8HL, ENGLAND, p. 6015–6028, March 2023. doi: 10.1007/s00521-022-07968-x.

[11] R. Ming, O. Mohamad, N. Innab, and M. Hanafy, "Bagging Vs. Boosting in Ensemble Machine Learning? An Integrated Application to Fraud Risk Analysis in the Insurance Sector", APPLIED ARTIFICIAL IN TEL LIGENCE , vol. 38, No. 1. TAYLOR \& FRANCIS INC, 530 WALNUT STREET, STE 850, PHILADELPHIA, PA 19106 USA, December 31, 2024. doi: 10.1080/08839514.2024.2355024.

[12] G. Attigeri, M. Pai MM, and RM Pai, "Supervised models for loan fraud analysis using big data approach," Eng. Lett. , flight. 29, no . 4, p. 1422–1435, 2021.

[13] H. Huang, B. Liu, X. Xue, J. Cao, "Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique" 154. ELSEVIER, RADARWEG 29, 1043 NX AMSTERDAM, NETHERLANDS, March 2024. doi: 10.1016/j.asoc.2024.111368.

[14] Y. Kultur and MU Caglayan, “Hybrid approaches for detecting credit card fraud”, EXPERT SYSTEMS , vol. 34, no . 2, SI. WILEY, 111 RIVER ST, HOBOKEN 07030-5774, NJ USA, April 2017. doi: 10.1111/exsy.12191.

[15] J. Jin and Y. Zhang, “Innovation in Financial Enterprise Risk Prediction Model: A Hybrid Deep Learning Technique Based on CNN-Transformer-WT,” JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING , vol. 36, no . 1. IGI GLOBAL, 701 E CHOCOLATE AVE, STE 200, HERSHEY, PA 17033-1240 USA, 2024. doi: 10.4018/JOEUC.361650.

[16] E. Jayanthi et al. , “Cybersecurity enhancement to detect credit card frauds in health care using new machine learning strategies”, SOFT COMPUTING , vol. 27, no . 11. SPRINGER, ONE NEW YORK PLAZA, SUITE 4600, NEW YORK, NY, UNITED STATES, p. 7555–7565, June 2023. doi: 10.1007/s00500-023-07954-y.

[17] I. Gonzalez-Carrasco, J. Luis Jimenez-Marquez, J. Luis Lopez-Cuadrado, and B. Ruiz-Mezcua, “Automatic detection of relationships between banking operations using machine learning,” INFORMATION SCIENCES , vol. 485. ELSEVIER SCIENCE INC, STE 800, 230 PARK AVE, NEW YORK, NY 10169 USA, p. 319–346, June 2019. doi: 10.1016/j.ins.2019.02.030.

[18] A. Hanae, B. Abdellah, E. Saida, and G. Youssef, “End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions,” Int. J.Adv. Comput. Sci. Appl. , flight. 14, no . 6, p. 749-757, 2023, doi: 10.14569/IJACSA.2023.0140680.

[19] M. Arya and H. Sastry G, “Deep Ensemble ALgorithm’framework for credit card fraud detection in real-time data stream with Google TensorFlow,” Smart Sci. , flight. 8, no . 2, p. 71–83, 2020, doi: 10.1080/23080477.2020.1783491.

[20] Y.-C. Shih, T.-S. Dai, Y.-P. Chen, Y.-W. Ti, W.-H. Wang, and Y. Kuo, “Fund transfer fraud detection: Analyzing irregular transactions and customer relationships with self-attention and graph neural networks,” Expert Syst. Appl. , flight. 259, 2025, doi: 10.1016/j.eswa.2024.125211.

[21] A. Vashistha and AK Tiwari, “Building Resilience in Banking Against Fraud with Hyper Ensemble Machine Learning and Anomaly Detection Strategies,” SN Comput. Sci. , flight. 5, no . 5, 2024, doi: 10.1007/s42979-024-02854-w.

[22] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, “A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System,” Ann. Data Sci. , flight. 11, no . 1, p. 103–135, 2024, doi: 10.1007/s40745-022-00433-5.

[23] NH Hassan and AS Fakharudin, “Web Phishing Classification Model using Artificial Neural Network and Deep Learning Neural Network,” Int. J.Adv. Comput. Sci. Appl. , flight. 14, no . 7, p. 535–542, 2023, doi: 10.14569/IJACSA.2023.0140759.

[24] J. Singla, AK Bashir, Y. Nam, NUI Hasan, and U. Tariq, “Handling class imbalance in online transaction fraud detection,” Comput. Mater. Continue. , flight. 70, no . 2, p. 2861–2877, 2022, doi: 10.32604/cmc.2022.019990.

[25] B. Ribeiro, F. Antunes, D. Perdigão, and C. Silva, “Convolutional Spiking Neural Networks targeting learning and inference in highly imbalanced datasets,” Pattern Recognit. Lett. , 2024, doi: 10.1016/j.patrec.2024.08.002.

[26] Y.-R. Chen, J.-S. Leu, S.-A. Huang, J.-T. Wang, and J.-I. Takada, “Predicting Default Risk on Peer-to-Peer Lending Imbalanced Datasets,” IEEE Access , vol. 9, p. 73103–73109, 2021, doi: 10.1109/ACCESS.2021.3079701.

[27] K. Zhu, N. Zhang, W. Ding, and C. Jiang, “An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection,” IEEE Trans. Artif. Intel. , flight. 5, no . 8, p. 4026–4041, 2024, doi: 10.1109/TAI.2024.3359568.

[28] N. Chhabra Roy and S. P, “Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks”, Digit. Policy Reg. Gov. , flight. 26, no . 6, p. 678-707, 2024, doi: 10.1108/DPRG-02-2024-0029.

[29] CS Kolli and T. Uma Devi, “Hybrid Optimization and Deep Learning for Detecting Fraud Transactions in the Bank,” Int. J. Inf. Secur. Private , flight. 16, no. 1 , 2022, doi: 10.4018/IJISP.300323.

[30] Y. Kültür and MU Çağlayan, “Hybrid approaches for detecting credit card fraud”, Expert Syst. , flight. 34, no. 2 , 2017, doi: 10.1111/exsy.12191.
[31] H. Huang, B. Liu, X. Xue, J. Cao, and X. Chen, “Unbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique,” Appl. Soft Computing. , flight. 154, 2024, doi: 10.1016/j.asoc.2024.111368.
[32] P.-A. Buigues, “Technologies: how not to be left behind by Asia?”, Telos, Jan. 4, 2023. [Online]. Available: https://www.telos-eu.com/fr/economie/technologies-comment-ne-pas-se-faire-distancer-par.html
[33] F. Khaled Alarfaj and S. Shahzadi, “Enhancing Fraud Detection in Banking with Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention,” IEEE Access, vol. 13, p. 20633–20646, 2025, doi: 10.1109/ACCESS.2024.3466288.
[34] U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, “Using generative adversarial networks for improving classification effectiveness in credit card fraud detection,” Inf. Sci. , flight. 479, p. 448–455, 2019, doi: 10.1016/j.ins.2017.12.030.
[35] MA Ahmed, NTA Haleem, and AM Idrees, “A Smart Framework for Enhancing Automated Teller Machines (ATMs) Fraud Prevention,” Int. J.Adv. Comput. Sci. Appl. , flight. 15, no . 2, p. 153-162, 2024, doi: 10.14569/IJACSA.2024.0150217.
[36] Manta AG, Bădîrcea RM, Doran NM, Badareu G, Gherțescu C, Popescu J. Industry 4.0 transformation: Analysing the impact of artificial intelligence on the banking sector through bibliometric trends. Electronics. 2024 Apr 27;13(9):1693.
[37] Jannah R, Sari MP, Utaminingsih NS, Budiantoro RA. A Bibliometric Analysis of Artificial Intelligence and Blockchain Technology in Fraud Prevention and Detection. Akuisisi: Jurnal Akuntansi. 2024 May 21;20(1):96-115.