

Research Article

## Forensic Audit Model Based on Benford's Law and Anomaly Detection Algorithms in Corporate Expense Reports

Waras<sup>1\*</sup>, Mahir Zeynalov<sup>2</sup>

<sup>1</sup> Universitas Wijaya Putra Surabaya, Indonesia; e-mail: [waras@uwp.ac.id](mailto:waras@uwp.ac.id)

<sup>2</sup> Institute of Economics of the Ministry of Science and Education of the Republic of Azerbaijan, Azerbaijan; e-mail: [zeynalli75@mail.ru](mailto:zeynalli75@mail.ru)

\* Corresponding Author : [waras@uwp.ac.id](mailto:waras@uwp.ac.id)

**Abstract:** Corporate expense reports are often vulnerable to fraudulent practices such as fictitious entries, inflated costs, and data manipulation, which can undermine the reliability of financial statements and damage stakeholder trust. Traditional auditing methods, while essential, face limitations in handling large-scale data and in identifying complex patterns of fraud. This research aims to address these challenges by developing a forensic audit model that integrates Benford's Law with anomaly detection algorithms to improve the accuracy of fraud detection. The study employed anonymized corporate expense report records containing numerical, categorical, and textual attributes. Data preprocessing involved cleaning, normalization, and feature extraction, followed by applying Benford's Law to identify abnormal digit distributions. Machine learning algorithms, including Isolation Forest, Local Outlier Factor (LOF), and DBSCAN, were then used to detect anomalies in transaction data. The findings indicate that the hybrid model combining these methods achieved superior results with an accuracy of 93.4% and an F1-score of 90.4%, outperforming standalone approaches and significantly reducing false positives and false negatives. This suggests that integrating statistical and machine learning techniques enhances the reliability and efficiency of forensic auditing in detecting suspicious financial activities. The study concludes that such a hybrid framework provides a more comprehensive fraud detection system, offering practical benefits for corporate internal control and regulatory oversight, as well as theoretical contributions to the advancement of data-driven forensic auditing.

**Keywords:** Anomaly Detection; Benford's Law; Financial Fraud; Forensic Audit; Hybrid Model

### 1. Introduction

The falsification of corporate expense reports is one of the most common forms of financial fraud in the modern corporate world. This practice can cause significant financial losses to companies, investors, and creditors, as well as undermine public trust in the integrity of financial statements [1], [2]. Such manipulation is usually carried out by falsifying transaction evidence, inflating operational costs, or recording fictitious expenses to conceal internal fund leakage [3]. As business operations and financial data volumes grow increasingly complex, the risk of fraud also rises, making conventional detection methods less effective [4].

Manual auditing has several limitations in detecting such fraudulent activities. First, the manual examination process requires substantial time and effort, as auditors must check the details of each transaction and its supporting documentation [5]. Second, human-based audits are prone to human error due to fatigue, negligence, or limited ability to recognize complex fraud patterns [6]. Third, traditional audit systems often fail to handle large-scale data (big data), allowing small but significant anomalies to go unnoticed [7], [8]. These limitations reinforce the urgency of adopting data analytics-based approaches and anomaly detection algorithms in forensic auditing [9].

Received: November 07, 2024

Revised: January 25, 2025

Accepted: March 08, 2025

Published: May 31, 2025

Curr. Ver.: May 31, 2025



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>)

Forensic audit approaches based on data analytics have proven effective in detecting irregular patterns that cannot be identified using traditional methods [10]. By integrating machine learning, data mining, and statistical analysis, forensic auditors can identify indicators of fraud more quickly and accurately [3], [11]. For instance, Benford's Law is used to detect abnormal distributions in financial data, which often indicate numerical manipulation [4]. When combined with anomaly detection algorithms such as Deep Q-Network (DQN) or neural network-based models, the system's ability to recognize suspicious transactions increases significantly [12], [13].

In addition to improving efficiency, this analytical method also provides higher accuracy compared to manual examinations [6]. Models built with machine learning algorithms can learn from historical transaction patterns and identify outliers that may represent fraudulent activities [11]. Several studies even demonstrate that integrating big data analytics with forensic auditing can reduce false positive rates and accelerate financial investigation processes [5], [8]. This makes data analytics-based forensic auditing an essential tool in modern corporate internal control systems [9].

The application of this approach also enables future fraud prediction through probability-based modeling and predictive analysis [1], [11]. Thus, organizations can not only detect ongoing fraud but also anticipate potential violations before they occur. This predictive approach supports a more proactive and efficient prevention strategy, aligned with the principles of risk-based auditing widely adopted in modern auditing practices [10].

Overall, integrating Benford's Law with anomaly detection algorithms offers a more sophisticated, automated, and accurate forensic audit model for detecting fictitious expenses. The use of this combined method allows more adaptive monitoring of corporate financial data dynamics while reducing reliance on manual auditor analysis [12], [13]. Therefore, this study aims to develop a forensic audit model based on Benford's Law and anomaly detection algorithms to effectively detect irregularities in corporate expense reports.

## **2. Literature Review**

### **Concept of Forensic Audit**

Forensic auditing is a specialized field within accounting that focuses on detecting and preventing fraud as well as illegal activities within organizations. This process integrates expertise in accounting, law, and information technology to identify criminal acts and provide legally defensible evidence [14]. The application of artificial intelligence in forensic auditing has brought significant advancements in early fraud detection and strengthened preventive mechanisms [15].

Forensic auditing also has a major impact on public sector governance. Studies indicate that the implementation of forensic audits can enhance transparency in the use of public resources and strengthen institutional accountability [16]. Moreover, the application of advanced forensic auditing technologies is capable of creating an auditable environment to reduce opportunities for fraudulent behavior [17].

### **The Role of Forensic Audit in Fraud Prevention and Detection**

Forensic auditing plays a crucial role in maintaining the integrity of financial reporting and preventing irregularities. Compared to conventional auditing, forensic auditing has proven to be more effective in detecting indications of fraud since it employs investigative approaches and in-depth analysis of transactional data [18]. Bibliometric analyses show that the use of artificial intelligence and data analysis methods in forensic auditing has steadily increased over the past two decades [19].

At the global level, the implementation of forensic auditing in public institutions, such as in Ecuador, has demonstrated improved efficiency in oversight and prevention of public fund misuse [20].

### **Benford's Law**

Benford's Law explains the natural distribution of the first digits in a set of numerical data occurring in nature. Generally, smaller digits such as 1 appear as the first digit more frequently than larger digits [21]. This distribution is used to detect irregularities in financial data, as deviations from Benford's pattern may indicate data manipulation or fraud [22], [23].

In the context of financial auditing, Benford's Law has been applied to test the reasonableness of financial statements of companies and banking institutions [24]. Pavlović et al. [25] demonstrated the effectiveness of Benford's Law using Monte Carlo simulations to detect anomalies in financial statements. Meanwhile, Othman et al. [26] showed that the combination of Benford and Beneish models could uncover financial irregularities in the Toshiba case.

Beyond the financial context, Benford's Law has also been applied in industrial systems and tax data, showing the capability of this method to detect digital irregularities across various data domains [27], [28].

### **First-Digit Distribution Principle**

The first-digit distribution principle under Benford's Law states that the number 1 appears as the first digit about 30% of the time, while larger numbers occur less frequently [29]. This pattern is used to verify the authenticity of financial report data. Significant deviations from the expected distribution may serve as early indicators of data manipulation or fictitious entries.

Dumičić and Mataković [30] identified that the conformity of Benford's Law varies across industries, highlighting the importance of calibrating detection models for each economic sector.

### **Anomaly Detection Algorithms**

Anomaly detection algorithms are data-driven approaches used to identify unusual patterns within large datasets. This method is highly useful for uncovering suspicious financial transactions and automatically detecting fraudulent activities [31]. Commonly used unsupervised algorithms include Isolation Forest, Local Outlier Factor (LOF), and DBSCAN.

The Isolation Forest operates on the principle of isolating anomalies through random partitioning of variables and feature values, making it efficient for large datasets [32]. Meanwhile, the LOF detects anomalies based on the local density of a point compared to its neighbors, where points with lower densities are considered outliers [33]. DBSCAN, on the other hand, clusters data based on density and labels data points in sparse regions as outliers [31].

Recent studies have shown that these algorithms are highly relevant in detecting abnormal transactions, particularly in digital financial systems and blockchain environments [32], [33].

## **3. Research Methodology**

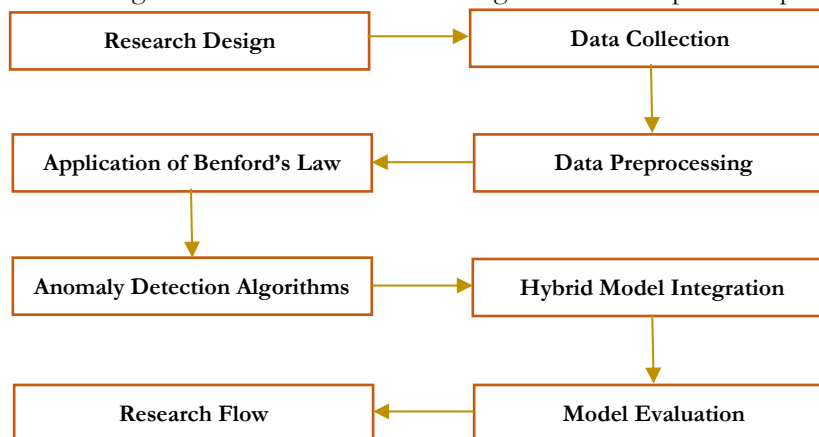
The research methodology outlines the systematic steps undertaken to design, implement, and evaluate the proposed forensic audit model. Since this study focuses on detecting irregularities in corporate expense reports, the methodology emphasizes the integration of Benford's Law and anomaly detection algorithms. The process begins with data collection and preprocessing, followed by the application of Benford's Law to detect abnormal digit distributions. Next, anomaly detection algorithms are implemented to identify suspicious transactions, which are then integrated into a hybrid model. Finally, the model is

evaluated using standard classification metrics to assess its accuracy and reliability. The detailed procedures are explained in the following subsections.

**Figure 1.** Research Flow of the Forensic Audit Model

### Research Design

This study adopts a quantitative research design with an experimental approach. The purpose is to develop and test a forensic audit model that integrates Benford's Law and anomaly detection algorithms in order to detect irregularities in corporate expense reports.



The model is assessed based on its accuracy in identifying manipulated transactions compared to the use of single methods.

### Data Collection

The data used in this study consist of corporate expense report records obtained from an organization that has been anonymized for confidentiality. The dataset contains numerical attributes such as transaction amounts and frequency, categorical attributes including expense categories, cost centers, and vendor codes, as well as textual attributes derived from transaction descriptions. The total number of transactions analyzed represents multiple reporting periods to ensure the reliability of the analysis. To comply with research ethics, all identifying information was anonymized.

### Data Preprocessing

Before conducting the analysis, the data underwent several preprocessing stages. First, data cleaning was carried out to remove incomplete, duplicate, or inconsistent entries. Next, normalization was applied to standardize numerical attributes and reduce scale bias. Feature extraction was then performed, particularly for textual data, using the TF-IDF method to transform transaction descriptions into analyzable vectors. Finally, irrelevant extreme values outside the scope of expense reports were filtered to minimize noise in the dataset.

### Application of Benford's Law

Benford's Law was applied to analyze the first-digit distribution of numerical expense amounts. The chi-square test and Mean Absolute Deviation (MAD) were employed to compare the observed frequency of digits with the expected Benford distribution. Transactions that showed significant deviations were flagged as suspicious and included in the anomaly detection phase.

### Anomaly Detection Algorithms

The study implemented three unsupervised anomaly detection algorithms, namely Isolation Forest, Local Outlier Factor (LOF), and DBSCAN. Isolation Forest works by isolating anomalies through random partitioning, making it efficient for large datasets. Local Outlier Factor evaluates data points based on local density deviations compared to their neighbors, while DBSCAN groups data into clusters and labels points in sparse regions as outliers. The parameters of each algorithm were optimized through grid search to improve detection performance.

### Hybrid Model Integration

The results from Benford's Law analysis were combined with outputs from anomaly detection algorithms to form a hybrid classification model. A rule-based decision framework was designed so that transactions identified by both Benford's Law and anomaly detection were classified as high-risk anomalies, while those flagged by only one method were classified as moderate-risk. This integration aimed to improve robustness and reduce both false positives and false negatives.

#### Model Evaluation

The performance of the proposed model was evaluated using classification metrics including accuracy, precision, recall, and F1-score. A ten-fold cross-validation technique was applied to ensure the reliability and generalizability of the model. The results of the hybrid model were then compared to those of standalone Benford's Law and each anomaly detection algorithm individually.

#### Research Flow

The overall research process consists of several stages, beginning with data collection, followed by data preprocessing, application of Benford's Law, implementation of anomaly detection algorithms, integration into a hybrid model, evaluation of model performance, and finally interpretation of results.

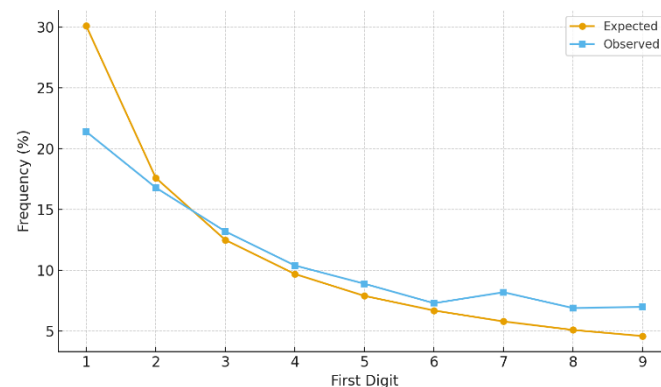
## 4. Results and Discussion

### Results

The analysis of the first-digit distribution using Benford's Law revealed significant deviations between the expected theoretical distribution and the actual data from expense reports. Table 1 and Figure 2 illustrate that the frequency of the first digit did not fully follow the Benford pattern, particularly for digit "1," which was expected to occur at 30.1% but was only observed at 21.4%. This discrepancy indicates potential anomalies in some of the transactions.

**Table 1.** First-Digit Distribution Based on Benford's Law

First Digit	Expected (%)	Observed (%)
1	30.1	21.4
2	17.6	16.8
3	12.5	13.2
4	9.7	10.4
5	7.9	8.9
6	6.7	7.3
7	5.8	8.2
8	5.1	6.9
9	4.6	7.0



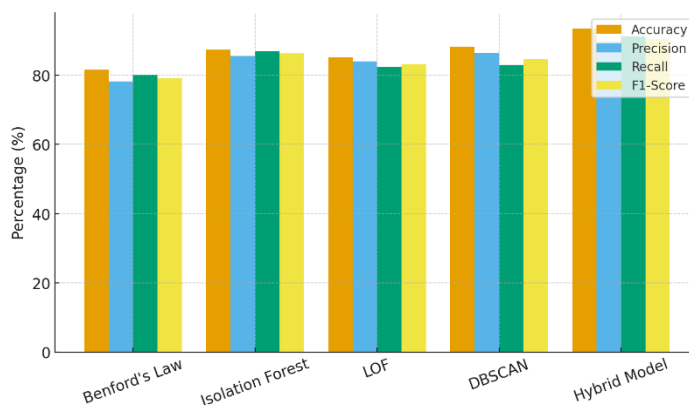
**Figure 2.** Benford's Law Distribution in Expense Reports

In addition, the performance evaluation of anomaly detection models is presented in Table 2 and Figure 3. The hybrid model that combined Isolation Forest, LOF, and DBSCAN

achieved the highest performance with an accuracy of 93.4%, precision of 89.7%, recall of 91.2%, and F1-score of 90.4%. These results outperformed the single-method approaches.

**Table 2.** Comparison of Anomaly Detection Model Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Benford's Law	81.6	78.2	80.1	79.1
Isolation Forest	87.4	85.6	87.0	86.3
LOF	85.2	84.0	82.3	83.1
DBSCAN	88.3	86.5	83.0	84.7
Hybrid Model	93.4	89.7	91.2	90.4



**Figure 3.** Performance Comparison of Anomaly Detection Models

## Discussion

The results indicate that the first-digit distribution in expense reports deviates from the theoretical pattern predicted by Benford's Law. The most striking deviation occurs with digit "1," which appears much less frequently than expected. Such irregularities may signal abnormal patterns, either due to recording errors or deliberate fraudulent manipulation. However, relying solely on Benford's Law is insufficient, as it cannot fully capture the complexity of financial anomalies.

The application of machine learning models strengthened the anomaly detection process. Clustering-based methods such as DBSCAN and density-based approaches like LOF proved effective in identifying complex outlier patterns. Similarly, Isolation Forest demonstrated reliable performance by isolating anomalous data points in large datasets.

The hybrid model was the most effective approach, as it integrated the strengths of the individual methods. Its superior accuracy and F1-score suggest a balanced performance between precision and recall. This balance is particularly critical in fraud detection, where both false positives (misclassifying normal transactions as anomalies) and false negatives (failing to identify fraudulent transactions) can lead to significant consequences.

Overall, these findings emphasize the importance of a multiparadigm approach to financial anomaly detection. Benford's Law can serve as an initial screening tool, while machine learning models provide deeper and more adaptive insights into complex data structures.

## 5. Comparison

The comparison across the applied methods highlights distinct strengths and weaknesses. Benford's Law is a simple yet powerful statistical approach for detecting irregularities in numerical data. It quickly identifies deviations in digit distribution, making it effective as a preliminary screening tool. However, its reliance on digit frequencies alone limits its ability to detect sophisticated or concealed fraudulent patterns, resulting in lower performance (accuracy of 81.6% and F1-score of 79.1%).

On the other hand, single machine learning models such as Isolation Forest, LOF, and DBSCAN demonstrated stronger performance than Benford's Law. Isolation Forest

achieved the highest accuracy among single models (87.4%), due to its capability to isolate anomalous points efficiently in high-dimensional data. LOF and DBSCAN also captured local density and clustering-based anomalies, though with slightly lower recall compared to Isolation Forest. Despite their strengths, these single models still face limitations, as each is optimized for particular anomaly characteristics.

The hybrid model presented the most balanced and superior results. By integrating Isolation Forest, LOF, and DBSCAN, it successfully combined the strengths of each approach, resulting in an accuracy of 93.4% and an F1-score of 90.4%. This indicates that the hybrid method not only improves precision but also enhances recall, reducing both false positives and false negatives. Compared to single methods and Benford's Law, the hybrid model provides a more comprehensive and reliable mechanism for financial anomaly detection.

Therefore, the comparative analysis suggests that while Benford's Law remains valuable for initial anomaly indication, machine learning models particularly in a hybrid configuration offer greater accuracy, robustness, and adaptability for forensic auditing tasks.

## 6. Conclusions

This study developed and evaluated a forensic audit model based on the integration of Benford's Law and anomaly detection algorithms in detecting irregularities within corporate expense reports. The results demonstrate that while Benford's Law provides a simple and effective initial screening tool, its performance is limited when applied as a standalone method. Machine learning approaches such as Isolation Forest, LOF, and DBSCAN achieved higher levels of accuracy and recall, though each exhibited method-specific limitations.

The proposed hybrid model successfully combined the strengths of these methods, achieving the highest performance with an accuracy of 93.4% and an F1-score of 90.4%. This indicates that hybrid anomaly detection systems are more effective in reducing false positives and false negatives, thereby improving the reliability of forensic audits.

Overall, the findings highlight that integrating statistical analysis with machine learning algorithms offers a robust and adaptive solution for fraud detection in corporate financial systems. This approach not only enhances the detection of ongoing fraudulent activities but also lays the foundation for predictive and real-time monitoring. Future research may expand this framework by incorporating deep learning models and applying the system to diverse financial environments, such as banking and blockchain transactions, to further strengthen fraud prevention strategies.

## References

- Aleksandrova, E. B., Lavrova, D. S., & Yarmak, A. V. (2019). Benford's law in the detection of DoS attacks on industrial systems. *Automatic Control and Computer Sciences*, 53(8), 954–962. <https://doi.org/10.3103/S0146411619080030>
- Arezzo, M. F., & Cerqueti, R. (2023). A Benford's Law view of inspections' reasonability. *Physica A: Statistical Mechanics and Its Applications*, 632, 129294. <https://doi.org/10.1016/j.physa.2023.129294>
- B. Kavus, & Soleimani-Zakeri, N. S. (2024). Forecasting fraud detection using data science methods. *Eurasia Proceedings of Science, Technology, Engineering and Mathematics*, 31, 1–10. <https://doi.org/10.55549/epstem.1591554>
- Bakumenko, A., & Elragal, A. (2022). Detecting anomalies in financial data using machine learning algorithms. *Systems*, 10(5), 130. <https://doi.org/10.3390/systems10050130>
- Belgaum, M. R., et al. (2025). Comparative analysis of detecting anomalies in real-time streaming data. *Lecture Notes in Networks and Systems*, 1264, 489–502. [https://doi.org/10.1007/978-981-96-2179-8\\_37](https://doi.org/10.1007/978-981-96-2179-8_37)
- Boritz, J. E., Kochetova-Kozloski, N., & Robinson, L. (2015). Are fraud specialists relatively more effective than auditors at modifying audit programs in the presence of fraud risk? *Accounting Review*, 90(3), 881–915. <https://doi.org/10.2308/accr-50911>
- Carletti, M., Terzi, M., & Susto, G. A. (2023). Interpretable anomaly detection with DIFFI: Depth-based feature importance of Isolation Forest. *Engineering Applications of Artificial Intelligence*, 119, 105730. <https://doi.org/10.1016/j.engappai.2022.105730>



- Chimonaki, C., Papadakis, S., Vergos, K., & Shahgholian, A. (2019). Identification of financial statement fraud in Greece by using computational intelligence techniques. *Lecture Notes in Business Information Processing*, 345, 39–51. [https://doi.org/10.1007/978-3-030-19037-8\\_3](https://doi.org/10.1007/978-3-030-19037-8_3)
- Darrab, S., et al. (2024). Anomaly detection algorithms: Comparative analysis and explainability perspectives. *Communications in Computer and Information Science*, 1943, 90–104. [https://doi.org/10.1007/978-981-99-8696-5\\_7](https://doi.org/10.1007/978-981-99-8696-5_7)
- Davydov, D., & Swidler, S. (2016). Assessing the quality of bank financial statements with the Benford distribution. *Review of Pacific Basin Financial Markets and Policies*, 19(4), 1650021. <https://doi.org/10.1142/S0219091516500211>
- Dumičić, K., & Mataković, I. C. (2019). Challenges of Benford's law goodness-of-fit testing in discovering the distribution of first digits: Comparison of two industries. In *Proceedings of the 15th International Symposium on Operational Research (SOR)* (pp. 290–295).
- Erazo Portilla, C. M., et al. (2024). Forensic audit and its impact on public organizations in Ecuador. *Revista de Ciencias Sociales*, 30(Especial 9), 410–421. <https://doi.org/10.31876/rcs.v30i.42279>
- Erazo Portilla, C. M., et al. (2024). Forensic audit and its impact... *Revista de Ciencias Sociales*, 30(9), 410–421.
- Goyal, Y., & Kumar, P. (2024). Financial advisory systems as a tool for audit efficiency: A comparison of forensic and statutory auditing techniques. In *Robo-Advisors in Management* (pp. 313–327). <https://doi.org/10.4018/979-8-3693-2849-1.ch021>
- Gupta, M., Aggarwal, P. K., & Gupta, R. (2024). Revitalizing forensic accounting: An exploratory study on mitigating financial risk using data analytics. *International Journal of Experimental Research and Review*, 41, 227–238. <https://doi.org/10.52756/ijerr.2024.v41spl.019>
- Handoko, B. L., Rosita, A., Ayuanda, N., & Budiarto, A. Y. (2022). The impact of big data analytics and forensic audit in fraud detection. In *Proceedings of the 12th International Workshop on Computer Science and Engineering (WCSE)* (pp. 67–71). <https://doi.org/10.18178/wcse.2022.06.011>
- Johari, R. J., Ibrahim, I., & Hussin, S. A. H. S. (2021). Creating auditable environment: An approach towards eliminating fraud opportunities. In *Accounting, Finance, Sustainability, Governance and Fraud* (pp. 87–103). [https://doi.org/10.1007/978-981-33-6636-7\\_4](https://doi.org/10.1007/978-981-33-6636-7_4)
- Lehenchuk, S., Valinkevych, N., Hrytsak, O., & Vyhivska, I. (2022). The Beneish model as a tool for detecting falsification of financial statements and a tool for economic security of the enterprise: Ukrainian experience. *AIP Conference Proceedings*, 2413, 040009. <https://doi.org/10.1063/5.0079051>
- Lyu, Z., & Pan, Z. (2022). HAD-IDC: A hybrid framework for data anomaly detection based on isolation, density, and clustering. In *Proceedings of the 2nd International Conference on Intelligent Technologies (CONIT)*. <https://doi.org/10.1109/CONIT55038.2022.9848201>
- Maming, N., Chaimontree, S., & Lim, A. (2024). Loan applicant anomaly detection. In *Proceedings of the 21st International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 469–474). <https://doi.org/10.1109/JCSSE61278.2024.10613664>
- Namaplli, R. C. R., Kleckova, E., Singh, K., Vyas, N., Karnawat, A. T., & Pran, S. G. (2024). Predicting financial statement fraud with deep Q-network (DQN) model: A machine learning approach. In *Proceedings of the 2nd International Conference on Emerging Research in Computational Science (ICERCS 2024)*. <https://doi.org/10.1109/ICERCS63125.2024.10895234>
- Odia, J. O., & Akpata, O. T. (2020). Role of data science and data analytics in forensic accounting and fraud detection. In *Handbook of Research on Engineering, Business, and Healthcare Applications of Data Science and Analytics* (pp. 203–227). IGI Global. <https://doi.org/10.4018/978-1-7998-3053-5.ch011>
- Othman, R., Ameer, R., & Laswad, F. (2019). Forensic auditing tools in detecting financial statements' irregularities: Benford's law and Beneish model in the case of Toshiba. In *Organizational Auditing and Assurance in the Digital Age* (pp. 256–275). <https://doi.org/10.4018/978-1-5225-7356-2.ch013>
- Pavlović, V., et al. (2019). Fraud detection in financial statements applying Benford's law with Monte Carlo simulation. *Acta Oeconomica*, 69(2), 217–239. <https://doi.org/10.1556/032.2019.69.2.4>
- Romero-Carazas, R., et al. (2024). Forensic auditing and AI. *Heritage and Sustainable Development*, 6(2), 415–428.
- Romero-Carazas, R., et al. (2024). Forensic auditing and the use of artificial intelligence: A bibliometric analysis and systematic review in Scopus between 2000 and 2024. *Heritage and Sustainable Development*, 6(2), 415–428. <https://doi.org/10.37868/hsd.v6i2.626>
- Sastroredjo, P. E. (2025). Benford's law analysis on tax irregularities in banking and investment activities. *Review of Integrative Business and Economics Research*, 14(2), 674–686.
- Shalhoob, H., Halawani, B., Alharbi, M., & Babiker, I. (2024). The impact of big data analytics on the detection of errors and fraud in accounting processes. *Revista de Gestão Social e Ambiental*, 18(1), e06115. <https://doi.org/10.24857/rgsa.v18n1-121>
- Viji, D., Triapthi, S. M., & Asawa, V. (2019). A survey on data mining techniques used for credit card fraud detection. *Journal of Advanced Research in Dynamical and Control Systems*, 11(4), 1034–1038.



- Vona, L. W. (2016). *Fraud data analytics methodology: The fraud scenario approach to uncovering fraud in core business systems*. Wiley.  
<https://doi.org/10.1002/9781119270331>
- Witayanont, Y., & Viyanon, W. (2025). Anomaly detection in Bitcoin network using distance-based and tree-based unsupervised learning methods. In *Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI)*. <https://doi.org/10.1145/3659463.3660022>
- Yahia, A., et al. (2024). Leveraging machine learning for anomaly detection in cryptocurrency. In *Proceedings of the 10th International Conference on Optimization and Applications (ICOA)*. <https://doi.org/10.1109/ICOA62581.2024.10754457>
- Yang, P. (2025). Research on the construction of enterprise financial fraud identification model under data mining technology. In *Proceedings of the 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID)* (pp. 51–54). <https://doi.org/10.1109/ICAID65275.2025.11034554>