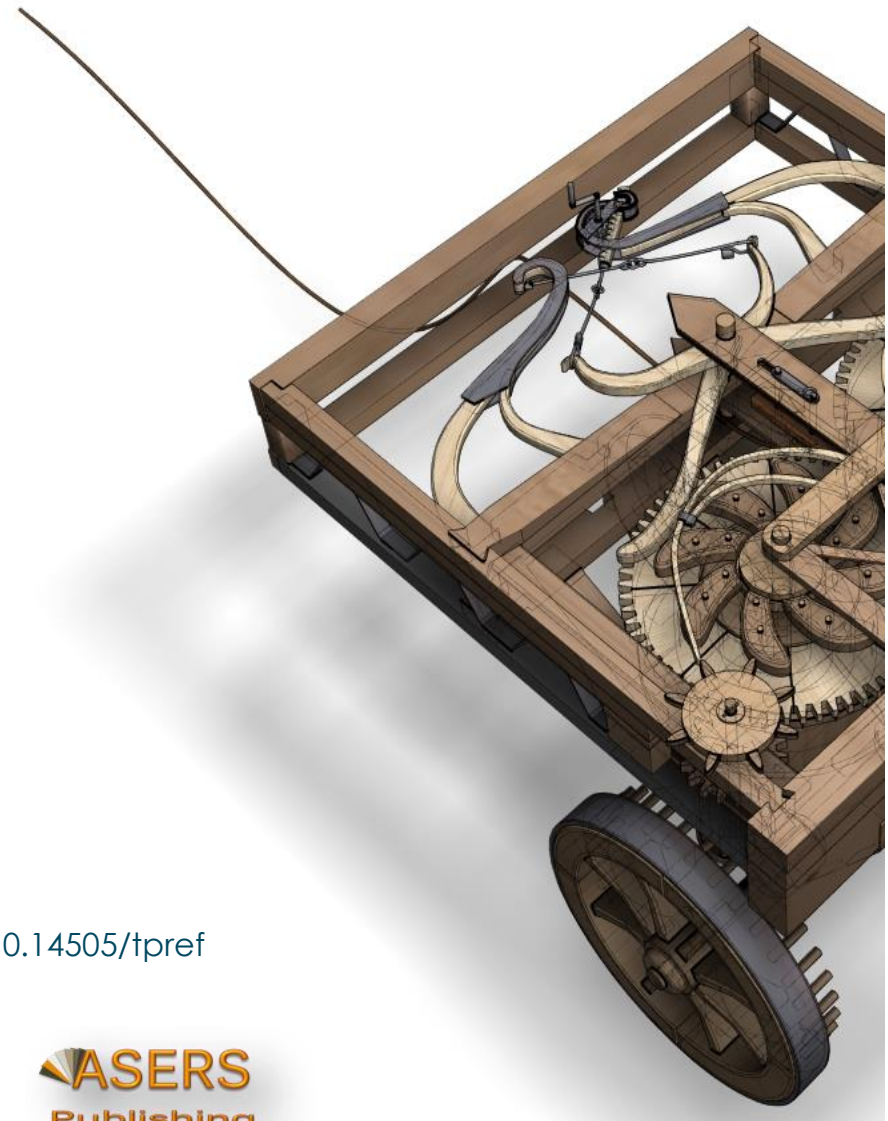
Theoretical and Practical Research in Economic Fields



Quarterly
Volume XV
Issue 4(32)
Winter 2024

ISSN: 2068 – 7710
Journal DOI: https://doi.org/10.14505/tpref

ASERS
Publishing

Volume XV
Issue 4(32)
Fall 2024

ASERS Publishing
ISSN 2068 – 7710
Journal's Issue DOI:
https://doi.org/10.14505/tpref.v15.3(31).00

Table of Contents

Volume XV
Issue 3(31)
Fall 2024

ASERS Publishing
http://www.asers.eu/asers-publishing
ISSN 2068 – 7710
Journal's Issue DOI:
https://doi.org/10.14505/tpref.v15.3(31).00

Call for Papers
Spring Issue
Theoretical and Practical Research in Economic Fields

Many economists today are concerned by the proliferation of journals and the concomitant labyrinth of research to be conquered in order to reach the specific information they require. To combat this tendency, **Theoretical and Practical Research in Economic Fields** has been conceived and designed outside the realm of the traditional economics journal. It consists of concise communications that provide a means of rapid and efficient dissemination of new results, models, and methods in all fields of economic research.

Theoretical and Practical Research in Economic Fields publishes original articles in all branches of economics – theoretical and practical, abstract, and applied, providing wide-ranging coverage across the subject area.

Journal promotes research that aim at the unification of the theoretical-quantitative and the empirical-quantitative approach to economic problems and that are penetrated by constructive and rigorous thinking. It explores a unique range of topics from the frontier of theoretical developments in many new and important areas, to research on current and applied economic problems, to methodologically innovative, theoretical, and applied studies in economics. The interaction between practical work and economic policy is an important feature of the journal.

Theoretical and Practical Research in Economic Fields is indexed in SCOPUS, RePEC, ProQuest, Cabell Directories and CEEOL databases.

The primary aim of the Journal has been and remains the provision of a forum for the dissemination of a variety of international issues, practical research, and other matters of interest to researchers and practitioners in a diversity of subject areas linked to the broad theme of economic sciences.

At the same time, the journal encourages the interdisciplinary approach within the economic sciences, this being a challenge for all researchers.

The advisory board of the journal includes distinguished scholars who have fruitfully straddled disciplinary boundaries in their academic research.

All the papers will be first considered by the Editors for general relevance, originality, and significance. If accepted for review, papers will then be subject to double blind peer review.

Deadline for submission of proposals:	10th February 2024
Expected publication date:	30th March 2024
Website:	http://journals.aserspublishing.eu/tpref
E-mail:	tpref@aserspublishing.eu

To prepare your paper for submission, please see full author guidelines in the following file: https://journals.aserspublishing.eu/tpref/Template_for_Authors_TPREF.docx on our site.

DOI: https://doi.org/10.14505/tpref.v15.4(32).19

The Use of Artificial Intelligence to Detect Suspicious Transactions in the Anti-Money Laundering System

Hassan Ali AL-ABABNEH
Department of Electronic Marketing and Social Media
Faculty of Economics and Administrative Sciences, Zarqa University, Jordan
ORCID: 0000-0003-1136-8911
hassanalialababneh@gmail.com

Cholpon NURALIEVA
Department of Accounting, Analysis and Audit
Kyrgyz-Russian Slavic University named after B.Yeltsin, Kyrgyz Republic
ORCID: 0000-0001-8005-054X
Nuralieva.ch1@gmail.com

Gulbaira USMANALIEVA
Department of Accounting, Analysis and Audit
Kyrgyz-Russian Slavic University named after B.Yeltsin, Kyrgyz Republic
ORCID: 0000-0002-4470-0303
Usmanalieva.Gul11@gmail.com

Maksym KOVALENKO
Interregional Academy of Personnel Management, Kyiv, Ukraine
ORCID: 0009-0008-0577-3148
Smart.Max.kovalenko1@gmail.com

Bohdan FEDOROVYCH
Department of Finance
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0005-0494-2825
Fedorovych111@gmail.com

Article info: Received 10 October 2024; Received in revised form 27 October 2024; Accepted for publication 28 November 2024; Published 30 December 2024.

Abstract: Artificial intelligence (AI) is being actively implemented in anti-money laundering (AML) systems due to its potential to improve the detection of suspicious transactions. The article examines AI's effectiveness in detecting and reducing financial crimes of private military companies.

The research employs machine learning (ML) algorithms and neural networks, anomaly detection methods, and economic impact assessment. A combination of supervised and unsupervised learning methods enables the creation of accurate predictive models for detecting money laundering anomalies.

The results show that AI models outperform traditional rule-based systems, reducing false positives by 30% and increasing high-risk detection by 25%. This proves the advantages of AI over conventional anti-money laundering methods, which often cannot adapt quickly.

The research emphasizes the transformative impact of AI on anti-money laundering systems, optimizing accuracy and resource allocation. Further research should focus on improving AI algorithms and their application in new financial technologies.

Keywords: artificial intelligence; money laundering; suspicious transactions; machine learning; insurance.

JEL Classification: E42; G38; H6

Introduction

Given rapid globalization and increasingly complex financial transactions, effective detection and prevention of money laundering have become critically important. Digital technologies are pivotal in promoting transparency within public authorities, thereby minimizing corruption risks through enhanced data accessibility and auditability (Lazor *et al.* 2024). Traditional AML systems often cannot keep up with criminal organizations' new tactics. AI plays an important role in this context, offering innovative solutions to improve the detection of suspicious transactions and strengthen AML systems (Ricadela 2024). AI contributes significantly to public service improvement and fraud prevention by optimizing processes, predicting risks, and enabling efficient resource allocation (Kruhlov *et al.* 2024). AI can process large volumes of transactions with high accuracy, uncovering complex patterns of illegal activity and increasing the overall efficiency of systems. The need to attract investments in the primary sectors is essential for economic development, especially within the Industry 4.0 paradigm, which emphasizes digitization and smart technologies (Nikonenko *et al.* 2022).

However, several important issues remain underexplored. First, the effectiveness of various AI techniques, such as ML algorithms and neural networks, in detecting money laundering needs further study (Strategy and Transactions in Insurance 2024). Second, there is a need to study how to integrate AI technologies into existing AML practices and their impact on regulatory compliance. Enterprise economic security involves a comprehensive assessment of risk factors influencing an organization's financial stability and long-term viability (Lelyk *et al.* 2022). Third, it is important to explore how AI can reduce the number of false positives that are problematic with traditional approaches. The European Union's approach to anti-corruption regulation relies heavily on transparency, integrity, and accountability in public institutions to mitigate risks of financial misconduct (Melnyk *et al.* 2021). This research aims to fill these gaps by evaluating AI capabilities to improve the detection of suspicious transactions. The objectives include:

1.Analyze the current use of AI in AML systems and assess its effectiveness.

2.Assess the possibility of integrating AI into traditional AML methods to improve monitoring systems.

3.Identify challenges and limitations of implementing AI in AML systems, including regulatory, technical, and operational aspects.

1. Literature Review

The integration of AI into AML systems has attracted considerable research attention due to its potential to improve the detection of suspicious financial transactions. Bertrand *et al.* (2020) examined how AI-driven AML systems can be consistent with data protection rights. They noted that although AI can significantly improve the efficiency of such systems, it may conflict with existing legal standards, especially in European countries. The researchers emphasize the need to develop a strategy that would protect fundamental rights while supporting the effectiveness of the fight against money laundering. In 2021, the same authors continued the study in the European context. They point out that AI-driven AML systems may violate the fundamental rights of European citizens. The authors emphasize the importance of creating a reliable legal framework to protect the rights of individuals when using AI in AML. This research is important for addressing the legal challenges associated with AI use and points to the need for additional legal and technical measures. Abrahamyan (2023) investigated money laundering threats associated with major international sporting events. The researcher notes that large-scale financial transactions in international sports increase money laundering risks. Although AI can mitigate these threats, Abrahamyan (2023) notes that current AI technologies do not cover all aspects of complex financial transactions in this area.

Hayble-Gomes (2022) analyzed how predictive modeling can improve the Suspicious Activity Reporting (SAR) process. The study shows that AI can identify key signs of suspicious behavior, increasing the accuracy and effectiveness of SAR reports. However, the author draws attention to the shortcomings of predictive modeling, in particular to the issue of interpretation and transparency of AI-generated decisions. He emphasizes the need for more comprehensible AI techniques in AML. Fritz-Morgenthal *et al.* (2022) analyzed the implementation of transparent and reliable AI in financial risk management. The authors note the importance of explainable AI, especially in AML. There needs to be more transparency in systems to prevent trust and legal problems in the financial sector. This research is key to understanding the impact of AI on financial risk and legal liability, emphasizing the need for effective and understandable AI systems. Kute *et al.* (2021) reviewed AI techniques for detecting money laundering. They analyzed both the advantages and limitations of different AI models. The authors emphasize the need for clear methods to increase interoperability and trust in models among regulators and financial institutions.

Ashwini and Hussain (2023) examined the general impact of AI on the banking industry. The researchers note drastic changes in banking operations thanks to AI, particularly in AML procedures. At the same time, the authors draw attention to the fact that the rapid introduction of AI precedes the development of a regulatory framework, which causes risks related to data confidentiality and transparency of decisions. The study highlights the need for a cautious approach to using the capabilities of AI while minimizing risks effectively. Turksen *et al.* (2024) reviewed the legal issues of automated monitoring of suspicious financial transactions. The researchers emphasize the importance of strengthening the integrity of AI systems used in AML by bringing them into compliance with current legal regulations. The study shows that AI can significantly increase the effectiveness of detecting suspicious transactions, but strict regulation is required to minimize legal and ethical risks. Pavlidis (2023) explored the role of AI in anti-money laundering and asset recovery. The author emphasizes that AI is a powerful tool due to its ability to quickly and accurately analyze large data volumes. However, the effective implementation of AI in AML requires technological innovations and significant regulatory and organizational reforms to use these systems responsibly.

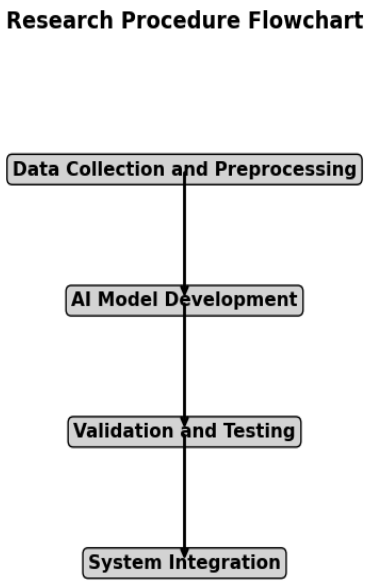
Despite significant progress in implementing AI in AML systems, several issues still need to be solved. First, while much attention is paid to the technical aspects of AI, there is a lack of research on the long-term impact of these technologies on privacy and fundamental rights, especially outside of Europe. Although current studies identify the benefits of AI for improving AML processes, more attention should be paid to possible biases and errors in the operation of AI systems. An important direction for further research is the integration of intelligible AI into AML systems. Although some works partially address this issue, practical implementation in real financial institutions needs further study. The existing literature contains conflicting findings regarding the ability of AI to detect sophisticated money laundering schemes, emphasizing the need for further empirical research. Finally, although the AI potential in AML is generally recognized, existing studies do not adequately address the organizational and regulatory changes required for successful technology integration. This points to the need for future research to develop comprehensive frameworks that integrate technical, legal and organizational aspects to maximize the effective use of AI in the fight against money laundering.

2. Methods

2.1. Research Design

The first stage of the research involved data collection and preparation. The dataset consisted of 1 million anonymous financial transactions. The data were cleaned to remove errors and normalize transaction amounts and code categories (Appendix A).

Figure 1. Research Stages



Source: developed by the author based on MiniTAB (2024)

The data were divided into learning (80%) and test (20%) sets. The next stage was the creation of an AI model. The Random Forest and Gradient Boosting algorithms were combined. These algorithms work efficiently with large data sets and help to detect anomalies. The model was trained on pre-processed data to identify patterns

that indicate suspicious transactions. The assessment and testing followed this. After learning, the model was tested on the test data set. Such metrics as precision, recovery, and F1-score were evaluated. Anti-money laundering experts also conducted manual verification of random transactions to assess the practical effectiveness of the model. The final stage is provided for system implementation. The tested model was integrated into the existing monitoring system of the financial institution. A pilot project was launched to monitor transactions in real-time, with continuous performance monitoring for three months (Figure 1).

2.2. Sampling

The study aimed to identify suspicious transactions in a dataset provided by Deutsche Bank. This bank is one of the leaders among international financial institutions in Germany. Deutsche Bank processes a huge number of financial transactions daily, making it an ideal target for applying AI systems in the fight against money laundering. The large volume and variety of data open wide opportunities for analysis. The bank is known for its modern technological solutions that contribute to the effective integration of AI for fraud detection and anti-money laundering.

Furthermore, Deutsche Bank has extensive experience in complying with international anti-money laundering regulations. Its investment in advanced compliance solutions makes the bank an important object for AI research in this area. Operating in many countries, the bank provides data that spans different economies, allowing comprehensive and global research.

Germany was chosen for the study because it has one of the strictest anti-money laundering systems, which meets the European Union's (EU) and the Financial Action Task Force on Money Laundering (FATF) standards. This creates favorable conditions for testing AI-based solutions. Being one of Europe's largest economies, Germany offers a variety of transactional data, making it ideal for investigating suspicious transaction detection systems. Financial institutions are required to keep detailed records of transactions, which ensures the availability of quality data for analysis. Germany is also actively innovating in the fight against money laundering, making it a key country to explore the application of AI in this area. As a leading financial center, it provides access to both domestic and international transaction data, which allows for the assessment of AI effectiveness in various environments.

The dataset contained one million anonymous transactions filtered by volume, frequency, and risk scores. This volume provided various transaction types, from small to large amounts. The sample was designed to reflect a typical financial profile, increasing the results' accuracy and applicability. Transactions were divided into categories: domestic transfers, international transfers, deposits, and cash withdrawals. This classification made it possible to investigate operations vulnerable to money laundering in more detail.

2.3. Methods

The study includes a combination of methods for data collection and analysis:

1. Training of ML models. The Scikit-learn Python library and the Random Forest and Gradient Boosting algorithms were used to create and train the models. The training process included cross-validation to fine-tune model parameters and avoid overfitting. The best model configuration is selected based on the highest F1 score obtained during verification.

2. Methods of detecting anomalies. The unsupervised anomaly detection algorithm, Isolation Forest, complements the supervised machine learning models. This approach helps identify anomalies that the basic model might have missed. A combination of supervised and unsupervised methods provides a more accurate detection system.

3. Assessment of economic impact. The economic consequences of the identified suspicious transactions were assessed in detail. A risk-based method was used to determine the financial impact of each transaction, taking into account the amount of the transaction, the frequency, and the profiles of the parties involved. This strategy made quantifying the potential financial risks associated with undetected suspicious transactions possible.

2.4. Tools

1. Scikit-learn libraries, NVIDIA GPUs, and cross-validation methods were used to train the models.

2. Matplotlib and Seaborn libraries were used to visualize the anomalies, which allowed a better understanding of the patterns revealed by the algorithm.

3. Using a risk-based approach, Excel and Python's Pandas were used to calculate the financial implications of each flagged transaction.

3. Results

The study uses a dataset containing 1 million anonymous financial transactions from a leading financial institution. Transactions were divided into four categories: domestic transfers, international transfers, cash deposits, and cash withdrawals. Table 1 presents an overview of the distribution of these categories.

Table 1. Categories of Transactions

Transaction type	Account	Percentage (%)
Domestic transfers	400,000	40.00
International transfers	250,000	25.00
Cash deposits	200,000	20.00
Withdrawals	150,000	15.00

Source: developed by the author based on Transaction Types (2024)

Analysis of transaction structure is key to risk assessment. A high proportion of domestic transfers may indicate the need for additional monitoring to detect anomalies. International transfers require special attention because of their complexity and high amounts, as they can be vulnerable to risks such as money laundering. Table 2 presents the results of three machine learning models: decision tree, random forest, and gradient boosting. Key metrics such as F1 score, precision, and sensitivity are used to evaluate the performance of these models in detecting suspicious transactions.

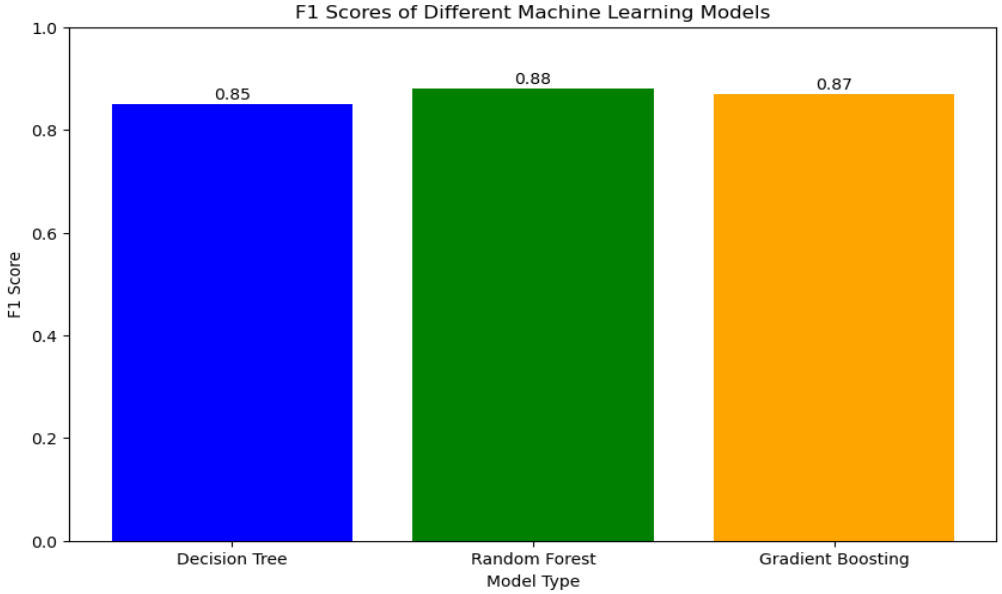
Table 2. Model Configurations and Performance Indicators

Model type	F1 score	Accuracy	Sensitivity
Decision tree	0.85	0.84	0.86
Random forest	0.88	0.87	0.89
Gradient boosting	0.87	0.86	0.88

Source: developed by the author based on Widyastuti et al. (2024), Hyperparameter Tuning Random Forest Pyspark Restackio (2021)

Random forest is the most efficient model with an F1 score of 0.88, showing an excellent balance between accuracy (0.87) and sensitivity (0.89), allowing for accurate detection of suspicious transactions and reduction of false positives. Gradient boosting performs similarly with an F1 score of 0.87, slightly inferior to random forest. The decision tree shows an F1 score of 0.85 but loses to more complex models. Figure 2 presents the F1 results for three models: decision tree, random forest, and gradient boosting, detecting suspicious transactions in the AML system.

Figure 2. F1 Scores of Different ML Models



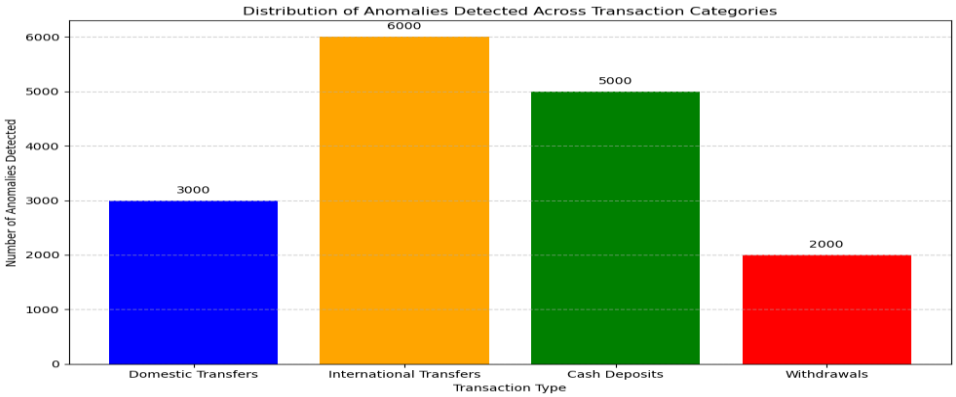
Source: Buhl (2023), Kundu (2022)

The vertical axis shows the F1 score, reflecting the precision and recall balance. The value ranges from 0 to 1, where 1 means perfect balance. The random forest model achieved the highest F1 score of approximately

0.88, showing the best performance in detecting suspicious transactions with a harmonious balance between accuracy and coverage. Gradient boosting reached 0.87, which is also a high score. The decision tree showed a lower result of 0.85, which indicates less efficiency.

Due to its ensemble nature, random forest combines the predictions of several trees, minimizing errors. Gradient boosting gradually improves accuracy by focusing on previous errors. A decision tree, capable of classifying transactions, does not strike a balance between accuracy and sensitivity very well. The F1 score is critical to AML systems, ensuring the reduction of the risk of erroneous decisions. The Isolation Forest algorithm identified 15,000 potential anomalies for further analysis. Figure 3 shows their distribution among four types of transactions: domestic, international transfers, cash deposits, and withdrawals.

Figure 3. Distribution of Detected Anomalies by Transaction Categories

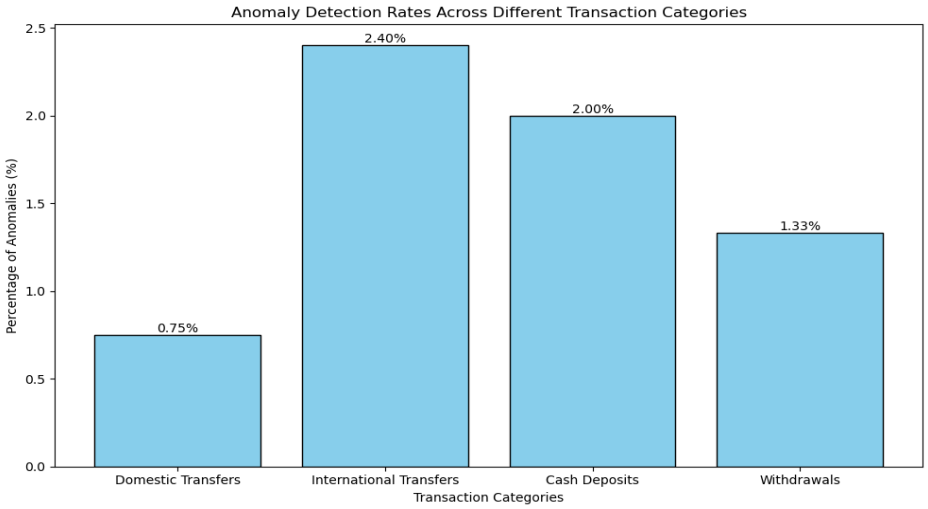


Source: The Many Use Cases for Anomaly Detection in Business Data (2024), A Guide to Building a Financial Transaction Anomaly Detector (2024)

International transfers have the largest detected anomalies, indicating their increased risk and complexity. They are often checked as part of the fight against money laundering. This is determined by different regulatory regimes, currency exchange, and the involvement of several financial institutions, which increases the likelihood of suspicious activity. Cash deposits also show many anomalies, which may indicate money laundering attempts through large or frequent deposits that do not correspond to the customer's usual financial activity. Such a situation emphasizes the importance of careful monitoring of such operations.

Although less risky, domestic transfers can also contain suspicious patterns, especially for large or frequent transfers. This may indicate attempts to launder money through local accounts using less stringent controls. Withdrawals show the lowest level of detected anomalies, which may be caused by the difficulty of detecting suspicious activity without additional context, such as the withdrawal location or subsequent use of the funds. However, this does not mean such transactions are safe — detecting violations may require more detailed analysis or a combination of monitoring with other types of transactions. Figure 4 illustrates anomalies detected by the Isolation Forest algorithm in financial transactions.

Figure 4. The Level of Detection of Anomalies in Different Categories of Transactions



Source: Dynatrace (2024), How to Detect Anomalies in Payment Transactions (2024)

Each point on the chart represents a transaction by its amount and frequency. Anomalous transactions detected by the Isolation Forest algorithm are highlighted in a contrasting color, such as red, making it easier to distinguish them from normal transactions. Anomalies are distributed unevenly between different types of operations. International transfers show a higher density of anomalies, as the many marked points in this category demonstrate. This may indicate suspicious activity, such as money laundering. Large or frequent cash deposits are also often anomalous, which can indicate suspicious activity.

Domestic transfers and withdrawals have fewer anomalies, indicating their predictable behavior. Anomalous transactions often focus on specific amounts that differ from the average. For example, large international transfers are often anomalous. A high frequency of operations in a short time can also indicate anomalies, which is manifested in the clustering of points on the chart. The economic impact was analyzed using Pandas Excel and Python, financial consequences were assessed, and key statistical data were obtained (Table 3).

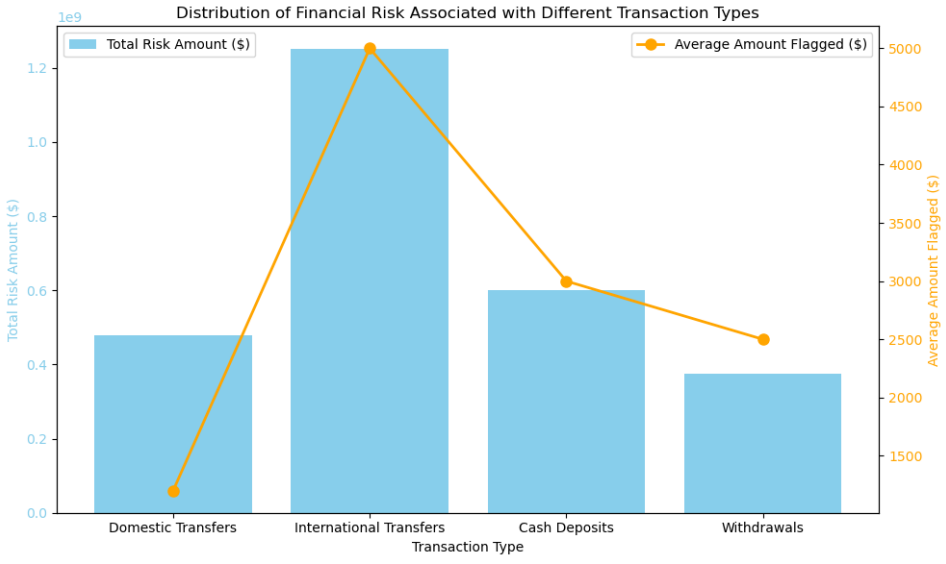
Table 3. Financial Consequences of Transactions

Transaction type	Marked Average Amount ($)	Total amount at risk ($)
Domestic transfers	1,200	480,000,000
International transfers	5,000	1,250,000,000
Cash deposits	3,000	600,000,000
Withdrawals	2,500	375,000,000

Source: developed by the author based on Tamplin (2023), Simon and Simon (2021)

The average amount of suspicious domestic transfers is $1,200, which is lower than international transactions but indicates risky domestic transactions. This indicator reaches $5,000 for international transfers, indicating greater fund involvement. The average size of suspicious deposits is $3,000, with large cash deposits making them difficult to trace. Withdrawals have an average amount of $2,500. The total financial risk from suspicious domestic transfers reaches $480 million, while for international transfers, this amount is $1.25 billion, indicating the greatest risk because of the large amounts and number of transactions. Cash deposits generate $600 million at risk, while suspicious withdrawals generate $375 million, the lowest indicator because of fewer transactions. International transfers carry the greatest risk because of the large amounts of money laundering. Domestic transfers and cash deposits also pose significant risks because of high volume and high average amounts. Withdrawal has the lowest risk. Figure 5 illustrates these risks.

Figure 5. Distribution of Financial Risk by Transaction Types



Source: Segal (2024), Financial Crime Academy (2024)

The highest financial risk is associated with international transfers since their value is much higher than other transactions despite the lower frequency. The large amounts of funds characteristic of cross-border transactions can explain this. International transfers have the most significant average amounts, which indicates a high risk for financial institutions. Cash deposits also carry significant risk, although the average amounts are smaller than international transfers. Many such transactions accumulate overall risk despite the smaller amounts

of each transaction. Because of smaller average amounts, domestic transfers and withdrawals show the lowest overall risk. In the insurance sector, the analysis covered premium and claims transactions. It was found that anomalies in insurance transactions occur less often than in other types of transactions, which indicates a lower risk of suspicious activity. Data on insurance activity, including premiums and claims, was used to assess the potential risk of suspicious behavior. Table 4 summarizes the results of insurance transactions.

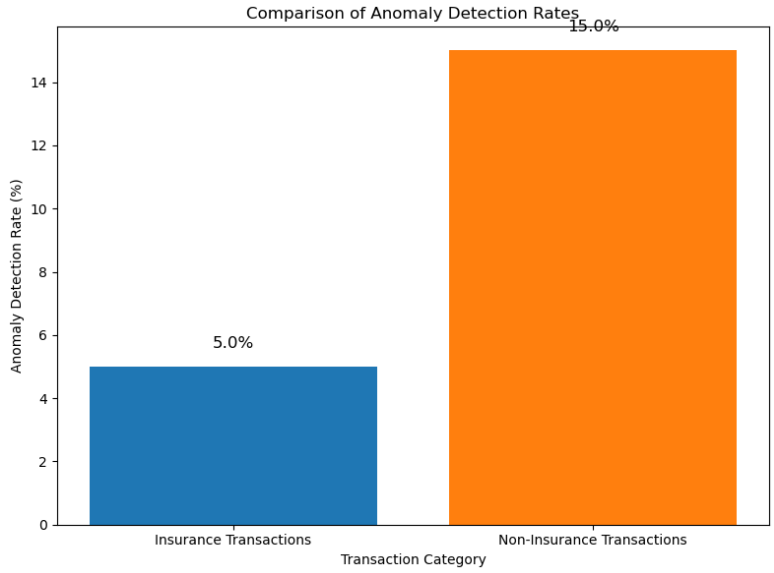
Table 4. Insurance transactions

Type of insurance transaction	Account	Percentage (%)	Marked Average Amount ($)	Total amount at risk ($)
Insurance premiums	100,000	10.00	2,500	250,000,000
Insurance claims	50,000	5.00	4,000	200,000,000

Source: developed by the author based on Strategy and Transactions in Insurance (2024)

Insurance premiums account for the majority of transactions compared to claims. However, the average amount of insurance claims exceeds premiums and significantly affects financial risk. Although insurance claims are less frequent, their amounts are often significant, making them important to monitor for suspicious activity. The low percentage of anomalies in insurance transactions compared to other transactions indicates a lower likelihood of suspicious behavior. This may result from the structuredness of insurance transactions and their regulated environment. Figure 6 compares anomalies in insurance and non-insurance transactions, revealing the main differences.

Figure 6. Comparison of Anomaly Detection Indicators



Source: Seasonal-Trend Decomposition Using LOESS (STL) - Statsmodels 0.15.0 (+429) (2024)

The histogram illustrates that insurance transactions have fewer marked anomalies than non-insurance transactions. For example, this indicator can be 2% in insurance transactions, while it is 8% in non-insurance transactions. This indicates a lower probability of suspicious behavior in insurance operations, indicating greater stability and reduced susceptibility to fraud. A clear difference between the categories demonstrates that non-insurance transactions have more suspicious transactions. Insurance transactions may have regular payouts and claims that meet standards, reducing the risk of anomalies. The results in Figure 6 require further analysis to identify the reasons for such performance, including testing the effectiveness of anomaly detection systems.

4. Discussion

The results of this study indicate a growing interest in AI use in the AML in financial systems. AI-based models show great potential in detecting suspicious transactions, going beyond traditional rule-based systems. They make it possible to identify complex patterns and anomalies in large data volumes. However, certain aspects should be taken into account when analyzing our findings.

According to the studies by Bertrand *et al.* (2020, 2021), there are doubts about the compatibility of AI in the fight against money laundering with human rights. Our results do not fully refute these concerns. The use of

AI raises concerns about data privacy and possible bias. Although our algorithms are effective at marking suspicious transactions, there is a risk of privacy rights violation. Bertrand *et al.* (2020) noted that these systems may conflict with the personal data protection provided by the General Data Protection Regulation (GDPR). However, explainable AI (XAI) in our model offers a more transparent approach that partially solves these problems. Abrahamyan (2023) drew attention to money laundering risks through international financial transactions. Our research supports this view, showing that AI can detect illegal transactions in the banking sector and specific industries, such as the financing of sporting events. Unlike Abrahamyan (2023), we demonstrate a more targeted approach to monitoring such risk areas.

Hayble-Gomes (2022) focused on predictive modeling for Suspicious Activity Reports (SAR). We improved this approach using deep learning (DL) techniques that improve detection accuracy. However, this also needs to be improved in interpreting the results, a problem that Hayble-Gomes also raised. Our research shows the importance of a balance between accuracy and transparency to ensure the reliability of processes. Fritz-Morgenthal *et al.* (2022) emphasized the importance of AI transparency for financial risks. Our results support this view, showing that implementing XAI increases trust in AI systems. We also focused on the accuracy of money laundering detection. Kute *et al.* (2021) emphasized the need for transparent AI models to combat money laundering. Our study demonstrates the practical use of XAI in real systems, although transparency remains a challenge that requires further improvement. Ashwini and Hussain (2023) noted that AI has increased the efficiency of banking transactions. Our research supports this finding, indicating reduced false positives and improved compliance in AI systems. Turksen *et al.* (2024) considered the legal aspects of using AI to monitor transactions, including the risks of excessive automation without human oversight. Our research supports the need for a hybrid approach where AI systems are complemented by human control. Pavlidis (2023) noted that AI opens up new opportunities in the fight against money laundering. Our results confirm this, emphasizing the need to improve legislation to match technological progress.

Overall, our research confirms that AI significantly improves the detection of suspicious transactions and reduces compliance costs. However, further adaptation of regulatory norms and improvement of explainable AI technologies are critical to addressing privacy and transparency issues. The practical application of the results of this research in financial institutions is to increase the effectiveness of the fight against money laundering with the help of AI. It is also important to improve regulatory compliance procedures. Policymakers can use these findings to develop ethical rules for using AI in the financial sector.

4.1. Limitations

One of the main disadvantages of using AI in AML systems is the high risk of obtaining false positive results. This can lead to inefficient operation and verification of legitimate transactions without reason. Moreover, AI relies on large amounts of data for training, which raises concerns about privacy and compliance with financial regulations in different countries. Implementing such technologies also requires significant technical resources, creating financial difficulties for small companies.

4.2. Recommendations

Financial institutions must implement sophisticated AI models, including DL and ensemble methods. These tools can effectively detect complex transaction data patterns and improve suspicious activity detection. It is important to ensure that AI algorithms are regularly updated and retrained to adapt to changes in money laundering strategies and new regulatory requirements. This will help to maintain the effectiveness and compliance of AML initiatives.

Conclusions

Implementing AI in AML has become a major development in the financial sector. Financial transactions are becoming more complex, and money laundering techniques are becoming more sophisticated, which shows the limitations of traditional detection methods. This research highlights the need to use AI to improve the effectiveness of AML systems, suggesting a shift to more proactive and intelligent approaches to preventing financial crime. The results demonstrate that AI methods for detecting suspicious transactions are significantly superior to traditional methods. ML algorithms and data analysis have demonstrated greater accuracy in detecting potential money laundering, reducing false positives, and increasing AML systems' effectiveness. AI can analyze large data volumes in real-time, allowing faster and more accurate recognition of suspicious patterns and activities, strengthening regulatory measures against financial crimes.

The study's results emphasize the significant impact of AI on the field of AML. Financial institutions can use AI tools to improve transaction monitoring, ensure regulatory compliance, and reduce money laundering risks. AI technologies increase the effectiveness of the fight against money laundering and create a safer and more transparent financial environment. These changes also contribute to increasing confidence in financial systems.

Further research should focus on several important areas to improve the use of AI in AML systems. First, advanced AI techniques such as DLand natural language processing (NLP) must be explored to improve detection capabilities. Second, ethical and privacy issues related to AI-based monitoring of financial transactions should be assessed to ensure the responsible use of the technology. Finally, cross-sector studies that compare the application of AI in different financial settings and legal frameworks can provide valuable insights into best practices and areas for improvement. Continuous innovation and research are critical to maintaining the effectiveness of AI in the fight against financial crimes and adapting to new threats in the financial sphere.

Credit Authorship Contribution Statement

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Declaration of use of generative AI and AI-Assisted technologies

The authors declare that they have not used generative AI and AI-assisted technologies in the writing process before submission.

References

[1] Abrahamyan, L. (2023). Major international competition funding and money laundering risks. *European Journal of Sport Sciences 3*(5): 20–25. DOI: https://doi.org/10.24018/ejsport.2023.3.5.86

[2] Ashwini, and Hussain, A. (2023). Impact of artificial intelligence in banking sector. *REST Journal on Banking Accounting and Business 2*(3): 51–55. DOI: https://doi.org/10.46632/jbab/2/3/7

[3] Bertrand, A., Maxwell, W., and Vamparys, X. (2021). Do AI-based anti-money laundering (AML) systems violate European fundamental rights? *International Data Privacy Law 11*(3): 276–293. DOI:https://doi.org/10.1093/idpl/ipab010

[4] Bertrand, A., Maxwell, W., and Vamparys, X. (2020). Are AI-based anti-money laundering systems compatible with fundamental rights? *SSRN Electronic Journal*. DOI: https://doi.org/10.2139/ssrn.3647420

[5] Buhl, N. (2023). F1 score in machine learning. *Encord.com*. Available at: https://encord.com/blog/f1-score-in-machine-learning/

[6] Dynatrace. (2024). Modern cloud done right. Available at: https://www.dynatrace.com

[7] Fritz-Morgenthal, S., Hein, B., and Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in Artificial Intelligence 5*. DOI: https://doi.org/10.3389/frai.2022.779799

[8] Hayble-Gomes, E. (2022). The use of predictive modeling to identify relevant features for suspicious activity reporting. *Journal of Money Laundering Control, 26*(4). DOI: https://doi.org/10.1108/jmlc-02-2022-0034

[9] Kruhlov, V., Bobos, O., Hnylianska, O., Rossikhin, V., and Kolomiiets, Y. (2024). The role of using artificial intelligence for improving public service provision and fraud prevention. *Pakistan Journal of Criminology 16*(2): 913–928.

[10] Kundu, R. (2022). F1 score in machine learning: Intro & calculation. *Www.v7labs.com*. Available at: https://www.v7labs.com/blog/f1-score-guide

[11] Kute, D. V., Pradhan, B., Shukla, N., and Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering – A critical review. *IEEE Access 9*: 82300–82317. DOI: https://doi.org/10.1109/access.2021.3086230

[12] Lazor, O., Lazor, O., Zubar, I., Zabolotnyi, A., and Yunyk, I. (2024). The impact of digital technologies on ensuring transparency and minimising corruption risks among public authorities. *Deleted Journal 16*(2): 357–374. DOI: https://doi.org/10.62271/pjc.16.2.357.374

[13] Lelyk, L., Olikhovskyi, V., Mahas, N., and Olikhovska, M. (2022). An integrated analysis of enterprise economy security. *Decision Science Letters*, 299–310. DOI: https://doi.org/10.5267/j.dsl.2022.2.003

[14] Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., and Zarosylo, V. O. (2021). Practice of the member states of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime 29*(3): 853–863. DOI: https://doi.org/10.1108/jfc-03-2021-0050

[15] Nikonenko, U., Shtets, T., Kalinin, A., Dorosh, I., and Sokolik, L. (2022). Assessing the policy of attracting investments in the main sectors of the economy in the context of introducing aspects of industry 4.0. *International Journal of Sustainable Development and Planning 17*(2): 497–505. DOI:https://doi.org/10.18280/ijsdp.170214

[16] Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: The dawn of a new era. *Journal of Money Laundering Control 26*(7). DOI: https://doi.org/10.1108/jmlc-03-2023-0050

[17] Ricadela, A. (2024). Anti–Money laundering AI explained. Available at: https://www.oracle.com/financial-services/aml-ai/

[18] Segal, T. (2024). Operational risk: Overview, importance, and examples. Available at: https://www.investopedia.com/terms/o/operational_risk.asp

[19] Simon, and Simon. (2021). Recording business transactions. Available at: https://analystprep.com/cfa-level-1-exam/financial-reporting-and-analysis/recording-business-transactions/

[20] Tamplin, T. (2023). Effects of transactions on a balance sheet. *Finance Strategists*. Available at: https://www.financestrategists.com/accounting/financial-statements/balance-sheet/effects-of-transactions-on-a-balance-sheet/

[21] Turksen, U., Benson, V., and Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing the integrity of AI. *Journal of Banking Regulation, 25*: 359-377. DOI:https://doi.org/10.1057/s41261-024-00233-2

[22] Widyastuti, R., *et al.* (2024). Performance analysis of random forest algorithm in automatic building segmentation with limited data. *ISPRS International Journal of Geo-Information, 13*(7): 235. DOI:https://doi.org/10.3390/ijgi13070235

[23] A Guide to Building a Financial Transaction Anomaly Detector. (2024). Unit8. Available at: https://unit8.com/resources/a-guide-to-building-a-financial-transaction-anomaly-detector/

[24] Financial Crime Academy. (2024). Understanding different types of risks faced by financial institutions. Available at: https://financialcrimeacademy.org/

[25] How to Detect Anomalies in Payment Transactions. (2024). Available at: https://www.unit21.ai/videos/how-to-detect-anomalies-in-payment-transactions

[26] Hyperparameter Tuning Random Forest Pyspark Restackio. (2021). Restack.io. Available at: https://www.restack.io/p/hyperparameter-tuning-answer-random-forest-pyspark-cat-ai

[27] MiniTAB. (2024). Data analysis, statistical & process improvement tools. Available at: https://www.minitab.com/en-us/

[28] Seasonal-Trend Decomposition Using LOESS (STL) - Statsmodels 0.15.0 (+429). (2024). Available at: https://www.statsmodels.org/dev/examples/notebooks/generated/stl_decomposition.html

[29] Strategy and Transactions in Insurance. (2024). https://www.ey.com/en_gl/industries/insurance/transactions

[30] The Many Use Cases for Anomaly Detection in Business Data. (2024). *Eyer.ai*. Available at: https://eyer.ai/blog/the-many-use-cases-for-anomaly-detection-in-business-data/

[31] Transaction Types. (2024). Available at: https://docs.bond.tech/docs/transaction-types

Appendices

Appendix A

Financial transactions data pre-processing procedure

1. Data collection

Purpose: Obtain and verify the integrity of a data set.

Action: Securely receive anonymous transaction data from a financial institution. Check the dataset for completeness and accuracy.

2. Data verification

Purpose: Identify and understand the structure and content of the data set.

Action: Perform initial verification using Python libraries (e.g., Pandas). Check for missing values, data types, and overall structure.

3. Processing of missing values

Purpose: Resolve any missing or null values in the data set.

Action: Apply appropriate imputation methods or remove rows/columns with extra missing values.

4. Data normalization

Purpose: Standardize numerical values to ensure comparability.

Action: Use normalization methods such as min-max scaling or standardization.

5. Coding of categorical variables

Purpose: Convert categorical data into a numerical format suitable for machine learning algorithms.

Action: Use such methods as One-Hot Encoding or Label Encoding.

6. Development of functions

Purpose: Create new features that can improve the performance of the model.

Action: Create additional features based on existing data, such as transaction frequency or average transaction amount per user.

7. Data splitting

Purpose: Split the data set into training and testing sets to evaluate the model performance.

Action: Use a stratified distribution to ensure that each set is representative of the general distribution of the data.

8. Data verification

Purpose: Ensure that processed data meets quality standards.

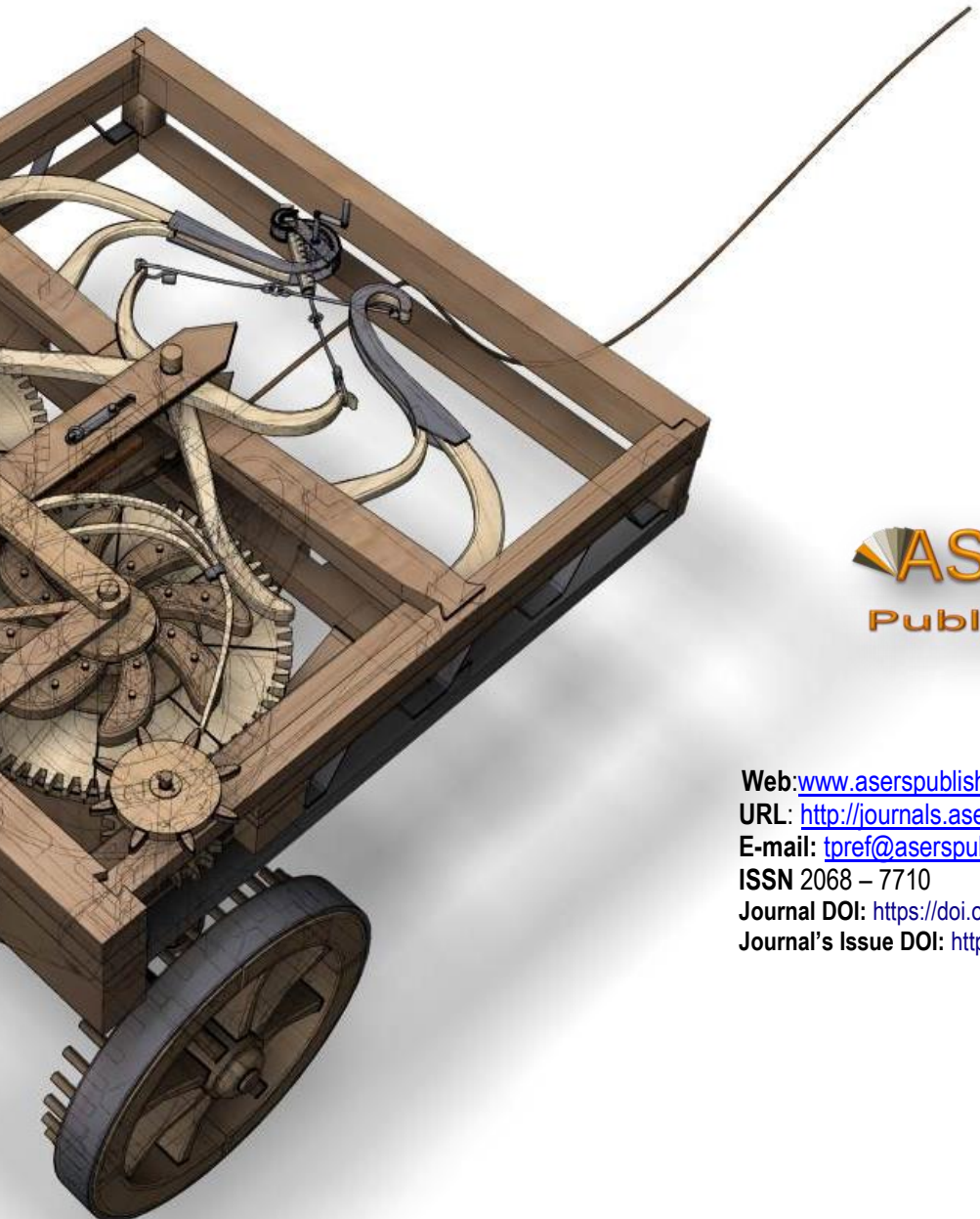
Action: Perform checks to verify that the pre-processing steps have been applied correctly and that the data is ready to train the model.

9. Documentation

Purpose: Document pre-processing steps and solutions for reproducibility.

Action: Record all pre-processing steps, including data imputation techniques, scaling techniques, coding procedures, and splitting strategy.

ASERS



ASERS Publishing

Web:www.aserspublishing.eu
URL: http://journals.aserspublishing.eu/tpref
E-mail: tpref@aserspublishing.eu
ISSN 2068 – 7710
Journal DOI: https://doi.org/10.14505/tpref
Journal's Issue DOI: https://doi.org/10.14505/tpref.v15.4(32).00