Journal of
Information System and Technology Auditing

Research Paper

Anomaly Detection in Information Technology Auditing Using Risk-Based Pseudo-Labels and the Random Forest Algorithm [1]

Mohammad Reza Keyvanpour [*2], Ghazaleh Kakavand Teimoory[3], Maryam Ghaebi[4], Negar Naghdian[5], Mahsa Bashavard[6] , Zahra Mohammadinejad[7] and Seyede Nazanin Neishaboorinejad[8]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 1, No. 2, Autumn & Winter 2025 - 2026
pp. 26-33

Received: 2026.01.05
Revised: 2026.02.14
Accepted: 2026.12.06

1. Introduction

Information Technology (IT) auditing is a systematic and independent process aimed at evaluating IT controls, data, processes, and infrastructures in order to ensure the accuracy, integrity, security, reliability, and alignment of information systems with organizational objectives (Dzuranin & Mălăescu, 2016). This concept is also defined within established standards such as ITIL and ISO, which describe auditing as a formal and documented process

[1] https://doi.org/10.22034/JISTA. 2026.570638.1080
[2] Professor, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. (Corresponding Author). Email: keyvanpour@alzahra.ac.ir
[3] M. Sc. Graduated, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: gh.kakavandteimoory@gmail.com
[4] M. Sc. Student, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: m.ghaebi@student.alzahra.ac.ir
[5] M. Sc. Student, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: naghdian.negar@gmail.com
[6] PhD Student, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: m.bashavard@alzahra.ac.ir
[7] M. Sc. Student, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: zahra.mohamadinjd@gmail.com
[8] M. Sc. Student, Data Mining Laboratory, Department of Computer Engineering Faculty of Engineering, Alzahra University Tehran, Iran. Email: nazanin.bul@gmail.com

for assessing compliance with standards, accuracy of records, and operational effectiveness. Although auditing has traditionally been associated with financial auditing, IT auditing has emerged as a critical subfield in modern organizations (Gantz, 2013). The rapid growth of data volumes, increasing technological complexity, and limitations in human auditing resources have significantly expanded the scope of IT auditing. In response, machine learning–based anomaly detection has been introduced as an effective approach to support IT audit activities (de Vries, 2022). Anomaly detection focuses on identifying patterns in data that deviate from expected behavior and may indicate errors, fraud, or security threats (Chacko et al., 2012; Quinn & Strauss, 2018). Its application in IT auditing has been shown to improve audit accuracy and quality while reducing manual and repetitive tasks (Rahmani et al., 2025). Anomalies in auditing are inherently cross-domain in nature. In financial auditing, anomalies typically manifest as fraud or material misstatements in financial data. In contrast, cybersecurity auditing anomalies are more commonly associated with unauthorized access, system intrusions, and abnormal user or system behavior, which may indirectly lead to financial and reputational risks (Hasan & Ahmed, 2025). Despite its advantages, implementing anomaly detection in IT auditing remains challenging due to the relatively smaller data volumes and the unstructured nature of IT audit data compared to financial data. Consequently, selecting appropriate detection methods and focusing on critical audit processes are essential for the effective application of this approach.

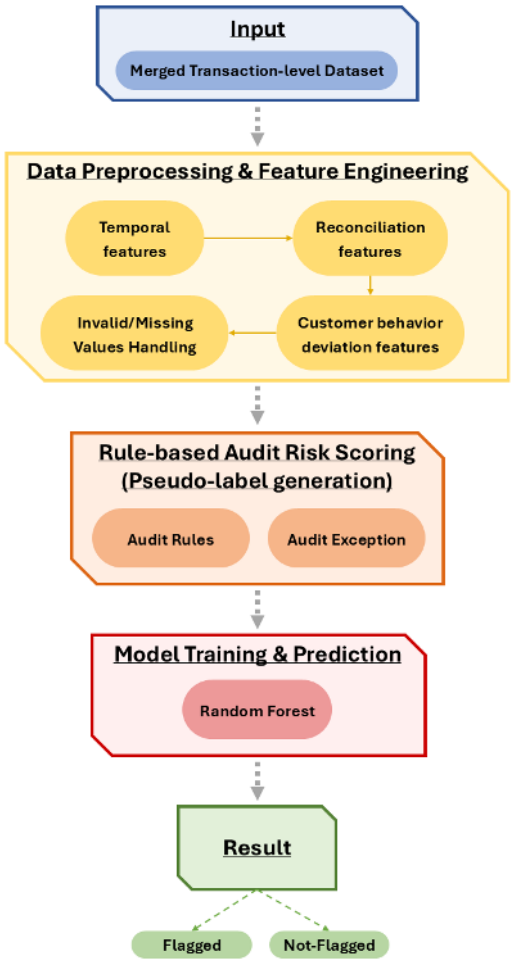
2. MATERIALS AND METHODS

Due to the sensitive and confidential nature of financial data and the associated legal and security constraints, direct access to real-world audit and anomaly detection datasets is generally not available to researchers. Therefore, in line with many prior studies, this research employs a synthetic yet realistic dataset designed based on statistical and behavioral patterns observed in real financial

scenarios. This approach preserves data confidentiality while enabling a reliable evaluation of the proposed model's performance.

The proposed methodology is based on a machine learning framework for anomaly detection and risk-based ranking in IT auditing. The input consists of an integrated dataset formed by merging multi-table transactional, customer, and merchant data. After data integration, a structured preprocessing phase is applied, including initial data inspection, time standardization, correction of invalid values, and imputation of missing data. Subsequently, audit-oriented features are engineered in three categories: temporal features to capture irregular transaction timing, consistency features to identify discrepancies between system-recorded transaction amounts, and customer behavior deviation features to quantify how abnormal a transaction is relative to a customer's typical behavior.

Because reliable anomaly labels are often unavailable or incomplete in real audit environments, a rule-based pseudo-labeling strategy is employed. An audit risk score is computed using a set of weighted, data-driven audit rules, and transactions in the top decile of the risk score distribution are labeled as audit exceptions. This design closely reflects real audit practices, where limited investigative resources necessitate prioritizing high-risk cases. A Random Forest classifier is then trained to predict the pseudo-label (AuditException) using the engineered feature set. To ensure generalization, the dataset is split into training and testing subsets using a stratified 70/30 ratio. The trained model produces a risk probability score for each transaction, which is used to rank transactions in descending order of risk. The final output is a Top-K list (top 5% of transactions), providing auditors with a prioritized set of high-risk anomalies for further manual investigation.



Proposed method diagram for identifying anomalies and prioritizing high-risk cases in IT auditing

3. RESULTS AND DISCUSSION

In this section, the performance of the proposed method is evaluated using an integrated dataset comprising 1,000 transactions described by 25 features. Analysis of the audit risk score distribution indicates a highly imbalanced dataset, with more than 90% of transactions classified as low-risk, highlighting the need for robust evaluation metrics beyond accuracy alone.

Model performance is assessed separately on the training and test sets using accuracy, precision, recall, and F1-score. On the training set, the proposed approach achieves an accuracy of 98.29%, with a precision of 89.19%, recall of 94.29%, and an F1-score of 91.67%, indicating effective learning of underlying risk patterns. On the unseen test set, the model maintains strong and stable performance, achieving an accuracy of 97.67%, precision of 84.85%, recall of 93.33%, and an F1-score of 88.89%. The close alignment between training and test results demonstrates good generalization capability and suggests no evidence of overfitting.

The relatively higher recall compared to precision reflects a deliberate trade-off suitable for IT auditing scenarios, where minimizing missed high-risk transactions is prioritized over reducing false alarms. Feature importance analysis further reveals that temporal attributes and customer-level transaction amount deviation are among the most influential factors in anomaly detection. Overall, these results confirm that the combination of targeted feature engineering and a Random Forest classifier provides a robust, reliable, and practical solution for anomaly detection in intelligent IT auditing systems.

4. CONCLUSION

This study presents a machine learning–based anomaly detection approach for IT auditing that addresses the growing complexity and volume of audit data. Through structured preprocessing and targeted feature engineering, the method identifies high-risk transactions based on temporal irregularities, system inconsistencies, and behavioral deviations. Using rule-based pseudo-labeling and a Random Forest model, the approach achieves robust performance with about 97.67% accuracy and an F1-score above 88.89%, even under class imbalance. Future work will focus on real-world validation, improved interpretability, and better handling of imbalanced data.

Keywords: Anomaly Detection, Information Technology Auditing, Machine Learning, Random Forest, Risk-Based Pseudo-Labeling

JEL classification: *M42, M15, C38, D81*

References

Ahmadi, S.J., Faghani Makarani, K., & Fazeli, N. (2024). Data mining techniques and financial statement fraud prediction. *Journal of Management Accounting and Auditing Knowledge*, *13*(52), 15–28. https://www.iaaaas.com/article_223291.html (in Persian)

Alsalmi, E., Alhuzali, A., & Alhothali, A. (2025). Log-based anomaly detection of system logs using graph neural network. *Computers, Materials and Continua*, *86*(2), 1–20.

Bagherian Kasegari, A., Raeisi Vanani, I., Amiri, M., & Homayoun, S. (2024). Detection of financial fraud in public companies using financial and non-financial criteria with a machine learning approach. *Intelligent Business Management Studies*, *13*(50), 99–142. https://ims.atu.ac.ir/article_18048.html (in Persian)

Chacko, N., Ravichandaran, M., Rao, R., & Chandra Shenoi, S. (2012). An anomalous cooling event observed in the Bay of Bengal during June 2009. *Ocean Dynamics*, *62*(5), 671–681.

Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint*, arXiv:1901.03407.

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*.

De la Cruz Cabello, M., Sales, T., & Machado, M. (2025). AIOps for log anomaly detection in the era of LLMs: A systematic literature review. *Intelligent Systems with Applications*, 200608.

De Vries, T. (2022). *Anomaly detection in IT audit: The possibilities and potential in the domain of IT audit* [Master's thesis, University of Turku].

Dzuranin, A. C., & Mălăescu, I. (2016). The current state and future direction of IT audit: Challenges and opportunities. *Journal of Information Systems*, *30*(1), 7–20.

Fazlzadeh, A., Haghighat, J., Pourkian, F., & Ahmadian, V. (2019). Testing the performance of the random forest algorithm and the deep neural network algorithm in a statistical arbitrage strategy. *Financial Engineering and Securities Management*, *10*(40), 349–364. https://sid.ir/paper/197626/fa (in Persian)

Gantz, S. D. (2013). The basics of IT audit: Purposes, processes, and practical information. *Elsevier*.

Hasan, M. T., & Ahmed, I. (2025). AI-driven anomaly detection for data loss prevention and security assurance in electronic health records. *Review of Applied Science and Technology*, *4*(3), 35–67.

Hilal, W., Gadsden, S., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, 116429.

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, *5*(1), 314. (in Persian)

Kakavand Teimoory, G., Keyvanpour, M. R., & Ghaebi, M. (2025). Explainable diabetes prediction via hybrid data preprocessing and ensemble learning. *International Journal of Web Research*, *8*(4), 51–66.

Karimi Far, A., Darabi, R., & Hamidian, M. (2025). Evaluating the efficiency of regression and deep learning approaches in detecting financial statement fraud with a focus on the justification dimension. *Accounting and Auditing Studies*, *15*(3), 241-282. https://journals.alzahra.ac.ir/article_8266.html?lang=en (in Persian)

Kazemi, T., & Piri, M. (2022). Predicting financial reporting fraud schemes using a multi-class machine learning approach. *Empirical Research in Accounting*, *12*(4), 255–280. https://jera.alzahra.ac.ir/article_6880.html (in Persian)

Mohan, C. K., & Mehrotra, K. G. (2017). Anomaly detection in banking operations. *IDRBT Journal*, 16.

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*, 122156.

Niu, W., Liao, X., Huang, S., Li, Y., Zhang, X., & Li, B. (2024). A robust wide and deep learning framework for log-based anomaly detection. *Applied Soft Computing, 153*, 111314.

Okolie, S., Amadi, C., Odii, J., Nwokorie, E., & Onyemauche, U. (2025). Anomaly detection in heterogeneous cybersecurity data. *Franklin Open*, 100426.

Patel, T., & Iyer, S. S. (2025). SiaDNN: Siamese deep neural network for anomaly detection in user behavior. *Knowledge-Based Systems*, 113769.

Pinto, S. O. & Sobreiro, V. A. (2022). Literature review: Anomaly detection approaches on digital business financial systems. *Digital Business*, 2(2), 100038.

Quinn, M., & Strauss, E. (2018). *The Routledge companion to accounting information systems*. Routledge.

Rahmani, A., Manavi, S., & Haddadi, N. (2025). Integrating artificial intelligence into auditing: Challenges and benefits. *Systems Auditing and Information Technology*, *1*(1), 1–27. (in Persian)

Rahnamay Roudposhti, F. (2012). Data mining and financial fraud detection. *Knowledge of Accounting and Management Auditing*, *1*(3), 17–33. https://sid.ir/paper/238039/fa (in Persian)

Ram, Murugan & Khamar (2024). AI-driven network anomaly detection for enhanced cybersecurity and performance. *Proceedings of the 9th International Conference on Communication and Electronics Systems (ICCES), IEEE*.

Rezaei Pithenoei, Y., Asghari Shalmani, M., & Deliridehbaneh, H. (2021). Introducing a suitable organizing framework for data mining applications in accounting and auditing: A review of popular techniques for financial data classification. *Journal of Modern Research Approaches in Management and Accounting*, *5*(19), 1507–1525. https://www.majournal.ir/index.php/ma/article/view/1207 (in Persian)

Romney, M. B., Stainbart, P. G., Summers, S. L., & Wood, D. A. (2006). *Accounting information systems*. Prentice Hall.

Soltani, M., Mohammadinejhad, Z., & Mohseni, A. H. (2024). BGP routing algorithm evaluation. *International Conference on Soft Computing*. https://civilica.com/doc/1967023/ (in Persian)

Sun, Y., Keung, J., Yang, Z., Liu, S., & Liao, Y. (2025). SemiSMAC: A semi-supervised framework for log anomaly detection with automated hyperparameter tuning. *Information and Software Technology*, 107869.

Thiprungsri, S., & Vasarhelyi, M. A. (2011). Cluster analysis for anomaly detection in accounting data: An audit approach. *International Journal of Digital Accounting Research*, *11*.

Uchida, H., Tominaga, K., Itai, H., Li, Y., & Nakatoh, Y. (2024). Improving log anomaly detection via spatial pooling: Combining SPClassifier with ensemble method. *Cognitive Robotics*, *4*, 217–227.

Wu, J., Zhang, S., Liu, H., & Yang, W. (2025). AAR-Log: A robust log anomaly detection method resisting adversarial attacks. *Computer Networks*, 111471.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ پژوهشی

تشخیص ناهنجاری در حسابرسی فناوری اطلاعات با استفاده از شبه برچسب‌های مبتنی بر ریسک و الگوریتم جنگل تصادفی [1]

محمدرضا کیوان‌پور [2]، غزاله کاکاوند تیموری [3]، مریم غائبی [4]، نگار نقدیان [5]، مهسا بشاورد [6]، زهرا محمدی‌نژاد [7] و سیده نازنین نیشابوری‌نژاد [8]

نشریه علمی حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال اول، پیاپی۲، پاییز و زمستان ۱۴۰۴
صص۹۲ - ۱۲۶

تاریخ دریافت: ۱۴۰۴/۱۰/۱۵
تاریخ بازنگری: ۱۴۰۴/۱۱/۲۵
تاریخ پذیرش: ۱۴۰۴/۱۲/۰۶

چکیده

با گسترش استفاده از سیستم‌های اطلاعاتی و افزایش حجم و تنوع داده‌های سیستمی، حسابرسی فناوری اطلاعات با چالش‌های جدیدی در شناسایی رفتارهای غیرعادی و پرخطر مواجه شده است. روش‌های سنتی حسابرسی که عمدتاً مبتنی بر بررسی‌های دستی و قواعد ایستا هستند، توانایی محدودی در کشف الگوهای پیچیده و غیرخطی داده‌های امروزی دارند. در این پژوهش، مسئله تشخیص ناهنجاری در حسابرسی فناوری اطلاعات به‌صورت یک طبقه‌بندی دودویی مدل‌سازی شده و یک رویکرد داده‌محور

---

[1] https://doi.org/10.22034/JISTA.2026.570638.1080

[2] استاد، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. (نویسنده مسئول). Email: keyvanpour@alzahra.ac.ir

[3] دانش‌آموخته کارشناسی ارشد مهندسی نرم‌افزار، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: gh.kakavandteimoory@gmail.com

[4] دانشجوی کارشناسی ارشد مهندسی نرم‌افزار، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: m.ghaebi@student.alzahra.ac.ir

[5] دانشجوی کارشناسی ارشد هوش مصنوعی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: naghdian.negar@gmail.com

[6] دانشجوی دکتری، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: m.bashavard@alzahra.ac.ir

[7] دانشجوی کارشناسی ارشد هوش مصنوعی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: zahra.mohamadinjd@gmail.com

[8] دانشجوی کارشناسی ارشد هوش مصنوعی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران. Email: nazanin.bul@gmail.com

مبتنی بر یادگیری ماشین برای شناسایی و اولویت‌بندی موارد پرخطر ارائه می‌شود. در روش پیشنهادی، داده‌های تراکنش، مشتری و پذیرنده یکپارچه شده و پس از پیش‌پردازش ساختاریافته، ویژگی‌های حسابرسی‌محور استخراج می‌گردد؛ از جمله الگوهای زمانی، شاخص‌های مغایرت بین‌سیستمی و انحراف از رفتار معمول مشتری. این پژوهش از مجموعه داده عمومی «IEEE-CIS Fraud Detection» شامل ۱۰۰۰ تراکنش با ۲۵ ویژگی استفاده می‌کند. ویژگی‌ها شامل داده‌های خام تراکنش و مشتری و همچنین شاخص‌های استخراج‌شده مبتنی بر رویکرد حسابرسی مانند الگوهای زمانی و انحراف از رفتار معمول هستند. به‌دلیل محدودیت برچسب‌های واقعی ناهنجاری، یک سازوکار شبه‌برچسب‌گذاری مبتنی بر قواعد حسابرسی و امتیازدهی ریسک طراحی شده و به‌عنوان متغیر هدف برای آموزش مدل جنگل تصادفی به‌کار می‌رود. خروجی مدل یک امتیاز احتمال است که امکان رتبه‌بندی تراکنش‌ها و استخراج موارد پرخطر اولویت‌دار را فراهم می‌کند. نتایج تجربی نشان می‌دهد روش پیشنهادی در مجموعه آزمون به صحت ۹۷٪، دقت ۸۵٪، فراخوانی ۹۳٪ و امتیاز F1 برابر ۸۹٪ دست یافته و می‌تواند به‌عنوان ابزار تصمیم‌یار مؤثر برای پشتیبانی از حسابرسی فناوری اطلاعات استفاده شود.

واژه‌های کلیدی: *تشخیص ناهنجاری، جنگل تصادفی، حسابرسی فناوری اطلاعات، شبه‌برچسب‌گذاری مبتنی بر ریسک، یادگیری ماشین*

طبقه‌بندی موضوعی: *D81،C38،M15،M42*

مقدمه

حسابرسی فناوری اطلاعات[1] فرآیندی نظام‌مند و مستقل است که با هدف ارزیابی، اطمینان‌بخشی و ایجاد ارزش، به بررسی کنترل‌ها، داده‌ها، فرایندها و زیرساخت‌های فناوری اطلاعات سازمان می‌پردازد تا از صحت[2]، یکپارچگی[3]، قابلیت اتکا[4]، امنیت اطلاعات[5]، رعایت الزامات قانونی و مقرراتی و هم‌راستایی سیستم‌های اطلاعاتی[6] با اهداف عملکردی و راهبردی سازمان اطمینان حاصل شود؛ به‌ویژه در محیطی که با افزایش حجم داده‌ها، پیچیدگی

[1] Information Technology (IT) Audit
[2] Accuracy
[3] Integrity
[4] Reliability
[5] Information's Security
[6] Information Systems

فناوری‌های نوظهور و تشدید الزامات نظارتی مواجه است (دزورانین و مالائسکو[1]، ۲۰۱۶). بر اساس تعریف ارائه‌شده در کتابخانه زیرساخت فناوری اطلاعات[2]، حسابرسی به‌عنوان یک فرایند بازرسی و تأیید رسمیت توصیف می‌شود که با هدف بررسی میزان رعایت استانداردها یا مجموعه‌ای از دستورالعمل‌ها، صحت و دقت سوابق و تحقق اهداف بهره‌وری و اثربخشی انجام می‌گیرد. این بدان معناست که کاربران می‌توانند به فناوری اطلاعات برای انجام هدف مورد نظر حسابرسی اعتماد کنند.

سازمان بین‌المللی استانداردسازی[3]، حسابرسی را فرآیند منظم، مستقل و مستندسازی شده برای به‌دست آوردن شواهد حسابرسی و ارزیابی عینی آن‌ها به منظور تعیین میزان تحقق معیارهای حسابرسی توصیف می‌کند. بر این اساس، هر دو چارچوب ITIL و ISO تعریفی از حسابرسی ارائه می‌دهند به‌گونه‌ای که امکان در نظر گرفتن حسابرسی فناوری اطلاعات به‌عنوان یکی از زیرشاخه‌های حسابرسی در چارچوب این استانداردها فراهم می‌شود. با وجود آنکه حسابرسی می‌تواند برای اشاره به حوزه‌ها و زمینه‌های متنوعی به کار رود، این مفهوم در اغلب موارد به‌طور سنتی با حسابرسی مالی[4] مرتبط است (گانتز[5]، ۲۰۱۳).

در کتاب سیستم‌های اطلاعات حسابداری (رامنی و همکاران[6]، ۲۰۰۶) شش هدف اصلی برای حسابرسی سیستم‌های اطلاعاتی در شکل ۱ معرفی شده است. نخست، امنیت کلی اطلاعات و فناوری اطلاعات باید به‌گونه‌ای تضمین شود که از دسترسی، تغییر یا تخریب غیرمجاز محافظت به عمل آید. دوم، فرایند توسعه و تهیه برنامه‌ها باید به‌صورت صحیح و تنها با مجوزهای لازم انجام شود. سوم، اصلاح و تغییر برنامه‌ها باید به‌درستی کنترل و مجاز شوند. چهارم، پردازش کامپیوتری داده‌ها باید از دقت و کامل بودن اطلاعات مهم اطمینان حاصل کند. پنجم، داده‌های منبع باید به‌گونه‌ای کنترل شوند که داده‌های نادرست یا دارای مجوز نامعتبر شناسایی و اصلاح گردند. در نهایت، پرونده‌های داده باید دقیق، کامل و محرمانه نگهداری شوند.

[1] Dzuranin & Mălăescu
[2] Information Technology Infrastructure Library (ITIL)
[3] The International Organization for Standardization (ISO)
[4] Financial auditing
[5] Gantz
[6] Romney et al.

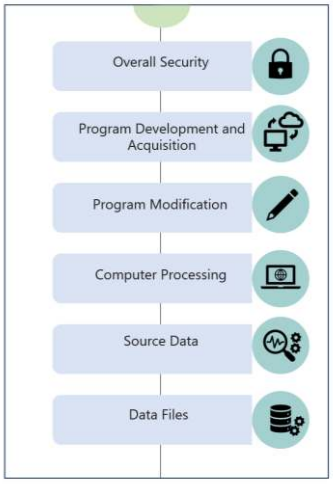


Figure 1. Six objectives for typical information system audits (De Vries, 2022)

شکل ۱. شش هدف برای حسابرسی‌های معمول سیستم‌های اطلاعاتی (دِفریز[1]، ۲۰۲۲)

میزان کار در حسابرسی فناوری اطلاعات در حال افزایش است و رشد تعداد حسابرسان فناوری اطلاعات قادر به همگام شدن با این سرعت نیست. یکی از راه‌حل‌های این مشکل می‌تواند جستجوی فناوری‌های جدیدی باشد که بتوانند از عملکردهای حسابرسی فناوری اطلاعات پشتیبانی کنند. یکی از این موارد، تشخیص ناهنجاری[2] است که توسط الگوریتم یادگیری ماشین[3] ممکن شده است (دِفریز، ۲۰۲۲).

تشخیص ناهنجاری به تازگی به عنوان یک حوزه کلیدی در فرآیند داده کاوی[4] مطرح شده است (کویین و استراوس[5]، ۲۰۱۸) و به مسئله یافتن الگوهای موجود در داده‌ها اشاره دارد که با رفتار مورد انتظار همخوانی ندارند و می‌توانند به عنوان تغییرات اساسی از حالت عادی[6] تعریف شوند. این حالت به نمونه طبیعی مورد انتظار یک فرآیند اشاره دارد، که منجر به داده‌هایی می‌شود که با سایر نمونه‌های همان فرآیند قابل قیاس هستند و به‌عنوان یک رویداد بالقوه

[1] De Vries
[2] Anomaly detection
[3] Machine Learning (ML)
[4] Data mining
[5] Quinn & Strauss
[6] Substantial variations from the norm

مشکوک شناسایی می‌گردد (چاکو و همکاران[1]، ۲۰۱۲) و شناسایی ناهنجاری‌ها در حسابرسی فناوری اطلاعات می‌تواند دقت و کیفیت فرایند حسابرسی را بهبود بخشد و در عین حال، میزان دخالت انسانی در انجام وظایف تکراری را کاهش دهد (رحمانی و همکاران، ۱۴۰۴).

هنگامی که از الگوریتم‌های تشخیص ناهنجاری سخن به میان می‌آید، عموماً منظور به‌کارگیری روش‌های هوش مصنوعی[2]، به‌ویژه الگوریتم‌های یادگیری ماشین، برای شناسایی الگوها و تغییراتی است که از رفتار عادی سیستم انحراف دارند و تشخیص آن‌ها با روش‌های سنتی دشوار است. (موهان و مهروترا[3]، ۲۰۱۷). این ابزار ناپیوستگی‌هایی را مشخص می‌کند که حسابرسان باید برای بررسی بیشتر آنها اقدام کنند. بنابراین کارهای تکراری کاهش یافته و دقت بیشتری در فرآیند ارائه می‌شود (چالاپاتی و چاولا[4]، ۲۰۱۹). دیگر حوزه‌هایی که در آنها شناسایی ناهنجاری مبتنی بر یادگیری ماشین با موفقیت به کار گرفته شده شامل بیمه، مراقبت‌های بهداشتی، بانکداری، مخابرات و کشف تقلب هستند (حسن و احمد[5]، ۲۰۲۵).

ناهنجاری در حسابرسی، مفهومی چندبعدی است و بسته به حوزه کاربرد حسابرسی می‌تواند اشکال و مصادیق متفاوتی داشته باشد. با گسترش استفاده از سیستم‌های اطلاعاتی، داده‌های حجیم و فناوری‌های دیجیتال، دامنه ناهنجاری‌ها دیگر صرفاً به تحریف‌های مالی محدود نبوده و حوزه‌های متنوع‌تری را در بر می‌گیرد. در ادبیات پژوهشی، تشخیص ناهنجاری به‌عنوان یک رویکرد مشترک در حوزه‌های مختلف حسابرسی مطرح شده است که مهم‌ترین آن‌ها شامل حسابرسی مالی و حسابرسی امنیت سایبری می‌شود (کی‌آر و همکاران[6]، ۲۰۲۴).

در حسابرسی مالی، ناهنجاری‌ها معمولاً به‌صورت تقلب[7]، تحریف با اهمیت صورت‌های مالی یا خطاهای غیرعمدی در داده‌ها و گزارش‌های مالی بروز می‌کنند. این نوع ناهنجاری‌ها اغلب در قالب الگوهای غیرعادی در تراکنش‌ها، مانده‌حساب‌ها یا نسبت‌های مالی شناسایی می‌شوند و هدف اصلی از تشخیص آن‌ها، افزایش قابلیت اتکای گزارشگری مالی و حمایت از تصمیم‌گیری ذی‌نفعان است (حضوری و همکاران، ۱۴۰۴). تمرکز اصلی این پژوهش حسابرسی

[1] Chacko et al.
[2] Artificial Intelligence (AI)
[3] Mehrotra & Mehrotra
[4] Chalapathy & Chawla
[10] Hassan &Ahmed
[6] KR et al.
[7] Fraud

مالی می‌باشد؛ چرا که حسابرسی مالی یکی از ابزارهای کلیدی در تضمین صحت و دقت اطلاعات مالی سازمان‌ها است و می‌تواند نقص‌ها و اشتباهات احتمالی را کشف کرده و به بهبود عملکرد مالی و شفافیت سازمان کمک کند. در شکل ۲، نمونه‌هایی از ناهنجاری‌ها در حوزه حسابرسی مالی ارائه شده است. در مقابل، در حسابرسی امنیت سایبری، ناهنجاری‌ها بیشتر به شکل سوءاستفاده از دسترسی‌ها[1] ، نفوذ[2] به سیستم‌ها ، رفتار غیرعادی کاربران یا سیستم‌ها و فعالیت‌های مخرب سایبری ظاهر می‌شوند (حسن و همکاران، ۲۰۲۵). این ناهنجاری‌ها لزوماً ماهیت مالی مستقیم ندارند، اما می‌توانند پیامدهای جدی برای محرمانگی[3]، یکپارچگی و دسترس‌پذیری اطلاعات سازمان به همراه داشته باشند و در نهایت منجر به ریسک‌های مالی و اعتباری شوند. بر این اساس، می‌توان گفت که تشخیص ناهنجاری در حسابرسی یک مفهوم بین‌حوزه‌ای[4] است که بسته به نوع حسابرسی، ماهیت داده‌ها و اهداف کنترلی، تعاریف و مصادیق متفاوتی پیدا می‌کند (سلطانی و همکاران، ۱۴۰۲؛ تیپرونگسری و واسارهیلی[5]، ۲۰۱۱).

Figure 2. Anomaly Detection in Finance

شکل ۲. تشخیص ناهنجاری در حوزه مالی

[1] Misuse
[2] Intrusion
[3] Confidentiality
[4] Cross-Domain
[5] Thiprungsri &Vasarhelyi

پیاده‌سازی موفق تشخیص ناهنجاری می‌تواند در محیط‌های بسیار رقابتی که نیازمند نوآوری و سازگاری مداوم هستند، مزیت رقابتی ارائه دهد، چرا که به‌طور بالقوه می‌تواند کارایی ،کیفیت و دقت حسابرسی فناوری اطلاعات را افزایش دهد. صاحبکار در فرآیند حسابرسی می‌تواند بر اثربخشی و کارایی فناوری اطلاعات با کیفیت بالاتر تأثیر بگذارد. با این حال پیاده‌سازی تشخیص ناهنجاری چالش‌های خاص خود را دارد. روش‌های مختلفی برای شناسایی ناهنجاری‌ها در این زمینه وجود دارد و هر روش نیازمند متناسب با عواملی چون تنوع داده‌ها، کیفیت داده‌ها و دقت مورد نیاز انتخاب می‌شود. علاوه بر این، داده‌های حسابرسی فناوری اطلاعات ساختار کمتری دارند، یعنی داده‌های عددی در حسابرسی مالی راحت‌تر قابل تحلیل هستند نسبت به ترکیب داده‌های متنی، نمودارها، تصاویر، کد و غیره که در حسابرسی فناوری اطلاعات موجود است. بنابراین، چالش اعمال تشخیص ناهنجاری در این حوزه در انتخاب و بررسی وظایف و فرآیندها نهفته است.

بیان مسئله

در این پژوهش، مسئله شناسایی ناهنجاری‌های حسابرسی به‌صورت یک مسئله طبقه‌بندی دودویی مدل‌سازی شده است که در آن هر تراکنش به‌صورت یک بردار ویژگی $\mathrm{x}_i \in \mathbb{R}^d$ نمایش داده می‌شود و برچسب متناظر آن $y_i \in \{0,1\}$ نشان‌دهنده عادی یا ناهنجار بودن تراکنش است. هدف، یافتن یک نگاشت مناسب مطابق فرمول (۱-۱) است که با کمینه‌سازی خطای پیش‌بینی، قادر به تشخیص درست رفتارهای ناهنجار باشد.

$$F(x_i) = y_i \qquad (۱-۱)$$

ساختار مقاله بدین ترتیب تنظیم شده است که ابتدا مبانی نظری و فرآیند توسعه فرضیه‌ها تبیین می‌شود تا چارچوب مفهومی پژوهش و منطق شکل‌گیری فرضیه‌ها روشن گردد؛ سپس فرضیه‌های پژوهش به‌صورت مشخص ارائه می‌گردد. در ادامه، روش‌شناسی پژوهش شامل معرفی داده‌ها، مراحل پیش‌پردازش، طراحی مدل و شیوه ارزیابی تشریح می‌شود. پس از آن، یافته‌های پژوهش با گزارش نتایج تجربی و خروجی‌های اصلی ارائه می‌گردد. در بخش بحث، نتایج تفسیر شده و پیامدها، محدودیت‌ها و دلالت‌های کاربردی آن بررسی می‌شود و در نهایت،

مقاله با نتیجه‌گیری شامل جمع‌بندی دستاوردها و پیشنهادهایی برای پژوهش‌های آینده خاتمه می‌یابد.

مبانی نظری و توسعه فرضیه‌ها

با افزایش دیجیتالی شدن فرایندهای سازمانی و رشد حجم داده‌های مالی و سیستمی، شناسایی رفتارهای غیرعادی و ناهنجاری‌ها به یکی از ابزارهای حیاتی برای کشف خطا، تقلب و سوءاستفاده تبدیل شده است. روش‌های سنتی مبتنی بر قوانین آماری، مانند قانون بنفورد[۱]، توانایی محدود در تشخیص الگوهای پیچیده و غیرخطی دارند و بیشتر برای غربالگری اولیه مناسب هستند. پژوهش‌های اخیر تأکید دارند که در محیط‌های پیچیده فناوری اطلاعات، این رویکردها باید با روش‌های پیشرفته‌تر ترکیب شوند تا قابلیت کاربرد عملی داشته باشند (هیلال و همکاران[۲]، ۲۰۲۲).

مطالعه منابع علمی نشان می‌دهد که الگوریتم‌های داده‌کاوی اخیراً جایگاه مهمی در تشخیص ناهنجاری‌های مالی و شناسایی رفتارهای متقلبانه پیدا کرده‌اند. با استفاده از روش‌های شبکه عصبی[۳]، درخت تصمیم[۴] و ماشین بردار پشتیبان[۵] در داده کاوی[۶]، صورت‌های مالی متقلبانه و غیرمتقلبانه تمییز داده شده‌اند (احمدی و همکاران، ۱۴۰۳). قابلیت‌های تحلیلی متنوع داده‌کاوی، از آن ابزاری اساسی برای مواجهه با چالش‌های پیچیده حوزه مالی ساخته است. این تکنیک‌ها امکان پیش‌بینی احتمال وقوع ورشکستگی، تشخیص زودهنگام بی‌ثباتی‌های مالی، کشف نشانه‌های سوءاستفاده توسط مدیران، محاسبه کمی سطح ریسک و تخمین روند آتی عملکرد بنگاه‌های اقتصادی را فراهم می‌آورند (رضائی پیته نوئی و همکاران، ۱۴۰۰).

در سال‌های اخیر، یادگیری ماشین بدون نظارت به عنوان رویکردی مؤثر برای شناسایی ناهنجاری در داده‌های تراکنش و گزارش سیستمی مطرح شده است. الگوریتم‌هایی مانند جنگل ایزوله[۷] و خوشه‌بندی‌های مبتنی بر فاصله قادرند بدون نیاز به داده‌های برچسب‌دار، رفتارهای

[1] Benford's law
[2] Hilal et al.
[3] Neural Network
[4] Decision Tree
[5] Support Vector Machine
[6] Data mining
[7] Isolation Forest

غیرعادی را تشخیص دهند. این رویکردها در محیط‌های حسابرسی فناوری اطلاعات که داده‌های برچسب‌دار محدود هستند، اهمیت ویژه‌ای دارند؛ هرچند حساسیت به نویز و محدودیت در توضیح‌پذیری هنوز از چالش‌های آن‌هاست (پینتو و سوبریرو[1]، ۲۰۲۲).

همزمان پیشرفت‌های حوزه یادگیری عمیق امکان تحلیل داده‌های تراکنش و گزارش‌های سیستمی پیچیده را فراهم کرده است. مدل‌هایی مانند خودرمزگذار[2]، حافظه طولانی کوتاه مدت[3] و مبدل[4] توانایی استخراج روابط غیرخطی و وابستگی‌های بلندمدت در داده‌ها را دارند و بهبود قابل توجهی در دقت تشخیص ناهنجاری ایجاد می‌کنند. با این حال، محدودیت اصلی این مدل‌ها، دشواری در ارائه توضیحات روشن و قابل فهم برای حسابرسان است (چن و همکاران[5]، ۲۰۲۵؛ باقریان کاسگری و همکاران، ۱۴۰۳).

برای رفع این محدودیت، پژوهش‌ها به سمت چارچوب‌های ترکیبی[6] حرکت کرده‌اند که در آن‌ها استانداردهای حسابرسی سنتی با الگوریتم‌های یادگیری ماشین تلفیق می‌شوند. در این چارچوب‌ها، داده‌ها ابتدا از فیلترهای مبتنی بر قوانین عبور می‌کنند و سپس مدل‌های پیشرفته رفتارهای غیرعادی را شناسایی می‌کنند، به گونه‌ای که هم دقت و هم قابلیت تفسیر نتایج افزایش می‌یابد (پینتو و سوبریرو، ۲۰۲۲).

یکی دیگر از رویکردهای نوین، یادگیری خودنظارتی[7] است که بدون نیاز به داده‌های برچسب‌دار، توانایی شناسایی انحرافات از رفتار طبیعی سیستم را دارد. این روش‌ها با ایجاد وظایف پیش‌متنی مانند بازسازی یا پیش‌بینی توالی‌ها، نمایشی از رفتار نرمال سیستم ایجاد می‌کنند و ناهنجاری‌ها را بر اساس انحراف از این نمایش شناسایی می‌کنند. مزیت این روش‌ها در انعطاف‌پذیری و کاهش وابستگی به داده‌های برچسب‌دار است (چن و همکاران، ۲۰۲۵).

همچنین استفاده از شبکه‌های عصبی گراف[8] برای تحلیل داده‌های تراکنش، امکان شناسایی ناهنجاری‌های شبکه‌ای و الگوهای پیچیده را فراهم کرده است. در این مدل‌ها، حساب‌ها یا کاربران به عنوان گره و تراکنش‌ها به عنوان لبه نمایش داده می‌شوند و روابط ساختاری بین

[1] Pinto &Sobreiro
[2] Autoencoder
[3] Long Short Term Memory (LSTM)
[4] Transformer
[5] Chen et al.
[6] Hybrid Frameworks
[7] Self-Supervised Learning
[8] Graph Neural Networks

آن‌ها بررسی می‌شود. این روش‌ها قادرند ناهنجاری‌هایی را کشف کنند که روش‌های سنتی قادر به تشخیص آن‌ها نیستند، اما تفسیر نتایج همچنان چالش‌برانگیز است، که موجب توسعه رویکردهای تشخیص ناهنجاری گراف پایه توضیح‌پذیر[1] شده است (مطیعی و راحمی، ۲۰۲۴). مطالعه پژوهش‌های گذشته نشان می‌دهد که حوزه تشخیص ناهنجاری در حسابرسی فناوری اطلاعات از روش‌های آماری سنتی به سمت یادگیری ماشین بدون نظارت، یادگیری عمیق، چارچوب‌های ترکیبی، یادگیری خودنظارتی و مدل‌های گرافی با قابلیت توضیح پذیری پیش رفته است. مطالعات اخیر تأکید دارند که برای موفقیت عملی، مدل‌ها باید علاوه بر دقت، قابلیت ارائه توضیح قابل فهم و انطباق با الزامات قانونی و حرفه‌ای را نیز داشته باشند (هیلال و همکاران، ۲۰۲۲؛ پینتو و سوبریرو، ۲۰۲۲؛ چن و همکاران، ۲۰۲۵؛ مطیعی و راحمی، ۲۰۲۴).

به‌منظور ارائه یک دید مقایسه‌ای از رویکردهای به‌روز تشخیص ناهنجاری در حوزه حسابرسی فناوری اطلاعات، جدول ۱ مجموعه‌ای از مطالعات منتخب را بر اساس نوع داده، روش مورد استفاده و نقاط قوت و محدودیت‌ها خلاصه می‌کند. این مطالعات نمایانگر گرایش‌های اخیر به استفاده از یادگیری ماشین، یادگیری عمیق، مدل‌های معناگرا و چارچوب‌های ترکیبی برای تحلیل گزارش‌های سیستمی، توالی رخدادها و رفتار کاربران هستند. هدف از ارائه این جدول، تسهیل مقایسه ساخت‌یافته روش‌ها و شناسایی روندهای غالب و خلأهای پژوهشی موجود است.

جدول ۱. مقایسه روش‌های تشخیص ناهنجاری در حسابرسی فناوری اطلاعات

Table 1. Comparition of anomaly detection methods in IT auditing

#	Author/Year	Data Type	Method	Strengths	Limitations
1	Karimi Far et al. (2025)	Financial Transaction Records	Regression, ANN, Deep Learning	Better performance of deep learning compared to regression and neural network in financial fraud detection	Lower generalizability of the model due to focus on a single market

[1] Explainable Graph-based Anomaly Detection

#	Author/Year	Data Type	Method	Strengths	Limitations
2	Kazemi & Piri (2022)	Financial statements of 134 companies (2009–2021)	Multi-classification with SVM, Logistic Regression, Decision Tree, Boosting	Effective multi-class fraud detection using SVM on imbalanced data with thorough model comparison	Unbalanced data, limited methods, geographic restriction, and high tuning demands.
3	Alsalmi et al. (2025)	System logs	BertGCN (BERT + GCN)	Simultaneously captures semantic text and graph structure features	High computational demand, depends on BERT embedding quality
4	De la Cruz Cabello et al. (2025)	System logs	LLM + RAG for Log Anomaly	Leverages strong language knowledge, high flexibility	Requires large LLM resources, challenging for real-time processing
5	Uchida et al. (2024)	Log text	SPClassifier + Ensemble	Higher accuracy than standard DNN, lower resource consumption	Limited to specific preprocessed datasets
6	Sun et al. (2025)	System logs	SemiSMAC (Semi-supervised)	Improves performance with limited labeled data, self-tuning parameters	Framework complexity, reliance on LLM for initial separation
7	Okolie et al. (2025)	Heterogeneous data	ML + DL hybrid	Adaptable to diverse datasets, combines network and behavioral data	Balancing sensitivity and specificity is challenging
8	Wu et al. (2025)	Attack-resilient logs	AAR-log	More robust against targeted attacks	Early-stage development, requires further testing
9	Niu et al. (2024)	System logs	WDLog (Wide & Deep Learning)	Combines strengths of Wide and Deep models	Larger model size, higher computational requirement
10	Patel & Iyer (2025)	User behavior	SiaDNN (Siamese DNN)	High accuracy in detecting deviation from normal behavior	Dependent on sample size and quality of normal behavior

مرور روش‌های خلاصه‌شده در جدول ۱ نشان می‌دهد که بخش قابل توجهی از پژوهش‌های اخیر بر تحلیل گزارش‌های سیستمی و توالی رخدادها با استفاده از مدل‌های دنباله‌ای و یادگیری عمیق متمرکز شده‌اند. مدل‌هایی مبتنی بر حافظه طولانی کوتاه مدت و واحد بازگشتی دروازه‌ای[1] با هدف یادگیری الگوهای رفتاری عادی سیستم و شناسایی انحراف از این الگوها توسعه یافته‌اند و در بسیاری از موارد به بهبود دقت تشخیص ناهنجاری منجر شده‌اند. حافظه طولانی کوتاه مدت نوعی شبکه عصبی بازگشتی است که با استفاده از سازوکارهای دروازه‌ای، توانایی حفظ و مدیریت اطلاعات در بازه‌های زمانی طولانی را دارد و مشکل محوشدگی گرادیان را کاهش می‌دهد. واحد بازگشتیِ دروازه‌ای مدلی ساده‌تر از حافظه طولانی کوتاه مدت در شبکه‌های عصبی بازگشتی است که با بهره‌گیری از دروازه‌های به‌روزرسانی و بازنشانی، وابستگی‌های زمانی داده‌ها را یاد می‌گیرد و با ساختاری کم‌پیچیده‌تر، کارایی محاسباتی بالاتری ارائه می‌دهد.

در سال‌های اخیر، توجه پژوهش‌ها به سمت استفاده از نمایش‌های معنایی و مدل‌های زبانی پیشرفته افزایش یافته است. ترکیب مدل‌های مبتنی بر برت[2] با ساختارهای گرافی یا استفاده از مدل‌های زبانی بزرگ در قالب چارچوب‌های بازیابی دانش، امکان استخراج هم‌زمان اطلاعات متنی و ساختاری از گزارش‌ها را فراهم کرده و توانایی شناسایی ناهنجاری‌های پیچیده را افزایش داده است (السلمی و همکاران[3]، ۲۰۲۵؛ دلا کروز سابلو و همکاران[4]، ۲۰۲۵). با این حال، این رویکردها معمولاً با هزینه محاسباتی بالا و چالش‌های پیاده‌سازی در محیط‌های عملیاتی بلادرنگ همراه هستند.

علاوه بر این برخی مطالعات به سمت چارچوب‌های نیمه‌نظارتی، ترکیبی و مقاوم حرکت کرده‌اند تا وابستگی به داده‌های برچسب‌دار کاهش یابد و پایداری مدل‌ها در برابر تغییر رفتار سیستم یا حملات هدفمند افزایش پیدا کند (اوکولی و همکاران[5]، ۲۰۲۵؛ سان،کئونگ و همکاران[6]، ۲۰۲۵؛ وو وهمکاران[7]، ۲۰۲۵؛ اوچیدا و همکاران[8]، ۲۰۲۵). همچنین روش‌های

[1] Gated Recurrent Unit (GRU)
[2] BERT
[3] Alsalmi et al.
[4] De la Cruz Cabello et al.
[5] Okolie et al.
[6] Sun et la.
[7] Wu et al.
[8] Uchidaet al.

مبتنی بر تحلیل رفتار کاربران با استفاده از شبکه‌های عصبی سیامی [1] معرفی شده‌اند که با یادگیری الگوهای شباهت، انحرافات معنادار رفتاری را شناسایی می‌کنند (نیو و همکاران [2]، ۲۰۲۴؛ پاتل و ایر [3]، ۲۰۲۵). در مجموع، این مطالعات نشان می‌دهند که روند غالب پژوهش‌ها در تشخیص ناهنجاری حسابرسی فناوری اطلاعات به سمت مدل‌های عمیق، معناگرا، ترکیبی و سازگار با الزامات عملیاتی و امنیتی سازمان‌ها در حال حرکت است.

فرضیه‌های پژوهش

در این پژوهش، به‌دلیل ماهیت حساس و محرمانه داده‌های مالی و محدودیت‌های قانونی و امنیتی مرتبط با افشای اطلاعات واقعی مشتریان، دسترسی به مجموعه‌داده‌های واقعی مورد استفاده در سامانه‌های حسابرسی و کشف ناهنجاری برای پژوهشگران به‌طور مستقیم امکان‌پذیر نیست. به همین دلیل، بسیاری از مطالعات معتبر پیشین نیز از مجموعه‌داده‌های شبیه‌سازی‌شده یا شخصی‌شده استفاده کرده‌اند. در همین راستا، در این پژوهش از یک مجموعه‌داده ساختگی اما واقع‌گرایانه استفاده شده است که با بهره‌گیری از الگوهای آماری و رفتاری استخراج‌شده از سناریوهای واقعی مالی طراحی شده و قادر است ویژگی‌های کلیدی تراکنش‌های واقعی، از جمله رفتارهای غیرعادی و ناهنجار را به‌درستی بازنمایی کند. این رویکرد ضمن حفظ محرمانگی اطلاعات، امکان ارزیابی دقیق و قابل‌اتکای عملکرد مدل پیشنهادی را فراهم ساخته و زمینه‌ای مناسب برای تحلیل و توسعه روش‌های هوشمند تشخیص ریسک در محیط‌های واقعی فراهم می‌آورد.

روش‌شناسی پژوهش

با توجه به اینکه کارآمدی تکنیک‌های داده‌کاوی در شناسایی تقلب و استخراج الگوهای ناهنجار در داده‌های مالی و حسابرسی گزارش شده است (رهنمای رودپشتی، ۱۳۹۱)، این بخش روش پیشنهادی یادگیری ماشین برای تشخیص ناهنجاری و رتبه‌بندی موارد استثنا و پرخطر در حسابرسی فناوری اطلاعات را توضیح می‌دهد. نمای کلی روش در شکل ۳ نمایش داده شده

[1] Siamese neural network
[2] Niu et al.
[3] Patel & Iyer

است. مرحله ورودی پژوهش با دریافت مجموعه‌داده در قالب یک جدول ادغام‌شده از داده‌های چندجدولی (تراکنش[1]، مشتری[2] و پذیرنده[3]) آغاز می‌شود و سپس یک مرحله پیش‌پردازش ساختاریافته اجرا می‌گردد که شامل بررسی اولیه داده‌ها، استانداردسازی فیلدهای زمانی، اصلاح مقادیر نامعتبر و تکمیل مقادیر گمشده است. در گام بعد، ویژگی‌های هدفمند حسابرسی استخراج می‌شوند تا ابعاد الگوی زمانی تراکنش‌ها، ناسازگاری یا عدم تطابق بین سامانه‌ها و انحراف از رفتار معمول مشتری پوشش داده شود.

از آنجا که برچسب‌ها برای موارد ناهنجاری و استثنای حسابرسی در بسیاری از سناریوهای واقعی کامل یا قابل اتکا و یا در دسترس نیستند، برای اینکه هدف روش به نیازهای عملی حسابرسی نزدیک‌تر باشد، یک شبه‌برچسب با استفاده از چند قاعده ساده و مبتنی بر توزیع داده‌ها و محاسبه امتیاز ریسک حسابرسی برای هر تراکنش تولید می‌شود. سپس داده‌ها به دو بخش آموزش و آزمون تقسیم شده و یک مدل جنگل تصادفی[4] برای پیش‌بینی احتمال وقوع ناهنجاری هر تراکنش آموزش داده می‌شود. در نهایت، مدل برای هر تراکنش یک امتیاز نمره ریسک تولید می‌کند و تراکنش‌ها بر اساس این امتیاز رتبه‌بندی می‌شوند تا یک فهرست کوتاه از موارد پرخطر جهت بررسی و رسیدگی به‌عنوان خروجی پژوهش داده شده و در اختیار حسابرس قرار گیرد.

در خصوص نمونه پژوهش، لازم به توضیح است که در این پژوهش از یک مجموعه‌داده معتبر و عمومی منتشرشده در پلتفرم Kaggle استفاده شده است که مشخصات آن در بخش «مجموعه‌داده» ارائه شده است. با این حال، تمامی مراحل طراحی روش، تعریف قواعد حسابرسی، تولید شبه‌برچسب و پیاده‌سازی مدل یادگیری ماشین در این مطالعه به‌صورت مستقل توسط پژوهشگران انجام شده است.

[1] Transactions
[2] Customers
[3] Merchants
[4] Random Forest

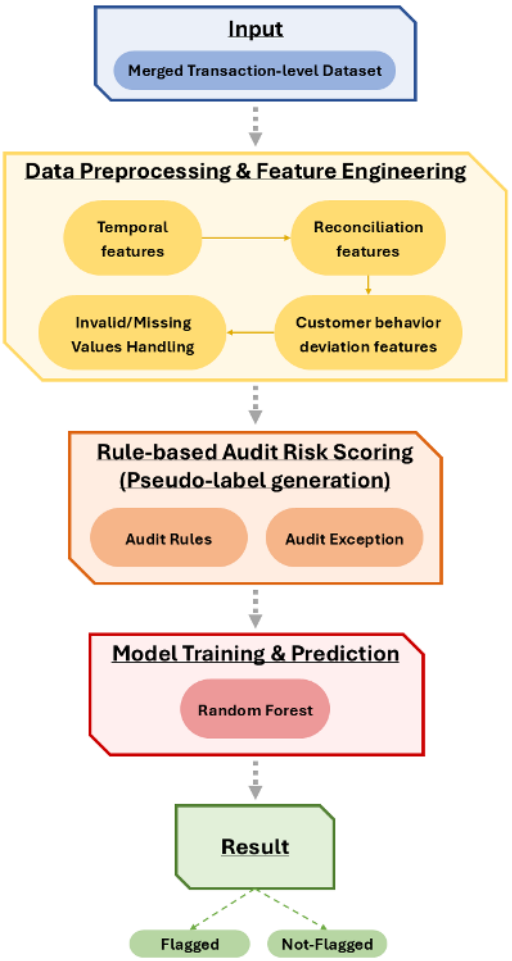


Figure 3. Proposed method diagram for identifying anomalies and prioritizing high-risk cases in financial auditing

شکل ۳. روش پیشنهادی برای شناسایی ناهنجاری‌ها و رتبه‌بندی موارد پرخطر در حسابرسی مالی

- **مرحله پیش‌پردازش و مهندسی ویژگی‌ها**

پس از بارگذاری داده‌ها، روش پیشنهادی با اجرای مراحل پیش‌پردازش و مهندسی ویژگی، سطرهای خام تراکنش در مجموعه‌داده را به مجموعه‌ای از نشانگرهای معنادار و مرتبط با حسابرسی تبدیل می‌کند.

برای هم‌راستاسازی کشف ناهنجاری با اهداف حسابرسی فناوری اطلاعات –از جمله کشف بی‌نظمی‌های زمانی، عدم تطبیق بین‌سیستمی و تشخیص انحرافات رفتاری مشتری– ویژگی‌ها در سه گروه طراحی شدند:

• ویژگی‌های زمانی

ویژگی‌های زمانی مستقیماً از برچسب زمانی تراکنش استخراج می‌شوند. به این معنا که از زمان ثبت تراکنش مجموعه‌ای از ویژگی‌های زمانی (ساعت تراکنش[1]، روز هفته[2] و شاخص آخرهفته بودن[3]) ساخته می‌شوند تا الگوهای معمول و همچنین زمان‌های غیرمعمولِ وقوع تراکنش‌ها ثبت شود؛ مؤلفه‌ای که در محیط‌های حسابرسی، معمولا سرنخ‌های مفیدی برای کشف ناهنجاری فراهم می‌کند.

• ویژگی‌های تطبیقی

در این مرحله، برای شناسایی ناسازگاری میان دو نمایش موجود از مبلغ تراکنش در داده‌ها (Amount و TransactionAmount) ویژگی‌های تطبیقی اختلاف مطلق[4] و نسبت اختلاف[5] ساخته می‌شوند. این ویژگی‌ها به‌صورت عملی این ایده را پیاده‌سازی می‌کنند که تراکنش‌های مشکوک اغلب با ناسازگاری بین سیستم‌ها و تفاوت در لایه‌های ثبت و گزارشگری همراه هستند.

ویژگی اختلاف مطلق (۱–۲) میزان عدم تطابق مبلغ ثبت‌شده بین دو سیستم را به‌صورت مستقیم اندازه‌گیری می‌کند و ویژگی نسبت اختلاف (۱–۳) شدت اختلاف را به‌صورت نسبی با مدیریت تقسیم بر صفر و مقادیر بی‌نهایت نشان می‌دهد. ذکر این نکته لازم است که مواردی که مخرج صفر دارند به‌عنوان مقدار گمشده در نظر گرفته می‌شوند تا در مرحله مدیریت مقادیر نامعتبر یا گمشده به‌صورت سازگار مدیریت شوند.

$$\text{AmountDiff} = |Amount - TransactionAmount| \qquad (۱–۲)$$

[1] Hour
[2] DayOfWeek
[3] IsWeekend
[4] AmountDiff
[5] AmountRatio

$$\text{AmountRatio} = \frac{Amount}{TransactionAmount} \qquad (۳-۱)$$

• ویژگی‌های انحراف رفتار مشتری

در نهایت، ویژگی‌های انحراف رفتاری مشتری محاسبه می‌شود تا مشخص شود هر تراکنش نسبت به الگوی معمول همان مشتری تا چه حد غیرعادی است؛ زیرا ناهنجاری‌ها در بسیاری از موارد مشتری‌محور هستند. بدین منظور، تراکنش‌ها بر اساس ویژگی CustomerID گروه‌بندی شده و میانگین[۱] (cust_mean_amount) و انحراف معیار مبلغ تراکنش‌های هر مشتری[۲] (cust_std_amount) محاسبه می‌گردد. سپس برای هر تراکنش، یک امتیاز انحراف استانداردشده مطلق (abs_amount_dev_vs_cust) طبق معادله (۱-۴) محاسبه شده و برای جلوگیری از ناپایداری در تقسیم، یک ثابت عددی کوچک ϵ به مخرج افزوده می‌شود. حاصل، یک مجموعه ویژگی فشرده است که به‌صورت هم‌زمان بی‌نظمی‌های زمانی، ناسازگاری و غیرعادی بودن نسبت به الگوی مشتری را پوشش می‌دهد.

$$\text{abs\_amount\_dev\_vs\_cust} = \frac{Amount - cust\_mean\_amount}{cust\_std\_amount + \varepsilon} \qquad (۴-۱)$$

• مدیریت مقادیر نامعتبر یا گمشده

در ابتدا پیش از مدیریت مقادیر عددی نامعتبر یا گمشده و ساخت ماتریس نهایی ویژگی‌ها برای آموزش مدل، متغیرهای زمانی به قالب‌های استاندارد زمانی تبدیل شده و برچسب‌های زمانی که قابل تبدیل به قالب استاندارد نباشند، به‌عنوان مقدار گمشده ثبت می‌شوند تا از بروز خطا در مراحل بعدی، به‌ویژه هنگام استخراج ویژگی‌های زمانی، جلوگیری شود.

سپس مقادیر نامعتبر و گمشده به‌گونه‌ای مدیریت می‌شوند که پایداری عددی در کل روش تضمین شود. این موضوع به‌ویژه برای ویژگی‌های نسبتی اهمیت دارد؛ زیرا همان‌طور که در قبل دیده شد در صورت وجود مخرج صفر، این متغیرها می‌توانند به مقادیر تعریف‌نشده یا نامتناهی منجر شوند. بر همین اساس، مقادیر عددی نامعتبر به‌صورت یکنواخت به مقدار گمشده تبدیل

[1] Customer-level mean transaction amount
[2] Customer-level standard deviation amount

می‌گردند تا اثر نامطلوب آن‌ها بر آموزش مدل حذف شود. در نهایت مقادیر گمشده باقی‌مانده در ماتریس ویژگی‌ها با استفاده از روش جایگذاری میانه[1] تکمیل می‌گردند تا از نشت اطلاعات جلوگیری شود.

- **امتیازدهی ریسک حسابرسی مبتنی بر قواعد و برچسب‌گذاری شبه‌واقعی**

از آنجا که برچسب‌های معتبر و قطعی برای موارد ناهنجاری و استثنا حسابرسی در بسیاری از سناریوهای واقعی در دسترس نیستند یا اینکه ممکن است کامل نباشند، یک شبه‌برچسب مبتنی بر قواعد الهام‌گرفته از منطق حسابرسی با بهره‌گیری از یک لایه امتیازدهی ریسک با عنوان AuditException تولید می‌شود تا تراکنش‌هایی را که ارزش بررسی و پیگیری دارند مشخص کند.

- **قواعد حسابرسی**

قواعد حسابرسی، مجموعه‌ای از قواعد دودویی الهام‌گرفته از منطق حسابرسی است که با استفاده از آستانه‌های به‌صورت داده‌محور مبتنی بر صدک‌ها (به‌جهت سازگاری قواعد با توزیع داده‌ها) در جدول ۲ تعریف شده است:

جدول ۲. قوانین حسابرسی مورداستفاده برای تولید شبه‌برچسب

Table 2. Audit Rules Used for Pseudo-label Generation

Rule	Threshold definition
R1	AmountDiff > Q95(AmountDiff)
R2	AmountRatio < Q01(AmountRatio) or AmountRatio > Q99(AmountRatio)
R3	Amount > Q95(Amount) and AccountBalance < Q05(AccountBalance)
R4	Hour ∈ [0, 5]
R5	abs_amount_dev_vs_cust > Q95(abs_amount_dev_vs_cust)

قاعده ۱ اختلاف زیاد بین دو سیستم ثبت مبلغ، قاعده ۲ ناسازگاری و عدم تطبیق نسبی بین سیستم‌ها، قاعده ۳ مبلغ زیاد با موجودی کم، قاعده ۴ فعالیت در ساعات غیرمعمول (بین ۱۲ شب تا ۵ صبح) و قاعده ۵ انحراف زیاد از رفتار معمول مشتری یعنی زمانی که تراکنش برای مشتری

[1] Median Imputation

غیرعادی باشد را نشان می‌دهد که هرکدام از این‌ها می‌تواند نشان‌دهنده رفتار پرخطر یا فعالیت مشکوک باشد.

• امتیازدهی و برچسب‌گذاری

خروجی قواعد حسابرسی در قالب یک امتیاز ترکیبی با عنوان AuditRiskScore تجمیع می‌شود؛ این تجمیع به‌صورت جمع وزن‌دار محاسبه می‌شود تا تفاوت شدت و اهمیت انواع سیگنال‌های ریسک در نظر گرفته شود. برای قواعدی که نشانگرهای قوی‌تری از ریسک و ناهنجاری محسوب می‌شوند، وزن‌های بزرگ‌تر در نظر گرفته می‌شود. امتیاز ریسک حسابرسی وزن‌دار به‌صورت معادله (۱-۵) محاسبه می‌گردد:

$$\text{AuditRiskScore} = 3 \times R1 + 2 \times R2 + 2 \times R3 + 1 \times R4 + 2 \times R5 \qquad (۵-۱)$$

در نهایت، شبه‌برچسب AuditException با انتخاب دهک بالایی از توزیع امتیاز ریسک تعریف می‌گردد؛ یعنی تراکنش‌هایی که امتیاز آن‌ها بزرگ‌تر یا مساوی صدک ۹۰ باشد به‌عنوان استثنای حسابرسی و ناهنجاری برچسب‌گذاری می‌شوند و سایر تراکنش‌ها غیراستثنا و معمول تلقی می‌گردند. این طراحی به‌صورت مستقیم با رویه حسابرسی هم‌سو است؛ این طراحی با جریان کار واقعی حسابرسی هم‌سو است؛ زیرا در عمل، منابع بررسی محدود است و به‌جای بررسی دستی همه تراکنش‌ها، تنها مجموعه کوچکی از موارد پرخطر بر اساس سیگنال‌های ریسک برای رسیدگی رتبه‌بندی می‌شوند.

پس تراکنش‌ها در نهایت بدین صورت به شبه‌برچسب تبدیل می‌شوند:

- AuditException = 1 (اگر امتیاز ریسک تراکنش در ۱۰٪ بالا (صدک ۹۰ و بالاتر) قرار گیرد)
- در غیر این صورت AuditException = 0

• آموزش مدل و پیش‌بینی

در بخش آموزش و پیش‌بینی، یک مدل یادگیری نظارت‌شده از نوع طبقه‌بند جنگل تصادفی با پیکربندی ارائه‌شده در جدول ۳ آموزش داده می‌شود تا شبه‌برچسب AuditException را بر اساس مجموعه‌ای از ویژگی‌های مهندسی‌شده و حسابرسی‌محور پیش‌بینی کند. انتخاب جنگل

تصادفی به چند دلیل انجام شده است: این الگوریتم در داده‌های جدولی معمولاً عملکرد پایداری دارد، می‌تواند الگوهای پیچیده و برهم‌کنش‌های غیرخطی میان سیگنال‌های ناهمگون حسابرسی (مانند ویژگی‌های مربوط به مبلغ، زمان، مغایرت سیستمی و رفتار مشتری) را بدون نیاز به فرض توزیعی خاص یاد بگیرد، و به‌صورت طبیعی نسبت به هم‌بستگی‌های متوسط بین ویژگی‌ها حساسیت کمتری نشان می‌دهد. علاوه بر این، با تکیه بر سازوکار تجمیع چندین درخت تصمیم، جنگل تصادفی نسبت به نویز و تغییرات موضعی داده مقاوم‌تر بوده و خطر بیش‌برازش را در مقایسه با یک درخت منفرد کاهش می‌دهد. به‌طور کلی، جنگل تصادفی با پیاده‌سازی سریع و آسان، عملکرد پیش‌بینی بالایی دارد و امکان استفاده از تعداد زیادی ویژگی را با حفظ تعمیم‌پذیری و کنترل بیش‌برازش فراهم می‌سازد (فضل‌زاده، حقیقت، پورکیوان و احمدیان، ۱۳۹۸).

به‌منظور افزایش قابلیت تعمیم‌پذیری، داده‌ها پس از انجام مراحل پاکسازی و آماده‌سازی (مانند مدیریت مقادیر گمشده، حذف یا جایگزینی مقادیر نامعتبر، و استخراج ویژگی‌های زمانی و رفتاری) به دو بخش آموزش و آزمون تقسیم شده‌اند. در این مطالعه از تقسیم‌بندی ۷۰ درصد برای آموزش و ۳۰ درصد برای آزمون استفاده شده است. برای جلوگیری از سوگیری ارزیابی، تقسیم داده‌ها به‌صورت stratified بر اساس شبه‌برچسب AuditException انجام می‌شود تا نرخ وقوع استثنا در هر دو مجموعه تقریباً ثابت بماند و مدل در هر دو بخش با توزیع مشابهی از نمونه‌های پرخطر و کم‌ریسک مواجه شود. این کار به‌ویژه در سناریوهای حسابرسی و کشف استثنا اهمیت دارد، زیرا رخدادهای پرخطر ذاتاً کمتر از نمونه‌های عادی بوده و در صورت عدم حفظ نسبت کلاس‌ها، سنجش عملکرد مدل می‌تواند گمراه‌کننده شود.

در مرحله آموزش، مدل با نمونه‌های مجموعه آموزش یاد می‌گیرد که چگونه ترکیب سیگنال‌ها به شکل‌گیری الگوهای پرخطر منجر می‌شود. سپس در مرحله آزمون، پیش‌بینی‌ها با مقادیر واقعی شبه‌برچسب مقایسه می‌شوند و معیارهای ارزیابی برای سنجش کیفیت طبقه‌بندی محاسبه می‌گردند. تمرکز بر این معیارها از آن جهت است که در کاربردهای حسابرسی، مدل باید بتواند از یک سو موارد پرخطر واقعی را تا حد امکان از دست ندهد و از سوی دیگر تعداد هشدارهای اشتباه را کاهش دهد تا بار بررسی دستی حسابرس افزایش نیابد.

در نهایت، طبقه‌بند برای هر تراکنش احتمال ناهنجاری و استثنا بودن را به‌صورت امتیاز

RF_score تولید می‌کند. برای عملیاتی‌سازی خروجی‌ها در چارچوب حسابرسی، تراکنش‌ها بر اساس RF_score به‌صورت نزولی رتبه‌بندی شده و ۵۰ مورد نخست به‌عنوان فهرست بررسی استخراج و گزارش می‌شوند. رویکرد Top-K بیانگر آن است که تحلیل‌های حسابرسی در اصل برای رتبه‌بندی مبتنی بر ریسک، در شرایط محدودیت ظرفیت بررسی (بازبینی دستی) به‌کار می‌روند. در این پژوهش، با توجه به تعداد تراکنش (رکورد) ۱۰۰۰، Top-50 متناظر با نمونه‌گیری مبتنی بر ریسک از ۵٪ موارد با بالاترین امتیاز است و یک فهرست با اولویت بالا از استثناها و ناهنجاری‌های حسابرسی برای بررسی دستی فراهم می‌کند.

جدول ۳. ابرپارامترهای طبقه‌بند جنگل تصادفی

Table 3. Hyperparameter of the Random Forest Classifier

Hyperparameter	Value
n_estimators	500
min_samples_leaf	5
class_weight	"balanced"
random_state	42
n_jobs	-1

یافته‌های پژوهش

در این بخش، به‌منظور ارائه درک جامع‌تری از عملکرد روش پیشنهادی ابتدا ساختار و ویژگی‌های مجموعه‌داده مورد استفاده، تشریح می‌شود. سپس توزیع نمرات ریسک استخراج‌شده از داده‌ها مورد تحلیل قرار گرفته و الگوهای رفتاری حاکم بر داده‌ها بررسی می‌گردد. در ادامه نتایج حاصل از ارزیابی روش پیشنهادی با استفاده از شاخص‌های متداول ارزیابی عملکرد ارائه شده است و میزان دقت، پایداری و توان تفکیک مدل در شناسایی نمونه‌های ناهنجار و عادی تحلیل می‌شود.

- **مجموعه‌داده**

داده‌های این پژوهش، یک مجموعه داده عمومی پژوهشی و معتبر است که در مطالعات حوزه کشف تقلب و تحلیل تراکنش‌های مالی مورد استفاده قرار می‌گیرد. این مجموعه داده[1] با عنوان «Fraud Detection Dataset» که در پلتفرم Kaggle منتشر شده است، به‌منظور تحلیل و

[1] https://www.kaggle.com/datasets/goyaladi/fraud-detection-dataset?select=Readme.md

مدل‌سازی ناهنجاری در تراکنش‌های مالی طراحی گردیده است. این مجموعه داده شامل پنج زیرپوشه است که هریک اطلاعات خاصی در زمینه اطلاعات تراکنش‌ها، اطلاعات مشتریان، شاخص‌ها و نشانگرهای رفتارهای مشکوک، مبالغ تراکنش‌ها، اطلاعات پذیرندگان می‌باشد.
در این پژوهش، تمامی زیرپوشه‌ها با یکدیگر ادغام شده و به یک فایل جامع دست‌یافته شده است. این فایل دارای ۱۰۰۰ ردیف و ۲۵ ویژگی می‌باشد. هر ردیف در این مجموعه، نمایانگر یک تراکنش مستقل میان مشتری و پذیرنده خدمات مالی است. از جمله ویژگی‌های اولیه این مجموعه می‌توان به شناسه تراکنش، شناسه مشتری، شناسه پذیرنده، زمان وقوع تراکنش، دسته‌بندی نوع تراکنش نظیر «آنلاین»، «سفر»و «غیره»، مبلغ تراکنش، مانده‌حساب مشتری، مکان پذیرنده و سن مشتری اشاره نمود. همچنین مجموعه شامل متغیرهای هدف از جمله «نشانگر ناهنجاری در تراکنش‌های مالی» و «پرچم مشکوک بودن» است که برای برچسب‌گذاری تراکنش‌های مشکوک به‌کار می‌روند.

افزون بر داده‌های خام، در این مجموعه ویژگی‌هایی مشتق‌شده نیز لحاظ شده‌اند که با هدف بهبود عملکرد مدل‌های پیش‌بینی ایجاد شده‌اند. از جمله این ویژگی‌ها می‌توان به اختلاف مطلق مبلغ واقعی و مبلغ گزارش‌شده‌ی تراکنش، نسبت بین این دو مبلغ، ساعت و روز هفته‌ی وقوع تراکنش و نشانگر تعطیلی اشاره نمود. همچنین با بهره‌گیری از زمان آخرین ورود مشتری به حساب کاربری، متغیرهایی نظیر «تعداد روزهای سپری‌شده از آخرین ورود» و «پرچم ورود در زمان غیرعادی» استخراج شده‌اند.

- **روش آزمون**

برای آزمون و ارزیابی روش پیشنهادی، پس از انجام پیش‌پردازش و استخراج ویژگی‌ها، داده‌ها به دو مجموعه آموزش و آزمون تقسیم شده‌اند؛ این تقسیم‌بندی با نسبت ۷۰ ٪ برای آموزش و ۳۰٪ برای آزمون انجام گرفته شده و به‌گونه‌ای توزیع شده است که نسبت نمونه‌های پرخطر و عادی در هر دو مجموعه حفظ شود. روش جنگل تصادفی صرفاً روی مجموعه آموزش یاد گرفت و سپس روی مجموعه آزمون که در فرآیند آموزش نقشی نداشت، امتیاز احتمال ریسک برای هر تراکنش را تولید کرد. در ادامه، پیش‌بینی‌های مدل با شبه‌برچسب‌های واقعی مقایسه شد و معیارهای عملکرد شامل صحت، دقت، یادآوری و امتیاز F1 محاسبه گردید تا هم توانایی مدل در شناسایی درست موارد پرخطر و هم میزان هشدارهای اشتباه به‌صورت

هم‌زمان سنجیده شود. این شیوه آزمون امکان ارزیابی واقع‌بینانه قابلیت تعمیم مدل و کارایی آن در شرایط نزدیک به کاربردهای عملی حسابرسی فناوری اطلاعات را فراهم می‌کند.

- **توزیع نمرات ریسک**

به‌منظور بررسی توزیع نمرات ریسک حسابرسی در داده‌های مورد مطالعه، از نمودار ۱ استفاده گردید. نمره ریسک به‌عنوان یکی از متغیرهای کلیدی در ارزیابی و طبقه‌بندی سطح خطرپذیری تراکنش‌های مالی، بازه‌ای از ۰ تا ۷ را پوشش می‌دهد. بررسی نمودار توزیع فراوانی نشان می‌دهد که بیشینه تعداد نمونه‌ها در نمره ۰ متمرکز شده است، به‌طوری‌که ۶۷۲ نمونه از مجموع ۱۰۰۰ نمونه، معادل ۶۷/۲ درصد، دارای نمره ریسک صفر بوده‌اند. همچنین، نمره یک با ۲۲۹ نمونه در رتبه دوم قرار دارد. این دو طبقه در مجموع حدود ۹۰/۱ درصد از کل جامعه آماری را شامل می‌شوند. سایر نمرات ریسک، به‌ویژه نمرات بالاتر از ۳، به‌صورت پراکنده و با فراوانی اندک در داده‌ها مشاهده می‌شوند.

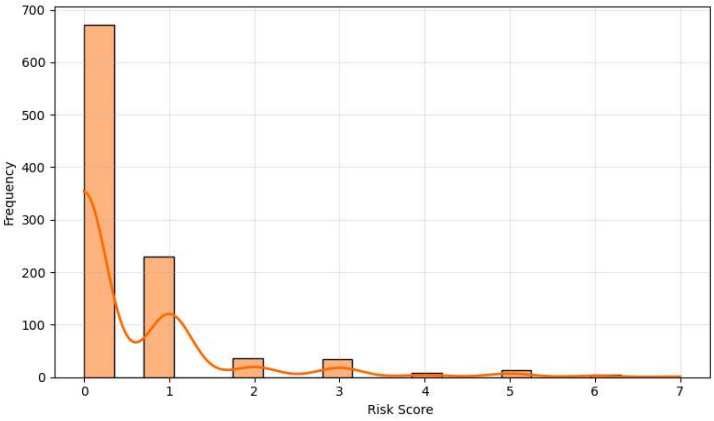


Chart 1. Distribution of risk score in dataset

نمودار ۱. توزیع نمرات ریسک در مجموعه‌داده

این عدم توازن آشکار در توزیع نمرات، که با عنوان نامتوازنی کلاس‌ها شناخته می‌شود، می‌تواند در روند مدل‌سازی آماری و یادگیری ماشین منجر به غلبه کلاس‌های اکثریت بر اقلیت شده و صحت مدل در شناسایی موارد پرخطر را به‌شدت کاهش دهد.

• نتایج ارزیابی

در این بخش، عملکرد روش پیشنهادی در طبقه‌بندی تراکنش‌های مالی مورد بررسی قرار می‌گیرد. به‌منظور ارزیابی کیفی و کمی مدل، از مجموعه‌ای از شاخص‌های استاندارد در حوزه یادگیری ماشین شامل صحت[1]، دقت[2]، فراخوانی[3]، و امتیاز F1 استفاده شده است. این معیارها به‌ویژه در مسائل طبقه‌بندی دودویی و به‌ویژه در زمینه‌هایی که با عدم توازن کلاس‌ها مواجه هستند از اهمیت بالایی برخوردارند.

هدف از این ارزیابی، سنجش میزان توانایی روش در شناسایی صحیح تراکنش‌های ناهنجار در برابر تراکنش‌های عادی، و همچنین تحلیل نرخ خطاهای احتمالی آن در طبقه‌بندی اشتباه می‌باشد. برای این منظور، از ماتریس درهم‌ریختگی[4]، منحنی دقت—فراخوانی[5] و تحلیل اهمیت ویژگی‌ها استفاده شده است. در ادامه، نتایج به‌دست‌آمده از هر یک از این روش‌ها به تفصیل گزارش و تحلیل خواهند شد.

شاخص‌های کلیدی ارزیابی عملکرد روش (کاکاوند تیموری و همکاران ، ۱۴۰۴) عبارت‌اند از:

- صحت: هدف این شاخص، نمایش نسبت پیش‌بینی‌های صحیح به کل نمونه‌ها می‌باشد و از فرمول ۱-۶ برای نمایش این نسبت استفاده می‌گردد. در این نسبت TP یا True Positive، تعداد نمونه‌هایی از کلاس مثبت یعنی تراکنش‌های ناهنجار است که مدل به‌درستی آن‌ها را به‌عنوان ناهنجاری شناسایی کرده است. این شاخص نشان‌دهنده توانایی روش در شناسایی موارد واقعی وقوع ناهنجاری است. TN یا True Negative، تعداد نمونه‌هایی از کلاس منفی یعنی تراکنش‌های عادی می‌باشد که روش به‌درستی آن‌ها را به‌عنوان تراکنش عادی شناسایی کرده است. FP یا False Positive، تعداد نمونه‌هایی که در واقع به کلاس منفی تعلق داشته‌اند اما روش پیشنهادی آن‌ها را به‌اشتباه در طبقه مثبت قرار داده است. FN یا False Negative،

[1] Accuracy
[2] Precision
[3] Recall
[4] Confusion Matrix
[5] Precision–Recall Curve

تعداد نمونه‌هایی که در واقع تراکنش ناهنجار بوده‌اند، اما روش پیشنهادی آن‌ها را به‌اشتباه به‌عنوان عادی طبقه‌بندی کرده است.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (۶-۱)$$

- دقت: هدف این شاخص، نمایش نسبت نمونه‌هایی که به‌درستی به‌عنوان مثبت یعنی ناهنجاری پیش‌بینی شده‌اند به کل نمونه‌هایی که روش آن‌ها را در این طبقه قرار داده است و از فرمول ۱-۷ برای نمایش این نسبت استفاده می‌گردد.

$$Precision = \frac{TP}{TP + FP} \quad (۷-۱)$$

- فراخوانی: هدف این شاخص، نمایش نسبت نمونه‌های مثبت واقعی که روش موفق به شناسایی صحیح آن‌ها شده است. این شاخص نشان‌دهنده‌ی توان روش در کشف جامع موارد تقلب است و از فرمول ۱-۸ برای نمایش این نسبت استفاده می‌گردد.

$$Recall = \frac{TP}{TP + FN} \quad (۸-۱)$$

- امتیاز F1: میانگین هارمونیک دقت و فراخوانی است و زمانی که توازن میان این دو شاخص اهمیت داشته باشد، به‌عنوان معیار ارزیابی اصلی در نظر گرفته می‌شود. برای نمایش این توازن از فرمول ۱-۹ استفاده می‌گردد.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (۹-۱)$$

در جدول ۴، عملکرد روش پیشنهادی بر روی داده‌های آموزش و آزمون به‌صورت مقایسه‌ای گزارش شده است. نتایج نشان می‌دهد که روش پیشنهادی در مرحله آموزش به صحت ۹۸/۲۹٪، دقت برابر با ۸۹/۱۹٪، فراخوانی معادل ۹۴/۲۹٪ و امتیاز F1 برابر با ۹۱/۶۷٪ دست یافته است که بیانگر یادگیری مؤثر الگوهای موجود در داده‌ها می‌باشد. در مرحله آزمون نیز عملکرد مدل همچنان پایدار باقی مانده و با دستیابی به صحت ۹۷/۶۷٪، دقت برابر با ۸۴/۸۵٪،

فراخوانی معادل ۹۳/۳۳٪ و امتیاز F1 برابر با ۸۸/۸۹٪، نشان می‌دهد که مدل از قابلیت تعمیم‌پذیری بالایی برخوردار است. نزدیکی مقادیر شاخص‌های عملکرد در مجموعه‌های آموزش و آزمون، بیانگر عدم بروز بیش‌برازش[1] بوده و تأیید می‌کند که روش پیشنهادی قادر است الگوهای واقعی داده را به‌صورت پایدار و قابل اعتماد شناسایی کند. تمامی این نتایج بار دیگر در شکل ۴ که نمایش ماتریس درهم‌ریختگی مدل می‌باشد نیز تایید شده است.

جدول ٤. عملکرد روش پیشنهادی در مجموعه‌های آموزش و آزمون بر اساس معیارهای ارزیابی

Table 4. Performance Evaluation of the Proposed Method on the Training and Test Sets Based on Evaluation Metrics

	Dataset split	Accuracy	Precision	Recall	F1 Score
Our proposed method	Training set	98.29%	89.19 %	94.29%	91.67%
	Test set	97.67%	84.85%	93.33%	88.89%

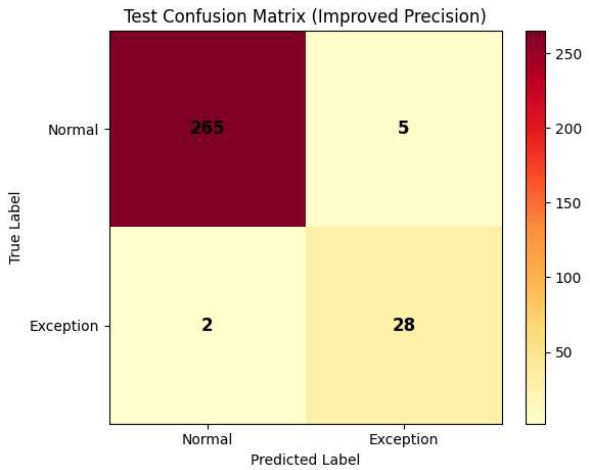


Figure 4. Confusion matrix of the proposed method

شکل ٤. ماتریس درهم‌ریختگی روش پیشنهادی

همچنین در این پژوهش از نمودار منحنی دقت – فراخوانی نیز استفاده شده است. هدف از استفاده از این نمودار، بررسی توان مدل در حفظ تعادل میان جلوگیری از پیش‌بینی‌های نادرست

[1] Overfitting

یا به عبارت بهتر افزایش دقت و پوشش کامل نمونه‌های مثبت واقعی یا همان افزایش فراخوانی است. همان‌طور که در نمودار ۲ نشان داده شده است، نتایج حاصل، حاکی از عملکرد بسیار مطلوب روش در شناسایی طبقه ناهنجار است. منحنی دقت–فراخوانی تقریباً به‌صورت یک خط افقی در نزدیکی دقت برابر با یک قرار گرفته است که نشان‌دهنده پایداری بالای دقت در سراسر طیف مقادیر فراخوانی است. یکی از شاخص‌های کلیدی استخراج‌شده از این نمودار، مساحت زیر منحنی دقت–فراخوانی است که برای این روش برابر با ۰/۹۹۸ گزارش شده است. این مقدار که به‌مراتب نزدیک به عدد یک است، حاکی از عملکرد نزدیک به ایده‌آل روش در تفکیک موارد ناهنجار از موارد عادی می‌باشد.

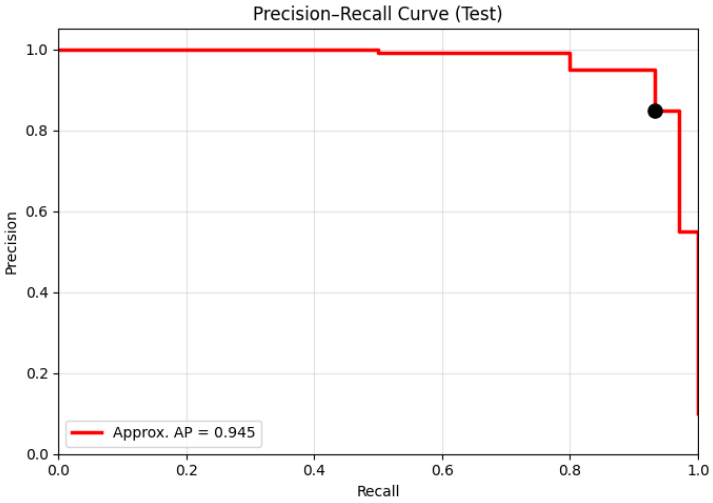


Chart 2. Precision–Recall curve of the proposed method

نمودار ۲. نمودار منحنی دقت–فراخوانی روش پیشنهادی

از سوی دیگر، همان‌طور که در نمودار ۳ نمایش داده شده است، در تحلیل اهمیت ویژگی‌ها بر مبنای مدل جنگل تصادفی، مشخص گردید که ویژگی "ساعت انجام تراکنش" با اختلاف قابل‌توجهی بیشترین نقش را در تصمیم‌گیری روش ایفا می‌کند. پس از آن، متغیرهای انحراف مطلق مبلغ تراکنش نسبت به میانگین مشتری یا abs_amount_dev_vs_cust و اختلاف مبلغ گزارش‌شده با مبلغ واقعی یا AmountDiff در رتبه‌های بعدی قرار دارند. سایر ویژگی‌ها نظیر

نسبت مبلغ، مبلغ تراکنش و مانده حساب، تأثیر کمتری در تصمیم نهایی روش داشته‌اند. این یافته‌ها نشان می‌دهند که زمان و انحراف مطلق مبلغ تراکنش، فاکتورهای کلیدی در پیش‌بینی ناهنجاری محسوب می‌شوند.

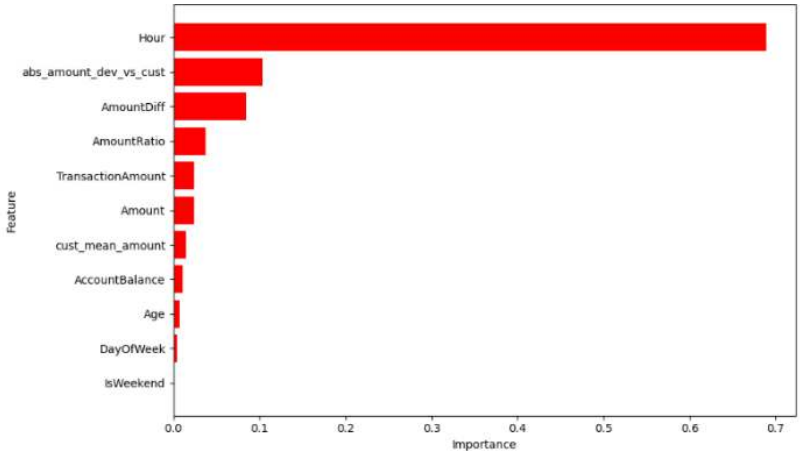


Chart 3. Feature importance of proposed method

نمودار ۳. اهمیت ویژگی‌ها در روش پیشنهادی و میزان تأثیر هر متغیر در فرآیند تصمیم‌گیری

همان‌طور که در شکل ۵ به عنوان یک نمونه درخت تصمیم از روش جنگل تصادفی نشان داده شده است؛ در سطوح بالایی درخت، ابتدا متغیر "ساعت تراکنش" برای تفکیک داده‌ها به‌کار رفته و در مراحل بعدی، ویژگی‌هایی نظیر "مقدار تراکنش"، "مانده حساب"و "نسبت مبلغ" به‌عنوان معیارهای اصلی برای تقسیمات داخلی انتخاب شده‌اند. این ساختار نشان‌دهنده آن است که روش در فرآیند تصمیم‌گیری، ابتدا بر ویژگی‌های رفتاری-زمانی متمرکز شده و سپس به متغیرهای مالی جزئی‌تر توجه می‌کند.

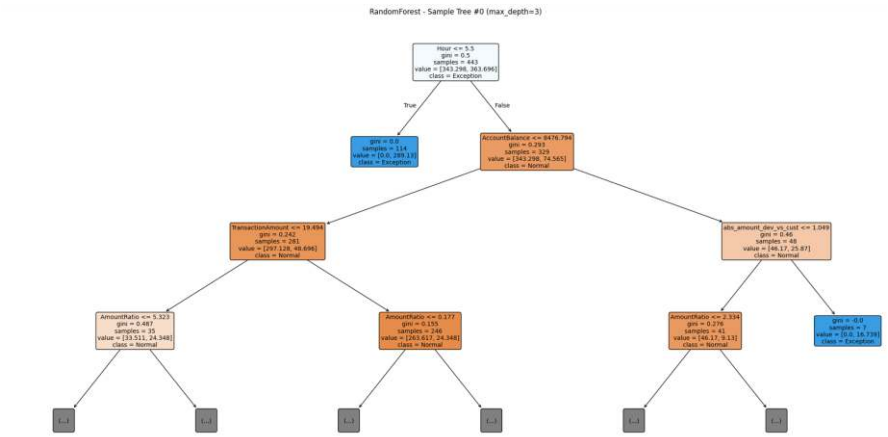


Figure 5. A representative decision tree extracted from our proposed method

شکل ۵. نمونه‌ای از درخت تصمیم استخراج‌شده از روش پیشنهادی

تحلیل نتایج

در این پژوهش، یک روش مبتنی بر یادگیری ماشین برای شناسایی تراکنش‌های ناهنجار طراحی و ارزیابی شد که در آن از ترکیب ویژگی‌های رفتاری مشتری، شاخص‌های مالی و الگوهای زمانی استفاده گردید. نتایج حاصل از ارزیابی عملکرد مدل نشان می‌دهد که روش پیشنهادی از توان تفکیک بسیار بالایی در شناسایی تراکنش‌های مشکوک برخوردار است.

مطابق با نتایج ارائه‌شده ، مدل در مجموعه آموزشی به صحت ۹۸/۲۹٪ و در مجموعه آزمون به صحت ۹۷/۶۷٪ دست یافته است. نزدیکی این دو مقدار بیانگر عدم بیش‌برازش و توانایی مناسب مدل در تعمیم به داده‌های دیده‌نشده است. همچنین مقادیر بالای دقت به‌ترتیب ۸۹٪ در آموزش و ۸۵٪ در آزمون، نشان می‌دهد که مدل در شناسایی تراکنش‌های ناهنجار، نرخ خطای مثبت کاذب بسیار پایینی دارد که این موضوع در کاربردهای مالی و حسابرسی از اهمیت بالایی برخوردار است، زیرا کاهش هشدارهای نادرست موجب صرفه‌جویی قابل توجه در منابع انسانی و عملیاتی می‌شود.

از سوی دیگر، مقدار فراخوانی بالا یعنی ۹۴/۲۹٪ در آموزش و ۹۳/۳۳٪ در آزمون، بیانگر توانایی روش در شناسایی تقریباً تمامی موارد ناهنجار واقعی است. این ویژگی نشان می‌دهد که روش نه‌تنها محافظه‌کارانه عمل نمی‌کند، بلکه توانایی کشف الگوهای پنهان و رفتارهای

غیرعادی را نیز دارد. مقدار بالای امتیاز F1 که بیش از ۸۸٪ است نیز بیانگر تعادل مطلوب میان دقت و فراخوانی بوده و نشان می‌دهد که روش در شرایط عدم توازن داده‌ها عملکرد پایداری دارد.

تحلیل نمودار اهمیت ویژگی‌ها نشان می‌دهد که متغیرهای مرتبط با زمان انجام تراکنش، انحراف مبلغ تراکنش نسبت به الگوی رفتاری مشتری، و نسبت مبلغ تراکنش به میانگین نقش کلیدی در فرآیند تصمیم‌گیری روش ایفا می‌کنند. این موضوع تاییدکننده آن است که رفتارهای غیرعادی زمانی و انحراف از الگوی مالی معمول مشتری از مهم‌ترین شاخص‌های شناسایی ریسک در سیستم‌های حسابرسی هوشمند محسوب می‌شوند. همچنین استفاده از ویژگی‌های مهندسی‌شده مبتنی بر دانش حوزه باعث افزایش قدرت تفکیک مدل نسبت به استفاده صرف از داده‌های خام شده است.

در مجموع، نتایج به‌دست‌آمده نشان می‌دهد که روش پیشنهادی، با ترکیب مهندسی ویژگی هدفمند و الگوریتم جنگل تصادفی، قادر است با دقت بالا و پایداری مناسب، تراکنش‌های ناهنجار را شناسایی نماید. این روش می‌تواند به‌عنوان یک ابزار تصمیم‌یار مؤثر در سیستم‌های حسابرسی هوشمند و مدیریت ریسک مالی مورد استفاده قرار گیرد و زمینه‌ساز توسعه سامانه‌های پیشرفته‌تر در حوزه کشف ناهنجاری‌های مالی باشد.

نتیجه‌گیری

حسابرسی فناوری اطلاعات با افزایش پیچیدگی سامانه‌ها و حجم داده‌ها، بیش از پیش به روش‌های خودکار برای شناسایی موارد پرخطر نیازمند است. با این حال، چالش‌هایی مانند کیفیت و تنوع داده‌ها، تغییر رفتار کاربران، مقیاس‌پذیری روش، تفسیرپذیری نتایج، محدودیت‌های امنیتی و حریم خصوصی همچنان باقی است که توجه به آن‌ها می‌تواند کارایی و اعتماد به روش پیشنهادی را در محیط‌های عملیاتی واقعی افزایش دهد.

در این پژوهش، یک روش مبتنی بر یادگیری ماشین برای تشخیص ناهنجاری ارائه شد که با پیش‌پردازش ساختاریافته داده‌های جدولی (استخراج ویژگی‌های زمانی، اصلاح مقادیر نامعتبر و تکمیل داده‌های گمشده) آغاز می‌شود و سپس ویژگی‌های هدفمند مرتبط با الگوهای زمانی، مغایرت‌های بین‌سیستمی و انحراف از رفتار معمول مشتری استخراج می‌گردد. نتایج نشان داد

متغیرهای زمانی و شاخص‌های انحراف رفتاری از مهم‌ترین عوامل مؤثر در شناسایی ناهنجاری هستند. در ادامه، با تولید شبه‌برچسب مبتنی بر قواعد حسابرسی و آموزش مدل جنگل تصادفی، احتمال وقوع ناهنجاری برای هر تراکنش برآورد و امکان رتبه‌بندی موارد پرخطر برای بررسی حسابرس فراهم شد. ارزیابی تجربی نشان داد صحت مدل در آموزش ۹۸٪ و در آزمون ۹۷٪ است که بیانگر تعمیم مناسب و عدم بیش‌برازش می‌باشد. به‌علاوه امتیاز F1 بیش از ۸۸٪ نشان می‌دهد تعادل مطلوبی میان دقت و فراخوانی برقرار بوده و مدل حتی در شرایط نامتوازن نیز عملکرد قابل اعتمادی دارد. در پژوهش‌های آینده، پیشنهاد می‌شود کارایی روش پیشنهادی با استفاده از داده‌های واقعی و عملیاتی در چند سامانه در محیط‌های حسابرسی داخل کشور و شرایط متفاوت ارزیابی شود تا میزان انطباق آن با ویژگی‌های بومی نظام مالی ایران، میزان پایداری روش در گذر زمان، قابلیت تعمیم آن در مواجهه با تغییر رفتار کاربران، تغییر سیاست‌های کنترلی و به‌روزرسانی سامانه‌ها مشخص گردد. همچنین، برای افزایش تفسیرپذیری نتایج، می‌توان سازوکارهایی برای توضیح تصمیم مدل به‌کار گرفت؛ به‌گونه‌ای که سهم هر ویژگی در تشخیص پرخطر بودن یک تراکنش مشخص شود و همراه با خروجی، یک گزارش قابل فهم برای حسابرس ارائه گردد. از سوی دیگر، با توجه به نامتوازن بودن داده‌ها، توصیه می‌شود از روش‌های مدیریت عدم توازن (مانند افزایش هدفمند نمونه‌های کلاس کم‌تعداد یا وزن‌دهی متفاوت به خطاها) استفاده گردد.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان

- **محمدرضا کیوان‌پور**: هدایت علمی و نظارت بر کلیت پژوهش، ارائه دیدگاه‌های مفهومی در حوزه حسابرسی فناوری اطلاعات، بازبینی علمی ساختار مقاله و تأیید نهایی مسیر پژوهش
- **غزاله کاکاوند تیموری**: طراحی روش‌شناسی کلی پژوهش، تعریف چارچوب حل مسئله و انتخاب رویکرد یادگیری ماشین، مدیریت فرآیند نگارش مقاله و هماهنگی بین بخش‌ها، یکپارچه‌سازی نهایی بخش‌های مختلف مقاله

- **مریم غائبی**: تدوین و نگارش بخش روش پیشنهادی، طراحی چارچوب مدل و منطق الگوریتم‌ها، تشریح فرآیند آموزش و پیش‌بینی مدل یادگیری ماشین، مشارکت در تبیین جنبه‌های فنی روش پیشنهادی
- **نگارنقدیان**: تعریف مسئله پژوهش و ضرورت انجام آن، اجرای ارزیابی‌های تجربی و آزمایش‌های مدل، تحلیل نتایج به‌دست‌آمده و مقایسه عملکرد، تفسیر یافته‌ها از منظر صحت، دقت، فراخوانی و کارایی حسابرسی، مشارکت در نگارش بخش نتایج و تحلیل
- **مهسا بشاورد**: جمع‌آوری و مرور مقالات و پژوهش‌های مرتبط، تدوین بخش پیشینه تحقیق، طبقه‌بندی و تحلیل رویکردهای پیشین در تشخیص ناهنجاری و حسابرسی IT
- **زهرا محمدی‌نژاد**: نگارش بخش مقدمه مقاله، تبیین چالش‌های موجود در حسابرسی فناوری اطلاعات، بیان انگیزه پژوهش و اهداف اصلی مطالعه
- **سیده نازنین نیشابوری‌نژاد**: نگارش بخش نتیجه‌گیری، جمع‌بندی دستاوردهای پژوهش IT، ارائه پیشنهادهایی برای تحقیقات آینده

تعارض منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

منابع

احمدی، سیدجلال؛ فغانی ماکرانی، خسرو؛ فاضلی، نقی. (۱۴۰۳). تکنیک‌های داده‌کاوی و پیش‌بینی تقلب صورت‌های مالی. *دانش حسابداری و حسابرسی مدیریت*، *۱۳*(۵۲)، ۱۵-۲۸.

باقریان کاسگری، عباس؛ رئیسی وانانی، ایمان؛ امیری، مقصود؛ همایون، سعید. (۱۴۰۳). شناسایی تقلب مالی در شرکت‌های سهامی‌عام با استفاده معیارهای مالی وغیرمالی با رویکرد یادگیری ماشین. *مطالعات مدیریت کسب و کار هوشمند*، *۱۳*(۵۰)، ۹۹-۱۴۲. doi: 10.22054/ims.2024.78018.2434

حضوری، علی؛ میرزایی، عباس؛ عفت پرور، مهدی. (۱۴۰۴). یک مرور جامع بر سیستم‌های تشخیص نفوذ با پیشرفت‌های یادگیری ماشین، یادگیری عمیق و چالش‌های نوظهور امنیت سایبری. *دیسکاور مصنوعی هوش*، ۵(۱)، ۳۱۴.

رحمانی، علی؛ معنوی، سمیرا؛ حدادی، نفیسه. (۱۴۰۴). ادغام هوش مصنوعی در حسابرسی؛ چالش‌ها و مزایا. *حسابرسی سیستم‌ها و فناوری اطلاعات*. *۱*(۱)، ۱-۲۷. doi: 10.22034/jista.2025.528769.1051

رضائی پیته نوئی، یاسر؛ اصغری شلمانی، مصطفی؛ دلیری دهنه، حسین. (۱۴۰۰). معرفی یک چارچوب مناسب سازماندهی برای کاربردهای داده کاوی در حسابداری و حسابرسی: مروری بر تکنیک‌های پرکاربرد طبقه بندی داده‌های مالی. *نشریه علمی رویکردهای پژوهشی نوین مدیریت و حسابداری*، ۵(۱۹)، ۱۵۰۷-۱۵۲۵. https://www.majournal.ir/index.php/ma/article/view/1207

رهنمای رودپشتی، فریدون. (۱۳۹۱). داده‌کاوی و کشف تقلب‌های مالی. *دانش حسابداری و حسابرسی مدیریت*، ۱(۳)، ۱۷-۳۳. https://www.jmaak.ir/article_7349.html.

سلطانی، مریم؛ محمدی نژاد، زهرا؛ حسام محسنی، عبدالرضا. (۱۴۰۲). ارزیابی الگوریتم مسیریابی BGP. *پنجمین کنفرانس بین‌المللی محاسبات نرم*. https://civilica.com/doc/1967023/.

فضل‌زاده، علیرضا؛ حقیقت، جعفر؛ پورکیوان، فرانک؛ احمدیان، وحید. (۱۳۹۸). آزمون عملکرد الگوریتم جنگل‌های تصادفی و الگوریتم شبکه عصبی عمیق در استراتژی آربیتراژ آماری. *مهندسی مالی و مدیریت اوراق بهادار (مدیریت پرتفوی)*، ۱۰(۴۰)، ۳۴۹-۳۶۴. https://sid.ir/paper/197626/fa

کاظمی، توحید؛ پیری، پرویز. (۱۴۰۱). پیش‌بینی طرح تقلب در گزارشگری مالی با استفاده از رویکرد یادگیری ماشین در فضای چند کلاسه. *پژوهش‌های تجربی حسابداری*، ۱۲(۴)، ۲۸۰-۲۵۵.

کریمی فر، ابوطالب؛ دارابی، رویا؛ حمیدیان، محسن. (۱۴۰۴). بررسی عملکرد رویکردهای رگرسیون و یادگیری عمیق برای کشف تقلب صورت‌های مالی با تمرکز بر ابعاد فشار/ انگیزه و فرصت. *پژوهش‌های تجربی حسابداری*، ۱۵(۳)، ۲۸۲ -۲۴۱.

References

Ahmadi, S.J., Faghani Makarani, K., & Fazeli, N. (2024). Data mining techniques and financial statement fraud prediction. *Journal of Management Accounting and Auditing Knowledge*, *13*(52), 15–28. https://www.iaaaas.com/article_223291.html (in Persian)

Alsalmi, E., Alhuzali, A., & Alhothali, A. (2025). Log-based anomaly detection of system logs using graph neural network. *Computers, Materials and Continua*, *86*(2), 1–20.

Bagherian Kasegari, A., Raeisi Vanani, I., Amiri, M., & Homayoun, S. (2024). Detection of financial fraud in public companies using financial and non-financial criteria with a machine learning approach. *Intelligent Business Management Studies*, *13*(50), 99–142. https://ims.atu.ac.ir/article_18048.html (in Persian)

Chacko, N., Ravichandaran, M., Rao, R., & Chandra Shenoi, S. (2012). An anomalous cooling event observed in the Bay of Bengal during June 2009. *Ocean Dynamics*, *62*(5), 671–681.

Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint*, arXiv:1901.03407.

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*.

De la Cruz Cabello, M., Sales, T., & Machado, M. (2025). AIOps for log anomaly detection in the era of LLMs: A systematic literature review. *Intelligent Systems with Applications*, 200608.

De Vries, T. (2022). *Anomaly detection in IT audit: The possibilities and potential in the domain of IT audit* [Master's thesis, University of Turku].

Dzuranin, A. C., & Mălăescu, I. (2016). The current state and future direction of IT audit: Challenges and opportunities. *Journal of Information Systems*, *30*(1), 7–20.

Fazlzadeh, A., Haghighat, J., Pourkian, F., & Ahmadian, V. (2019). Testing the performance of the random forest algorithm and the deep neural network algorithm in a statistical arbitrage strategy. *Financial Engineering and Securities Management*, *10*(40), 349–364. https://sid.ir/paper/197626/fa (in Persian)

Gantz, S. D. (2013). The basics of IT audit: Purposes, processes, and practical information. *Elsevier*.

Hasan, M. T., & Ahmed, I. (2025). AI-driven anomaly detection for data loss prevention and security assurance in electronic health records. *Review of Applied Science and Technology*, *4*(3), 35–67.

Hilal, W., Gadsden, S., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, 116429.

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, *5*(1), 314. (in Persian)

Kakavand Teimoory, G., Keyvanpour, M. R., & Ghaebi, M. (2025). Explainable diabetes prediction via hybrid data preprocessing and ensemble learning. *International Journal of Web Research*, *8*(4), 51–66.

Karimi Far, A., Darabi, R., & Hamidian, M. (2025). Evaluating the efficiency of regression and deep learning approaches in detecting financial statement fraud with a focus on the justification dimension. *Accounting and Auditing Studies*, *15*(3), 241-282. https://journals.alzahra.ac.ir/article_8266.html?lang=en (in Persian)

Kazemi, T., & Piri, M. (2022). Predicting financial reporting fraud schemes using a multi-class machine learning approach. *Empirical Research in Accounting*, *12*(4), 255–280. https://jera.alzahra.ac.ir/article_6880.html (in Persian)

Mohan, C. K., & Mehrotra, K. G. (2017). Anomaly detection in banking operations. *IDRBT Journal*, 16.

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*, 122156.

Niu, W., Liao, X., Huang, S., Li, Y., Zhang, X., & Li, B. (2024). A robust wide and deep learning framework for log-based anomaly detection. *Applied Soft Computing, 153*, 111314.

Okolie, S., Amadi, C., Odii, J., Nwokorie, E., & Onyemauche, U. (2025). Anomaly detection in heterogeneous cybersecurity data. *Franklin Open*, 100426.

Patel, T., & Iyer, S. S. (2025). SiaDNN: Siamese deep neural network for anomaly detection in user behavior. *Knowledge-Based Systems*, 113769.

Pinto, S. O. & Sobreiro, V. A. (2022). Literature review: Anomaly detection approaches on digital business financial systems. *Digital Business*, 2(2), 100038.

Quinn, M., & Strauss, E. (2018). *The Routledge companion to accounting information systems*. Routledge.

Rahmani, A., Manavi, S., & Haddadi, N. (2025). Integrating artificial intelligence into auditing: Challenges and benefits. *Systems Auditing and Information Technology*, *1*(1), 1–27. (in Persian)

Rahnamay Roudposhti, F. (2012). Data mining and financial fraud detection. *Knowledge of Accounting and Management Auditing*, *1*(3), 17–33. https://sid.ir/paper/238039/fa (in Persian)

Ram, Murugan & Khamar (2024). AI-driven network anomaly detection for enhanced cybersecurity and performance. *Proceedings of the 9th International Conference on Communication and Electronics Systems (ICCES), IEEE*.

Rezaei Pithenoei, Y., Asghari Shalmani, M., & Deliridehbaneh, H. (2021). Introducing a suitable organizing framework for data mining applications in accounting and auditing: A review of popular techniques for financial data classification. *Journal of Modern Research Approaches in Management and Accounting*, *5*(19), 1507–1525. https://www.majournal.ir/index.php/ma/article/view/1207 (in Persian)

Romney, M. B., Stainbart, P. G., Summers, S. L., & Wood, D. A. (2006). *Accounting information systems*. Prentice Hall.

Soltani, M., Mohammadinejhad, Z., & Mohseni, A. H. (2024). BGP routing algorithm evaluation. *International Conference on Soft Computing*. https://civilica.com/doc/1967023/ (in Persian)

Sun, Y., Keung, J., Yang, Z., Liu, S., & Liao, Y. (2025). SemiSMAC: A semi-supervised framework for log anomaly detection with automated hyperparameter tuning. *Information and Software Technology*, 107869.

Thiprungsri, S., & Vasarhelyi, M. A. (2011). Cluster analysis for anomaly detection in accounting data: An audit approach. *International Journal of Digital Accounting Research*, *11*.

Uchida, H., Tominaga, K., Itai, H., Li, Y., & Nakatoh, Y. (2024). Improving log anomaly detection via spatial pooling: Combining SPClassifier with ensemble method. *Cognitive Robotics*, *4*, 217–227.

Wu, J., Zhang, S., Liu, H., & Yang, W. (2025). AAR-Log: A robust log anomaly detection method resisting adversarial attacks. *Computer Networks*, 111471.