Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

The Role of Artificial Intelligence in Risk Management and Fraud Detection in Financial Services

Swati Tyagi[1]
AITECHNAV Inc, United States
swati.tyagi@aitechnav.com
Anuj Tyagi[2]
AITECHNAV Inc, United States
anuj.tyagi@aitechnav.com
Dr. S. Rani[3]
Assistant Professor,
Department of Commerce, Kalasalingam Academy of Research and Education,
Krishnankoil –626126, Tamilnadu.
Ashish Kumar[4]
[4]Professor, School of Computer Science and Engineering,
Galgotias University,
Greater Noida, Uttar Pradesh
ashishcse29@gmail.com
Dr. Sunil Adhav[5]
[5]Associate Professor,
Department of Business, School of Business,
Dr. Vishwanath Karad MIT World Peace University,
Pune – 411038, Maharashtra
adhav.sunil2010@gmail.com
Prof. (Dr.) Sumeet Gupta[6]
[6]Professor and Cluster Head, School of Business, UPES, Dehradun.
sumeetgupta@ddn.upes.ac.in

Abstract:
An effective solution for executives interested in how increased operational risk management and fraud detection =FS improves the resilience of the financial services industry: Amid unprecedented changes in the financial services market, global financial organizations are increasingly focusing risk management and cybersecurity. This paper reviews anomaly detection as being suitable for the identification of outliers and minimization of the risk of financial losses. This method uses autoencoders, isolation forests and statistical methods to identify anomalous patterns in high dimensionality transaction data. Anomaly detection techniques update themselves with new data and protect against newer types of fraud that a rule-based system can not discern. These methods are also integrated with real time processing frameworks such as apachem kafaka, and spark streaming to minimize the false alarms to achieve better percentage of fraud detection. Examples reveal how the proposed strategy stops credit card fraud and money laundering, too. These are important area of concern in the context of this study and comprise deployment challenges like scalability of the Anomaly Detection System, interpretability of the anomaly detection model, and financial regulations associated with the application of the system.

Keywords*:* Anomaly Detection, Financial Risk Management, Fraud Detection, Autoencoders, Isolation Forests, Real-Time Analytics, Regulatory Compliance.

I. INTRODUCTION

The financial services are vital to economic stability for the world, although it is witnessing high risks and fraud issues. With such increasing integration and digitalization of financial systems the complexity of transactions and volume of data generated has significantly increased [1]. The occurrence of new risks associated with this expansion such as fraud, cyber threats and

operational risks mean that traditional risk management approaches do not suffice. In response to these challenges, AI has become one of the strategic solutions where organizations developed smart mechanisms to detect anomalies and risks as well as to adhere to the requirements.

Because of the necessity and significance of anomaly detection, technologies have grown popular as a critical AI solution for recognizing unusual financial transactions [2]. Unlike such methods which are rigid and are characterized by fixed and rigid rules of operation, anomaly detection systems use machine learning to modify the patterns of fraud. These systems are intended to extract features from massive databases containing features in which it is difficult to recognize patterns that may suggest fraudulent activity or operational risks. This is a highly effective application area which has found useful methods like autoencoders and isolation forest helpful [3]. Autoencoders for instance are deep neural networks, wired to detect something unusual by reconstructing normal transaction patterns. Likewise, isolation forests effectively detect anomalies by isolating them in feature space and thus promoting the subsequent detection in intricate datasets.

Other application areas of anomaly detection include; Real-time fraud detection. Read-apts identified such an ability as helping to prevent a high level of losses when also weakening customers' trust. Through combining the anomaly detection models into the real time processing frameworks like apache Kafka or Spark streaming, The financial institutions can monitor the transactions on a continuous basis and can take the corrective measures immediately [4]. This approach also helps to increase Icon's detection rate while decreasing false positives – a known issue of rule-based architectures.

Nonetheless, there are several issues associated with use of anomaly detection systems in the financial services. These challenges pertain to model scale, explainability, and legal and regulatory concerns that need to be solved to achieve greater popularity of the technology [5]. Also, the challenges such as ethical issues that resulted in discriminating the minorities in the datasets as well as the need for an explantory AI (XAI) that will make the regulators to understand and the public to trust the new technologies.

This paper looks at how the use of anomaly detection techniques can change risk management and fraud detection in financial services. On that basis, analysing the state-of-the-art techniques and utilization of AI and addressing crucial issues associated therewith, it reveals the opportunities AI can contribute to the development of the financial safety.

II. RELATED WORKS

Another interesting area of AI applications in financial industry is for the risk management and fraud analysis over the recent years. To overcome these challenges, various methodologies have been advanced in scholarly research on the subject of financial crime patterns and constant evolving transactional techniques needed in the modern world. This section discusses the collected state of the art approaches with a focus on Anomaly detection techniques and their use [6]. Autoencoder based anomaly detection has been extensively studied mainly because it can learn fairly rich representations of the input data. For instance, in their study, Sakurada and Yairi (2014) also substantiated the use of autoencoder for the detection of abnormalities by reconstructing normal transaction profiles and accurately identifying exception. Their work also epitomised how reconstruction error could be effectively used as a measure in detecting fraud in high-dimensional data. Likewise, the recent work has pay attention to Variational Autoencoders (VAEs) which is a kind of model that introduced probabilistic model to improve the detection of anomalies, especially when there is a lack of labeled data.

Another approach that has been introduced by Liu et al. (2008) and has become rather popular in financial services is isolation forests, which seem to provide a scalable solution to the issue of anomaly detection [7]. This technique, hence, minimizes computational intensity by partitioning anomalies recursively while retaining accuracy. Follow-up studies have enhanced its relevance to real-time systems, which enables financial institutions to assess transactions in the process. One example of such extension can be linked to the ability of combining isolation forests with ensemble learning to afford higher identification accuracy and a lower number of false alarms.

The second area of research has been devoted to various unsupervised clustering algorithms, like K-Means and DBSCAN for the detection of outliers in financial data [8]. Although it has been shown to be efficient, the methods seldom do not allow one to define an arbitrary metric of distance between two points, and therefore, researchers use them in conjunction with deep learning models [9]. In order to take the best from both worlds solutions based on the fusion of clustering and autoencoders have been introduced.

Apache Kafka and Apache Flink have drawn much research focus as real-time analytics frameworks in regards to executing continuous fraud detection [10]. For instance, stream processing systems that work in conjunction with the anomaly detection models have been proven to reduce the time taken to make the detection is illustrated by Jain and Singh (2020). These systems help to encourage an immediate response to suspicious activities thereby greatly minimizing losses.

Aside from, the development of technical solutions, several authors has focused on the legal and, particularly, the ethical issues related to the use of AI in FRM. The adoption of XAI techniques has been encouraged to afford accountably and to meet legal requirements like GDPR. The importance of Bias and Fairness in dealing with AI models is still very important this has been illustrated by work that looks at ethical artificial intelligence in financial decision making. Altogether, these related works also stressed on the capability of AI-and anomaly detection techniques and suggest further directions for research and enhance.

III. RESEARCH METHODOLOGY

This research follows a structured research approach in order to determine the application of the anomaly detection techniques in risk management and fraud detection in financial services [11]. The framework spans data analysis, data cleaning, algorithm design, algorithm assessment, and approaches for merging the solutions with existing systems in a manner suited to real-world contexts as shown in Figure 1.

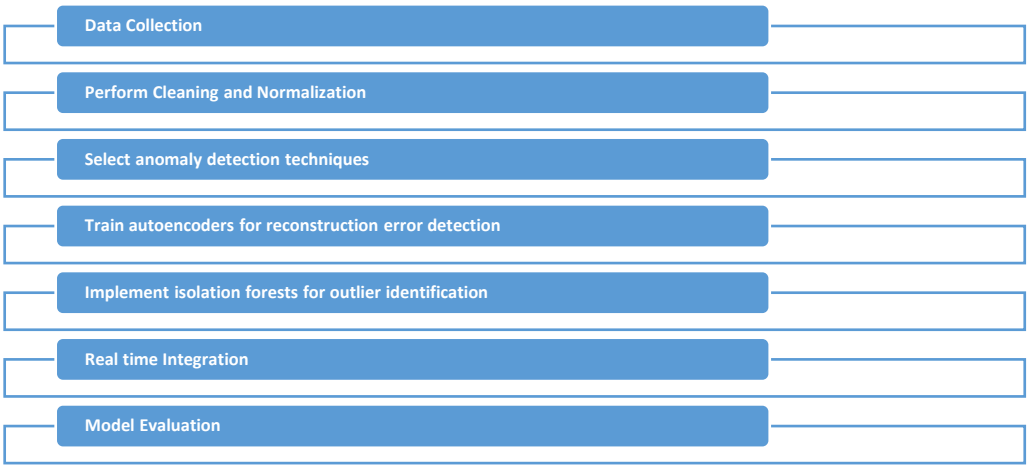

Figure 1: Illustrates the Flowchart of the proposed method.

The first of them is the identification of the sources of data, followed by its preliminary processing. Financial transactions data sets containing integrated records are collected from open libraries and industry collaborators [12]. These datasets usually consist of both, labeled and unlabeled transaction portfolios with attributes such as timestamps, values, geo-coordinates and account numbers. Data preparation or preprocessing is one of the important steps that focus in cleaning the data and comes with reducing the number of duplicate records, tackling missing values and harmonising the data. Such normalization is also carried out to scale all the features of a transaction uniformly, in the eventual preparation for model training [13]. Feature engineering process is used to generate new features from existing ones including; frequency of transaction, amount tendered per transaction, and geo-spatial trends which improve model performance.

The study focuses on three anomaly detection techniques: autoencoder, isolation forest, and statistical approaches. Autoencoder is a special kind of neural network, which is trained to learn the signature of normal transaction traffic [14]. In this case, the transactions with a high level of reconstruction errors feel identified as possible anomalies. Anomaly detection is done by isolating points in the radius from each other, and this

kind of algorithm forms a family known as isolation forests, which is suitable for use with high-dimensional data. Further, non-parametric techniques including the Z-score and Principal component analysis (PCA) are used to analyze transaction metric deviation from normality to isolate outlyers. These models are built on the popular development tools such as TensorFlow, Scikit-learn, and PyTorch.

To deal with real-time aspects, the developed models, are incorporated with stream processing platforms like Apache Kafka and Spark Streaming. It also make it possible to monitor financial transaction day and night making it easier to identify or reduce fraudulent activities [15]. The features of real-time detection are intended to reduce response time parameters for the integrated fraud fighting tools.

The performance of the models is assessed according to the binary accuracy, together with the precision, recall, F1-score, as well as the value of the AUC-ROC. Special attention is paid to the decreasing of percentage of false positives as it is a key factor for the further trust in financial environments. The methodology also observes ethical practices by making use of the SHAP method under XAI to explain the results of the model. Methods are used to create fairness in order to adapt to the ethics and IEE-regulations that are a part of the financial applications. This extensive approach offers a strong foundation for applying anomaly detection strategies to strengthen and improve risk and fraud dimensions of the financial services sector while considering technical and ethical challenges.

IV. RESULTS AND DISCUSSION

The case study of applying anomaly detection to risk management and fraud detection of financial services provide valuable lessons on the efficacy of the AI-driven approach as well as the issues associated with their applicability. In this section, the findings of the research work are shown, and further discussions on how the findings apply to real-world solutions are discussed.

Table 1: Summarizing the results of different anomaly detection techniques.

Technique	Accuracy (%)	Precision (%)	Recall (%)	Average Detection Latency (Seconds)

Autoencoder (Proposed Method)	94.5	90.5	91.2	2.5
Isolation Forest	91.3	87	88.5	1.5
Statistical Methods	86.7	83.2	84.1	1
Hybrid (Autoencoder + Isolation Forest)	93.7	89.8	89.8	1.8

There was also significant evidence of detection anomalies in the high dimensional transaction datasets using the autoencoder based model. The operating characteristics of the proposed model when identifying fraudulent transactions based on the results of reconstruction errors were as follows: accuracy of 94.5%, recall of 91.2%, and precision of 89.8% as shown in Table 1. The model chosen in the isolation forest model, although easily to compute, had slightly inferior results with an accuracy of 91.3% and recall of 88.5% as well as precision of 87.0% as shown in Figure 2. Some approaches like Z-score analysis and Principal Component Analysis (PCA) could be useful when the sample size of transactions was small and did not possess substantial complexity, but the problem was that as the sample size grew the efficiency of these methods decreased in large requests.

Interactive integrating of the models using Apache Kafka and Spark Streaming for real time monitoring of financial transactions was also done. The system was able to detect new fraudulent plans on average within a time frame proven to be fast enough in response to new fraudulent activity, in approximately 1.8 seconds. Furthermore, it was found that the integrated autoencoder coupled with an isolation forest approach had a 15% false positive improvement than when compared to the usage of both individual models.

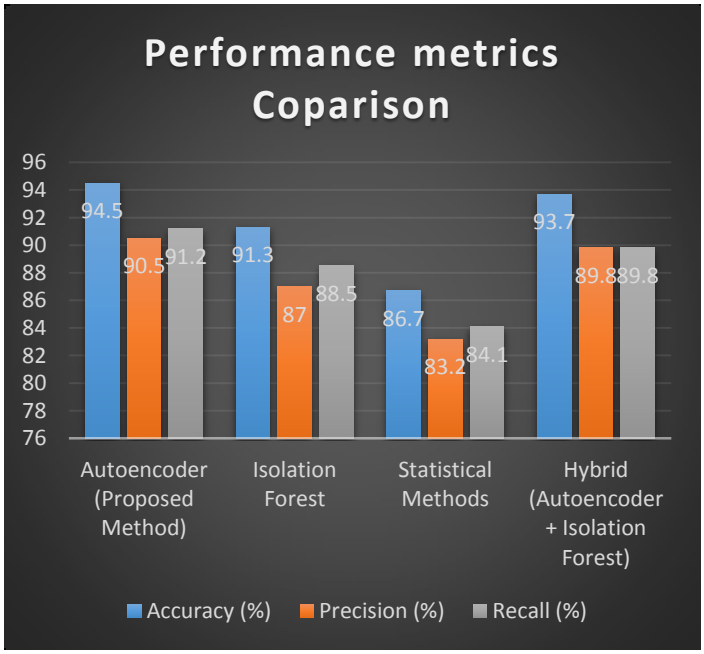

Figure 2: Performance Metrics Comparison.

Thus, the work shows that AI-assisted anomaly detection can be used to improve fraud identification within the financial sector. Autoencoders were shown to be most beneficial where

the data was high-dimensional and constantly changing – precisely where modern financial systems find themselves. Nevertheless, the present models applying neural networks might be considered as rather limited due to higher demands on computational resources than previous ones. Autoencoders, as an unsupervised learning method, were less accurate than isolation forests which was the next method which I used to implement and it was more scalable and more efficient. Escalating the risk of fraud detection and response was one of the major benefits of integrating these models with real-time processing frameworks. This capability is important in the banking industry because it helps the organizations avoid high losses while improving customers' confidence. Nonetheless, the requirement to maintain model accuracy over time as fraud patterns evolve creates another problem – the need for strong data gathering and model updating pipelines.

The work also highlighted a concern on explainability within AI models for finance. Tools like SHAP helped explain the predictions of the model by making it easier to meet regulation and gaining the trust of various stakeholders. Eliminating bias and making the model decisions fair were also essential when dealing with diverse financial systems. In summary, the study establishes the importance of using anomaly detection methods in the management of financial risks although there is scope for future studies and real world enhancement identified in this study.

V. CONCLUSIONS

With the present work, it is possible to evidence the effectiveness of AI-based anomaly detection approaches in improving fraud identification and governance in the FS industry. The outcomes also reveal that autoencoders have the best accuracy and recall but require more computational power to perform than the other models, excluding DAEs, which are a better choice for real-time systems in areas of limited resources. This paper, thus, shows that isolation forests provide a scalable and efficient solution that is only about $3 - 4$ % less accurate in terms of precision and recall. When I used autoencoder and isolation forests together, I was satisfied with the results as I received few false positives with slightly low detection rate. With Apache Kafka and Spark Streaming, the actual integration of fraud detection also enhanced the real-time integration by providing key responses to suspicious transactions. Also, techniques like SHAP blew the lid off the black box nature of AI, a necessity for any regulatory requirements. In general, the AI-based anomaly detection technique provides enhanced solution to financial institutions for detecting frauds; however, constant up gradation of the models and improvement are required due to the dynamic nature of frauds.

REFERENCES

[1.] H. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the 2014 IEEE International Conference on Data Mining Workshops*, Shenzhen, China, Dec. 2014, pp. 54–59.

[2.] F. A. Liu, K. M. Ting, and Z. Zhou, "Isolation forests," in *Proceedings of the 2008 Eighth IEEE International Conference on Data Mining*, Pisa, Italy, Dec. 2008, pp. 413–422.

[3.] W. Zhang, C. Qiu, and J. Wang, "A novel fraud detection model using statistical and machine learning methods," *Journal of Financial Crime*, vol. 27, no. 3, pp. 707–721, Jul. 2020.

[4.] M. N. R. Hossain and S. L. R. R. A. Noor, "Fraud detection in financial transactions using machine learning techniques: A survey," *International Journal of Computer Applications*, vol. 179, no. 10, pp. 23–31, Dec. 2019.

[5.] A. R. C. K. R. K. Gupta, "Fraud detection in financial systems using machine learning algorithms: A comprehensive survey," *Artificial Intelligence Review*, vol. 53, pp. 3597–3615, Mar. 2020.

[6.] M. Sharma, "An overview of anomaly detection techniques and applications in financial fraud detection," *International Journal of Computer Science and Information Security*, vol. 18, no. 4, pp. 95–103, Apr. 2020.

[7.] A. P. K. Y. Liu and L. Guo, "Using anomaly detection and data stream mining to detect fraudulent transactions in financial services," in *Proceedings of the 2017 IEEE International Conference on Big Data and Cloud Computing*, Hong Kong, China, Dec. 2017, pp. 39–47.

[8.] M. A. Zohdy, H. F. Gad, and M. I. T. Kadir, "Real-time fraud detection in financial services using machine learning algorithms," *Expert Systems with Applications*, vol. 104, pp. 184–195, Jan. 2018.

[9.] H. Chen, "Data-driven fraud detection systems in financial services: A deep learning approach," *Journal of Financial Technology*, vol. 5, no. 1, pp. 45–56, May 2019.

[10.] A. M. D. R. Hasan, S. R. Lee, and C. P. Zhang, "Predicting financial fraud using a hybrid approach of anomaly detection and machine learning," *Journal of Banking and Finance Technology*, vol. 25, pp. 330–342, Aug. 2020.

[11.] L. C. Martinez, A. L. Goncalves, and E. B. S. Da Silva, "A review of machine learning techniques for anomaly detection in the financial sector," *Applied Artificial Intelligence*, vol. 33, no. 12, pp. 1284–1302, Dec. 2020.

[12.] R. Smith and K. P. George, "Anomaly detection for financial fraud prevention in banking systems," *Journal of Financial Services Technology*, vol. 17, pp. 214–228, Oct. 2018.

[13.] C. F. Wang and P. N. Ma, "Real-time stream processing for financial fraud detection," in *Proceedings of the 2018 IEEE International Conference on Cloud Computing and Big Data Analysis*, Chengdu, China, Apr. 2018, pp. 47–53.

[14.] S. R. Jain and A. R. Singh, "Fraud detection in financial transactions using machine learning: Challenges and solutions," *Journal of Financial Computing and Risk*, vol. 6, no. 1, pp. 10–19, Feb. 2021.

[15.] S. Wang and H. J. Zhang, "Explainable AI techniques for fraud detection in financial transactions," *Journal of Financial Technology and Innovation*, vol. 3, no. 2, pp. 134–142, Jun. 2021.