**RESEARCH ARTICLE**

**Integrated Machine Learning Algorithms Applied to the Detection of Financial Accounting Fraud, Cases of Peruvian Companies**

Jorge M. Chávez-Díaz¹, Mark Barrueta-Pinto², Manuel Antonio Murillo Luna³, Alejandro Valencia Arias⁴, José L. Arquero⁵

¹,²,³Universidad Peruana de Ciencias Aplicadas
⁴Institución Universitaria ITM, Colombia
⁵Universidad de Sevilla, España

<table>
<thead>
<tr>
<th>ARTICLE INFO</th>
<th>ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received: May 22, 2024</td>
<td>This paper presents the result of the integrated use of three of the main algorithms proposed by the literature for fraud detection: the local outlier factor (LOF), the isolation forest (ISF) and the support vector machine (SVM). The study integrates them and applies them to financial information of Peruvian companies of different sizes (small, medium and large companies). The inductive generalization method is followed, whose level of knowledge is to describe the application of the algorithms described on certain databases. The methodological keys are the data collection, the application of the algorithms and for the evaluation a specialized software and the F1-Score model were used. The results showed that the application of Machine Learning algorithms detect clues for fraud detection, which should be part of a comprehensive procedure library according to the research planning. In addition, the results showed that the algorithms detect more than 50% of anomalies and that materiality thresholds should be considered to refine conclusions. The results promote the improvement of fraud detection and provide the first studies on the subject in Peruvian companies of different sizes through the application of machine learning algorithms. Future work could evaluate other algorithms on different financial accounting information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Outlier Factor</td>
</tr>
<tr>
<td>Isolation Forest</td>
</tr>
<tr>
<td>Forensic accounting</td>
</tr>
<tr>
<td>Fraud detection</td>
</tr>
<tr>
<td>Support vector machine</td>
</tr>
</tbody>
</table>

*Corresponding Author:*
pccajoch@upc.edu.pe

**INTRODUCTION**

Financial fraud is one of the most significant risks facing companies globally. Whether it is inflated expenses, embezzlement, CEO conflicts of interest, false payroll payments, bribes or even tax evasion. The proposed research shows how the use of machine learning helps substantially in the early detection of these malpractices.

This research work incorporates the use of machine learning algorithms applied to various financial accounting information to detect anomalies leading to possible cases of fraud. The proposed algorithms are taken from the conclusions of the latest scientific articles published (obtained from the Scopus database) and constitute basic knowledge that the forensic accountant (chartered accountant) should consider for their work in today’s competitive, technological, and digital industry such as Industry 4.0.
It is of great importance that the use of the proposed algorithms be incorporated into the training of forensic accountants to apply them to the multiple fields in which they find databases to be examined. The conclusions of this work will allow the implementation of machine learning routines in the day-to-day work of forensic accountants, whether at the labor, financial, tax or even in the expertise of the various fiscal and judicial processes.

Some works have been identified on the application of ML algorithms in financial transactions with F1-Score higher than 95% (Dávila-Morán et al., 2023) and LOF and ISF applications that show positive results in the detection of fraud on financial information (Vijayakumar et al., 2020). Research of this type will continue to be produced given the business needs to achieve sustainability and even more important in contexts of high perception of corruption (Chávez-Díaz et al., 2023).

As a result of the theoretical contributions, the following three research questions are presented:

(Q1) What are the results obtained in the application of combined Machine Learning (ML) algorithms for fraud detection?

(Q2) How to implement the findings obtained by application of combined ML algorithms with forensic fraud detection procedures?

(Q3) What is the degree of reliability of the results obtained in the application of combined ML algorithms for fraud detection?

To answer research questions Q1 and Q2, machine learning algorithms will be run on the proposed databases, so that the performance will be evaluated according to the size of the database. Regarding research question Q3, simulations will be performed and the results obtained will be measured with the F1-Score.

THEORETICAL FRAMEWORK

Fraud

According to the Association of Certified Fraud Examiners (ACFE) (2020) fraud is conceptualized in one of three ways: as misappropriation or misappropriation of an entity's resources; the second, corporate, which relates to fraudulent reporting; and the third, identified with corruption. And fraud detection is defined as the applied knowledge-intensive activities that are executed to prevent financial resources from being obtained through non-legal pretexts (Pitchayatheeranart & Phornlaphatrachakorn, 2023).

White-collar crimes refer to fraudulent actions carried out by people of high reputation, with strong personality, with a high orientation to success and achievement of goals, with some traits of psychopathy. These individuals, generally male, could be attractive and with a lot of charisma, such that they gain people's trust. Individuals that generate protection networks, being cultured, and educated, with professional studies and often with good dress and personal appearance (Clavería Navarrete & Carrasco Gallego, 2023).

Forensic Accounting

Forensic accounting is a profession that goes beyond standardized audit approaches to detect and prevent fraud (Afriyie et al., 2023) and is established in first-world countries such as Australia and varies according to different contexts (Al Shbeil et al., 2023). Although the field of forensic accounting is still relatively small compared to other accounting specializations, but there is a great deal of interest in it worldwide (Ozili, 2023).

In times of globalized economy, forensic accounting is an effective tool to detect and prevent fraud (Capraş & Achim, 2023), its use involves applying reliable principles and methods to obtain sufficient facts for prosecution in a court of law (Afriyie et al., 2023).
Forensic Accountant

Forensic accountants play a crucial role in investigating fraud, providing litigation support, performing business valuations, and detecting cybercrime (Al Shbeil et al., 2023). They need to possess skills such as communication, presentation, analytical thinking and objectivity, independence, attention to detail, courtroom procedures, IT skills, among others (Al-Daoud et al., 2023).

Various tools and techniques are used to uncover financial irregularities and include proactive audit, investigation and fraud detection methods (Afriyie et al., 2023). Traditional forensic accounting models focus on behavioral characteristics of executives or use numerical approaches based on financial data. However, more recent models combine big data analytics with psychological intuitions (Honigsberg, 2020).

Customer interviews to gather information in financial fraud cases are widely used techniques (Fico & Walsh, 2023). The skills and attributes of a forensic accountant, as well as the techniques used in forensic accounting, make them an effective tool for detecting and preventing fraud (Capraș & Achim, 2023).

In this regard, data analysis techniques are used to detect financial fraud by applying reliable principles and methods to obtain sufficient facts or data for prosecution (Afriyie et al., 2023). They need extensive knowledge of accounting, law, auditing, internal auditing, business management, psychology, criminal science, and computer technologies, among others (Kılıç, 2020). The use of big data techniques, data analytics and algorithms has improved the effectiveness of fraud inspections (Kılıç, 2020).

Techniques such as data mining and text mining are effective tools for detecting and preventing fraud (Capraș & Achim, 2023). However, data analytics as an effective tool in the fight against fraud is underutilized (Aboud & Robinson, 2022). The intention to adopt forensic accounting practices is influenced by coercive, mimetic, and normative pressures (Habis Alrawashedh, 2023).

Machine Learning

As a fundamental part of Artificial Intelligence, machine learning is a computer program that can automatically learn patterns and trends from historical data without being explicitly programmed by humans (Huang & Wang, 2023).

Machine learning algorithms fall into two categories: supervised and unsupervised learning. Supervised learning uses the program to predict the outcomes of future instances based on historical data. The data must include predefined outcomes based on which the machine learning algorithms can learn and find the correct class. Unsupervised learning algorithms learn normal patterns based on historical data without pre-defined classes (Huang & Wang, 2023).

Machine learning plays an important role in improving the effectiveness of data analysis for forensic accountants in detecting financial fraud (Ayad et al., 2023; Bao et al., 2022; Hu & Sun, 2022; Odia & Akpata, 2020). Machine learning algorithms improve the quality of accounting information by analyzing financial statements and detecting frauds (Ayad et al., 2023).

The use of machine learning in fraud detection is particularly relevant in the context of accounting fraud (Bao et al., 2022). Data science techniques, including machine learning, provide forensic accountants with the ability to extract, analyze, and visualize large volumes of data, allowing them to stay ahead of fraudsters (Odia & Akpata, 2020).

Machine learning is gradually being applied in tasks such as source document review, business transaction analysis, and risk assessment in the accounting and assurance profession (Cho et al., 2020). The use of machine learning in financial fraud detection has shown promising results, with
techniques such as support vector machines, artificial neural networks, and decision trees being commonly used, (Ramírez-Alpízar et al., 2020). These techniques have demonstrated effectiveness in detecting real cases of fraud, with accuracy values ranging from 70% to 99%, (Ramírez-Alpízar et al., 2020).

**Machine learning algorithms in forensic accounting. A brief review**

Recent research has used machine learning algorithms in data analytics to detect financial fraud. However, different approaches can be found in the forensic accounting literature:

<table>
<thead>
<tr>
<th>Algorithm used</th>
<th>Applications</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter-Fitted Automatic Set Learning (FFD-PTEML)</td>
<td>Fraud detection in the financial industry</td>
<td>(Atassi et al., 2024)</td>
</tr>
<tr>
<td>XGboost, LGBM, CatBoost, Random Forest (RF) and Decision Tree (DT).</td>
<td>On customer data privacy in the financial sector.</td>
<td>(Dasari &amp; Kaluri, 2024)</td>
</tr>
<tr>
<td>Quantum Machine Learning Model (QML).</td>
<td>Comparative study with models such as variational quantum classifier (VQC), estimator quantum neural network (QNN) and sampler quantum neural network (QNN Sampler).</td>
<td>(Innan et al., 2024)</td>
</tr>
<tr>
<td>Genetic Algorithm (GA)</td>
<td>Financial fraud in credit card transactions</td>
<td>(Mantena et al., 2024)</td>
</tr>
<tr>
<td>Logistic regression, Naive Bayes, KNN, Perceptron techniques and others.</td>
<td>Combating financial fraud in banking systems. Exploratory analysis.</td>
<td>(Moreira et al., 2022)</td>
</tr>
<tr>
<td>Support Vector Machines (SVM), artificial neural networks and decision trees.</td>
<td>Fraud detection in financial statements. Systematic mapping of 67 studies</td>
<td>(Ramírez-Alpízar et al., 2020)</td>
</tr>
<tr>
<td>Random Forest, XGBoost, Naive Bayes, K-Nearest Neighbors and Support Vector Machine</td>
<td>Ongoing fight against financial fraud and provides valuable guidance for future investigative efforts.</td>
<td>(Sinap, 2024)</td>
</tr>
<tr>
<td>Egret Swarm Optimization Algorithm (ESOA) integrated with machine learning method</td>
<td>Development of a fraud detection framework.</td>
<td>(Yi et al., 2023)</td>
</tr>
</tbody>
</table>

**Local Outlier Factor**

Early work indicated that, in many cases, it is more useful to assign each object a degree of outlier. This degree is called the local outlier factor (LOF) of an object. It is local in the sense that the degree depends on how isolated the object is with respect to the surrounding neighborhood. Observations with a high LOF value are anomalous (Stripling et al., 2018).

**Isolation Forest (IForest, ISF)**
Compared to general anomaly identification methods, the IForest algorithm does not require the sample data to fit the characteristics of the Gaussian distribution. Moreover, compared to other methods such as one-class SVM, IForest can capture more complex structural information. Therefore, in system integration, the IForest algorithm becomes our first choice for capturing implicit anomalous transactions. The algorithm first uses decision trees to build forests. Then, a feature is randomly selected and a random partition value between the minimum and maximum value of the selected feature is selected to create an isolated partition. This algorithm demonstrates higher accuracy and reliability in practical applications, which helps to identify and prevent potential asset laundering risks more effectively (Yang et al., 2023).

Support Vector Machine (SVM)
A literature review found that supervised analytical models such as SVM support vector machines can help mitigate threats in the marketplace and prevent millions of dollar losses (Ortíz et al., 2022). SVM is one of the most widely used techniques for financial statement fraud detection, with studies showing high effectiveness and accuracy rates ranging from 70% to 99.9% (Ramírez-Alpízar et al., 2020).

SVM has also been used in combination with other models, such as the M-S kernel and the Z-S kernel, to accurately predict financial statement fraud (Phong et al., 2022). In addition, SVM has been used to detect financial reporting fraud, which has yielded high accuracy rates (Chi et al., 2019). Several authors argue that SVM is a valuable tool for identifying patterns of financial fraud in forensic accounting (Chi et al., 2019; Ortíz et al., 2022; Phong et al., 2022; Ramírez-Alpízar et al., 2020).

Integration or combination of algorithms
Isolation Forest is only sensitive to global outliers and is weak in dealing with local outliers. Although LOF performs well in detecting local outliers, it has high time complexity. Therefore, there are studies showing that the joint application of Local Outlier Factor and Isolation Forest can significantly improve the outlier detection rate and greatly reduce the time complexity (Cheng et al., 2019).

The results considered anomalies are:

a) Upper limit exceptions, referring to the highest values above a given threshold.

b) Lower limit exceptions, where the lowest values of the group are identified.

c) Unicorn alert, identifies a single value with the highest anomaly and

d) Others, where values whose distance to other values is significant are included.

METHOD
The inductive generalization method is followed, whose level of knowledge is to describe the application of machine learning algorithms on a selected set of relevant databases, then classify the characteristics, identify irregularities and, therefore, project the directions of implementation of their results in the audit and forensic accounting processes.

The key aspects of the methodology are the collection and preparation of data, which were obtained from companies of different sizes as measured by revenue level. They were then subjected to the Local Outlier Factor, Isolation Forest and Support Vector Machine algorithms separately in a preparatory manner, and then applied together. Finally, for performance evaluation purposes, specialized software that follows the F1-Score model was used to measure fraud detection performance.

Databases used
Four databases were used for the work. The first one referred to the information of the purchase records of an SME company by monthly period in PLE format (Electronic Books Program, defined by the Peruvian Tax Administration - SUNAT), periods 2019 to 2023. The total number of observations was 51 with a total of 2,139 records evaluated. The tests performed were based on Local Outlier Factor (LOF), Isolation Forest (ISF) and Support Vector machine (SVM) analysis on the TP_CDP category (type of payment voucher) and the TOTAL numeric field (total amount of the document recorded).

A second group of data refers to savings bank account information of a non-profit organization, periods 2019 to 2020. The total number of observations was 24 with a total of 61,420 records evaluated. The tests performed were based on Local Outlier Factor (LOF), Isolation Forest (ISF) and Support Vector machine (SVM) analyses on the Period category and the numeric fields Charges and Credits.

The third group of data worked on are the class 6 expenses of the Daily Book of a large industrial company, in PLE format (Electronic Book Program, defined by the Peruvian Tax Administration - SUNAT), period 2022. The total number of observations was 12 with a total of 209,190 records evaluated. The tests performed were based on Local Outlier Factor (LOF), Isolation Forest (ISF) and Support Vector machine (SVM) analysis on the “Period” category and the numeric field Debit.

The fourth group of data worked on is the class 6 expenses from the journal of a large industrial company, in PLE format, period 2020. The total number of observations was 12 with a total of 46,512 records evaluated. The tests performed were based on Local Outlier Factor (LOF), Isolation Forest (ISF) and Support Vector machine (SVM) analyses on the “Two-digit accounting account” category and the numeric field Debit. This database will be used to carry out the simulation proposed in the third research question. For which a total of 24 manipulated records will be added.

**Table 2: Basic accounting information for analysis**

<table>
<thead>
<tr>
<th>No.</th>
<th>Entity</th>
<th>Information</th>
<th>Period</th>
<th>Numeric field</th>
<th>Tables</th>
<th>Total, records</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>SME Company</td>
<td>Purchase register</td>
<td>2019-2023</td>
<td>Total</td>
<td>51</td>
<td>2,139</td>
</tr>
<tr>
<td>02</td>
<td>Non-profit organization</td>
<td>Bank statements - savings</td>
<td>2019-2020</td>
<td>Charge and Credit</td>
<td>24</td>
<td>61,420</td>
</tr>
<tr>
<td>03</td>
<td>Industrial company 1</td>
<td>Journal - Class 6</td>
<td>2022</td>
<td>Debit</td>
<td>12</td>
<td>209,190</td>
</tr>
<tr>
<td>04</td>
<td>Industrial company 2</td>
<td>Journal - Class 6</td>
<td>2020</td>
<td>Debit</td>
<td>12</td>
<td>46,512</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>99</td>
<td>319,261</td>
</tr>
</tbody>
</table>

Caseware’s CAAT IDEA analysis tool and its IDEALabs - Anomalies add-on was used. An example of the interactions with the software to point out the categories and the numerical field corresponding to the first group of data are presented in Figure 1, and to set the parameters of the Machine Learning algorithms are shown in Figure 2.

The general statistics were generated in IDEA and the results of the evaluations by table were appended in a general table according to the source of information to be tabulated and finally exported to MS Excel for presentation purposes.
F1-Score
A metric recognized as a standard for measuring fraud detection performance will be used (Dávila-Morán et al., 2023). Based on the confusion matrix shown in Figure 3, formulas are developed to evaluate accuracy, precision, sensitivity, and the F1-Score as a robust conjunction of sensitivity and precision.
RESULTS AND DISCUSSION

First research question - Performance of machine learning algorithms

Entity 1. It was obtained that up to 98% of the monthly records are categorized as normal operations; upper limit exceptions up to 33%; unicorn alert up to 12.5%; lower limit exceptions up to 9% and others up to 12.5%, as presented in Table 3. The monthly records that make up the purchases range from 4 to 93. The number of monthly records exceeds 20 transactions; there are more reference points.  

<table>
<thead>
<tr>
<th>Entity 1</th>
<th>Normal</th>
<th>Outliers: 1</th>
<th>Outliers: 2</th>
<th>Total, general</th>
<th>Range of records per month (times)</th>
<th>Range % max. max. - min.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No comments</td>
<td>51</td>
<td></td>
<td></td>
<td>51</td>
<td>93 - 4</td>
<td>98.46% - 66.67%</td>
</tr>
<tr>
<td>Upper limit exception</td>
<td>35</td>
<td>4</td>
<td>39</td>
<td>2(5) - 1(34)</td>
<td>33.33% - 1.05%</td>
<td></td>
</tr>
<tr>
<td>Unicorn Alert</td>
<td>34</td>
<td>4</td>
<td>38</td>
<td>1(38)</td>
<td>12.5% - 1.05%</td>
<td></td>
</tr>
<tr>
<td>Lower limit exception</td>
<td>7</td>
<td></td>
<td>7</td>
<td>1(7)</td>
<td>9.09% - 1.52%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
<td></td>
<td>4</td>
<td>1(4)</td>
<td>12.5% - 5.56%</td>
<td></td>
</tr>
<tr>
<td>Total, general</td>
<td>51</td>
<td>80</td>
<td>8</td>
<td>139</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Entity 2. It was found that up to 98% of the monthly records are normal operations; the upper limit exceptions are up to 1%. In this case, it is observed that the more records evaluated, the more anomalies detected stabilize around 1% for each type of anomaly, as shown in Table 4

<table>
<thead>
<tr>
<th>Entity 2</th>
<th>Normal</th>
<th>Outliers: 1</th>
<th>Total, general</th>
<th>Records per month max - min</th>
<th>Range perc. % max-min</th>
</tr>
</thead>
<tbody>
<tr>
<td>Another</td>
<td>24</td>
<td>24</td>
<td>54 - 11</td>
<td>1.34% - 1.01%</td>
<td></td>
</tr>
<tr>
<td>Upper limit exception</td>
<td>24</td>
<td>24</td>
<td>45 - 11</td>
<td>1.03% - 0.73%</td>
<td></td>
</tr>
<tr>
<td>No comments</td>
<td>24</td>
<td>24</td>
<td>4843 - 1054</td>
<td>98.03% - 97.91%</td>
<td></td>
</tr>
<tr>
<td>Total, general</td>
<td>24</td>
<td>48</td>
<td>72</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Entity 3. It was obtained that up to 98% of the monthly records are categorized as normal operations; the upper limit exceptions up to 1% and others up to 1.5%, as presented in Table 5.
Table 5: Results in large company 1

<table>
<thead>
<tr>
<th>Entity</th>
<th>Normal</th>
<th>Outliers: 1</th>
<th>Total, general</th>
<th>Records per month max - min</th>
<th>Range perc. % max-min.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No comments</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>18593 - 15404</td>
<td>98.01% - 97.99%</td>
</tr>
<tr>
<td>Upper limit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exception</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>168 - 85</td>
<td>0.93% - 0.51%</td>
</tr>
<tr>
<td>Another</td>
<td>12</td>
<td>12</td>
<td>24</td>
<td>257 - 196</td>
<td>1.48% - 1.08%</td>
</tr>
<tr>
<td>Total, general</td>
<td>12</td>
<td>24</td>
<td>36</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Entity 4. It was obtained that up to 98.54% of the monthly records are categorized as normal operations; upper limit exceptions up to 1.06%; lower limit exceptions up to 0.67%; unicorn alert up to 0.38% and others up to 0.96%, as presented in Table 6.

Table 6: Results in large company 2

<table>
<thead>
<tr>
<th>Entity</th>
<th>Normal</th>
<th>Outliers: 1</th>
<th>Outliers: 2</th>
<th>Total, general</th>
<th>Records per month max - min</th>
<th>Range perc. % max. - min.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper limit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exception</td>
<td>12</td>
<td>1</td>
<td></td>
<td>13</td>
<td>49 - 1</td>
<td>1.06% - 0.03%</td>
</tr>
<tr>
<td>No comments</td>
<td>12</td>
<td></td>
<td></td>
<td>12</td>
<td>5140 - 1483</td>
<td>98.54% - 7.96%</td>
</tr>
<tr>
<td>Another</td>
<td>12</td>
<td></td>
<td></td>
<td>12</td>
<td>49 - 2</td>
<td>0.96% - 0.13%</td>
</tr>
<tr>
<td>Lower limit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exception</td>
<td>11</td>
<td></td>
<td></td>
<td>11</td>
<td>19 - 1</td>
<td>0.67% - 0.03%</td>
</tr>
<tr>
<td>Unicorn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert</td>
<td>5</td>
<td>1</td>
<td></td>
<td>6</td>
<td>15 - 1</td>
<td>0.38% - 0.02%</td>
</tr>
<tr>
<td>Total, general</td>
<td>12</td>
<td>2</td>
<td>40</td>
<td>54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following characteristics can be inferred from the results obtained:

1. Lower limit exceptions. Results were obtained only in one case for evaluations in the Journal - Class 6 (Table 5). The ML algorithms identified transactions with zero amount in the debit field. In the other database of the Journal - Class 6 (Table 4) no results were obtained since the category used was Period and not the two-digit Account.
Thus, it identifies transactions if analysis categories are specified. From the four evaluations performed, it can be concluded that the contribution would not be significant if it follows materiality-oriented procedures.

2. Upper bound exceptions. ML algorithms establish records of larger amounts from a threshold, which is usually around 1% of the records in a table. It is efficient for analyzing information from 20 records onwards. From the evaluations performed, this classification is important because it ensures significant amounts subject to further specific analysis.

3. Unicorn Alert. It only identified records with this type of classification in the case of entity 4 (Table 5). In this case, the two-digit account was considered as a category and the records identified showed a numerical value of zero (account 69).

From the four evaluations carried out, the contribution is not significant.

4. Others. It is observed for all four databases that records with unique unusual values are obtained. It does not distinguish material numerical amounts, i.e., it identifies values of any amount. The larger the database, the more efficient its results will be. This classification could be very useful if a materiality threshold is added in the audit planning or execution of the expertise, to refine the result.

According to the results obtained, the first research question is solved. The Machine Learning algorithms (LOF, ISF, SVM) provide significant results since they detect clues (material and outliers) that allow a deeper analysis in the process of detecting financial accounting fraud. Thus, it corroborates the findings of (Cheng et al., 2019; Vijayakumar et al., 2020).

Second research question.

The findings obtained can be implemented in conjunction with other fraud detection procedures such as the following:

- Benford’s Law of first digit. For the evaluation of fragmentation of expenses, especially in journal entries - Class 6 (Antunes et al., 2023).
- Application of duplicates. For evaluations of invoices recorded in the Purchase Register, Asset IDs or Codes in the Asset Ledger, invoices in the Sales Register, minor provisions in the Journal, etc.
- Application of omissions. For fields with correlative coding characteristics such as journal entry numbers in the Journal or payment voucher numbers in the Sales Register or Warehouse Receipt Parts for Inventories.
- Evaluation of round amounts and zero decimal places. Applied to accruals in the Journal or purchase invoices in the Purchase Register.

Third research question.

Two simulations were carried out. In the first one, records were entered in the database of entity 4, consisting of expenses for the same account and of repetitive high amounts.

The result showed that the manipulated records were not detected by the algorithms. This case
provides clues regarding the nature of the LOF, ISF and SVM algorithms, which detect anomalies, or outliers. With this approach, then, the added records do not constitute outliers and, therefore, the model provides confidence in not detecting false positives. The F1-Score did not show any results, as detailed in Figure 4.

![Figure 4: Result Simulation 1](image)

In a second simulation, 24 records with anomaly characteristics were added to the same database for entity 4. In this case, the model did detect more than 50% of the manipulated records (13 of 24). The F1-Score obtained is 0.029, still low (Figure 5). In this regard, it is explained that the resulting detections correspond to records with non-significant amounts, i.e., without materiality.

![Figure 5: Simulation result 2a](image)

In a variant of simulation 2, for a material analysis, the materiality threshold was established to obtain meaningful results. In this case, it was S/5,000. The result is more in line with the practice of the forensic or expert witness. The F1-Score improved considerably (0.17808). However, a classification ability of 17.8% is far from other studies that obtain an ability of up to 95% (Dávila-Morán et al., 2023). The model may be improved with the joint application of other algorithms in ML.

In this way, the usage model can become more meaningful as usage parameters are established based on the forensic expert’s experience. It should be noted that the recalled detections could be evaluated in a separate sub-process using Benford tests, to close the risk of fragmentation of significant amounts. The model reports a recall of 0.54167, i.e., it continues to detect more than 50% of the manipulated records, as detailed in Figure 6, which in monetary terms means that the entity is reducing the risk of fraud by that percentage.

![Figure 6: Simulation result 2b](image)

**CONCLUSIONS**

This paper presents its results on a multi-algorithmic approach in Machine Learning (LOF, ISF, SVM), which proved to provide a deep analysis of the information that makes it an effective tool in obtaining clues in the detection of financial and accounting fraud. Its efficiency is evidenced as the volume of information is greater and its application is executed on specific categories of information, such as, for example, monthly periods, two-digit accounting account, complete accounting account, cost center, bank account, etc.
For a successful implementation of the algorithms, it is necessary to use it in conjunction with other fraud detection procedures, and to add some parameters that the experience of the auditor or expert advises.

Initial research looked ahead to further research into a multi-algorithmic approach that would allow for the classification and evaluation of large datasets (Wheeler & Aitken, 2000). Therefore, further research is recommended to analyze other algorithms such as Bayesian Networks or others that engineering and data science recommend in fraud detection applied to the field of business, management, and accounting.

**FUNDING:** Research Direction of the Universidad Peruana de Ciencias Aplicadas. Code: A-046-2024.

**CONFLICT OF INTEREST:** The authors declare no conflict of interest.

**REFERENCES**


Capraș, I. L., & Achim, M. V. (2023a). An Overview of Forensic Accounting and Its Effectiveness in the


