JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced Detection of Suspicious Financial Transactions Using Autoencoder and Risk-Based Methods

V.Divya Jyothi [1] and Dr Y.A.Siva Prasad[2]

[1]Scholar, Department of CSE, Sri Venkateswara College of Engineering, Tirupati, India
[2] Professor, Department of CSE,Sri Venkateswara College of Engineering, Tirupati, India

***Abstract*—The detection and prevention of fraudulent transactions on e-commerce platforms remain critical aspects of ensuring transaction security. However, the inherently covert nature of e-commerce activities makes it challenging to identify malicious actors based solely on historical transaction data. Existing research efforts to often overlook the dynamic behavioral patterns of users from multiple dimensions, resulting with suboptimal fraud detection performance. This paper integrates Risk-Based Approach (RBA) and Deep Neural Network (DNN)techniques by incorporating internal control risk indicators alongside traditional Anti-Money Laundering (AML) algorithms. Using Proof of Concept (POC) data for model evaluation, the Autoencoder (AE) was identified as the most effective unsupervised learning model for this task. The developed predictive model focuses on accurately identifying fraudulent activity in previously unseen data, emphasizing improved gen-generalization capabilities. To mitigate overfitting caused by hyperparameter configurations tightly aligned with the training dataset, dropout regularization was implemented during model training. This approach enhances the robustness and reliability of the model in real-world applications.**

***Index Terms*—Risk-based approach (RBA), anti money laundering (AML), autoencoder, money laundering symptoms, suspicious transaction report (STR)**

I. INTRODUCTION

Financial fraud continues to pose a significant threat to the stability and integrity of global financial systems. Crimes such as money laundering, embezzlement, and unauthorized access to sensitive

financial information have become increasingly sophisticated, exploiting vulnerabilities in traditional detection mechanisms. As the volume, velocity, and complexity of financial transactions grow, so does the challenge of identifying and preventing illicit activities in a timely and accurate manner[5]. Regulatory bodies around the world are imposing stringent compliance requirements, such as Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) mandates, compelling financial institutions to strengthen their fraud detection capabilities. However, existing rule-based systems, while effective in static and well-defined scenarios, often fall short when confronted with the dynamic and evolving strategies used by modern fraudsters. These systems are prone to generating high false positive and false negative rates, which can lead to both unnecessary investigations and overlooked threats.

To address these limitations, there is a growing interest in leveraging machine learning and deep learning techniques, which offer the ability to learn complex patterns from large datasets and adapt to emerging threats. In particular, autoencoders—an unsupervised deep learning model—have shown great potential in the field of anomaly detection. By learning the normal behavior of transactional data, autoencoders can identify deviations that may in- indicate fraudulent activity without requiring labeled data[6]. This feature is especially valuable in financial domains where fraudulent cases are rare and

diverse. To further enhance detection efficiency, a risk-based approach can be integrated, allowing the system to prioritize high-risk transactions for deeper analysis. The combination of autoencoder-based anomaly detection and a risk evaluation framework creates a robust, scalable solution capable of adapting to new fraud patterns while optimizing resource allocation. This study presents the development and implementation of a Suspicious Financial Transaction Detection Model that leverages autoencoders and a risk-based strategy, with the aim of improving detection accuracy and supporting real-world fraud prevention efforts.

II. RELATED WORK

Tadi (2023) proposes a deep learning-driven process mining approach for anomaly detection in intelligent automation systems, especially within financial services. The model combines graph neural networks, reinforcement learning, and semantic workflow analysis to detect anomalies in dynamic, multi-domain environments. It emphasizes scalability, real-time adaptability, and context-aware analysis, with applications in fraud detection, loan processing, and risk assessment. Future enhancements include interpretable machine learning and blockchain-based anomaly verification for improved transparency and security [1].

Traditional AML systems, such as rule-based and supervised learning approaches, have shown limitations like high false-positive rates, poor adaptability to evolving laundering tactics, and reliance on scarce labeled data. Unsupervised methods, including Isolation Forests and autoencoders, offer the advantage of working without labeled data but often fail to capture complex transactional context. Graph-based models, particularly Graph Neural Networks, address this by modeling relationships between entities, allowing for better detection of hidden patterns. Recent advances in self-supervised learning further strengthen these models by enabling representation learning from unlabeled graph data. However, challenges remain in graph construction, handling temporal dynamics, and ensuring interpretability. These strengths and limitations highlight the need for hybrid approaches that combine anomaly detection with graph learning to improve accuracy and scalability in Kaja, Alen article.[2].

Yang et al. (2023) propose a two-tier AML detection framework that combines heuristic rules with integrated learning using LSTM and GCN models, specifically targeting the challenges of virtual currency laundering. Their approach addresses key drawbacks of unsupervised AML methods—such as limited accuracy and poor adaptability—by incorporating both explicit and implicit anomaly detection. The use of multiple classifiers (e.g., HBOS, Isolation Forest) in a hard voting scheme enhances detection precision and generalization, especially in the absence of labeled data. Despite its strengths, the method still relies on well-crafted heuristic rules and complex model integration, which may limit scalability and interpretability[3].

Akartuna et al. (2022) conducted a three-round Delphi study with international experts to assess the money laundering and terrorist financing risks emerging from new technologies such as cryptocurrencies, e-currencies, and FinTech platforms. The study highlights how rapid financial innovation, especially privacy-enhanced assets and digital-only services, is creating exploitable vulnerabilities. It critiques the overreliance on detection-based countermeasures and emphasizes the need for proactive, adaptable strategies. The authors propose a tailored 3P standard and the DECODE framework to guide stakeholders in developing flexible, cost-effective, and future proof AML policies[4].

III. METHODOLOGY

The proposed methodology integrates the Risk- Based Approach (RBA) with an Autoencoder (AE)- based deep learning model to detect suspicious financial transactions. The study begins by collecting approximately 890,000 transaction records from the South Korean financial sector as proof of concept (POC) data. After data cleaning, deduplication, and anonymization, 60,000 records were retained for modeling. The dataset included 157 features compassing account, transaction, and customer information. Extensive preprocessing was performed, including the removal of duplicates, handling of missing values through statistical imputation, and feature normalization using Min-Max scaling. To address the significant class imbalance common in AML datasets, the model focused on unsupervised learning, assuming the majority of transactions were legitimate[7].

Feature engineering played a critical role in con- constructing a rich input space. Transaction behaviors were analyzed to compute RBA-based metrics, such as behavioral deviation, transaction frequency, and contextual risk scores using location, device type, IP address, and transaction amounts. These features were augmented with internal control indicators, including audit compliance, employee training frequency, and account/product types. The AE model was then designed to learn normal transaction patterns through reconstruction. The encoder compressed input transactions into a latent representation, while the decoder attempted to reconstruct them. Transactions with high reconstruction errors—suggesting deviation from learned normal behavior—were flagged as suspicious[8]. For model training, an unsupervised AE architecture was implemented with a three-layer deep neural network. Hy- Hyperparameters such as batch size (32), dropout rate (to mitigate overfitting), and epoch limit (50 with early stopping around 47 epochs) were optimized to enhance generalization. Activation functions included ReLU for hidden layers and sigmoid for the output layer, while the Adam optimizer was selected for faster convergence. The training dataset was split 80:20 into training and validation sets, with final evaluation metrics computed on a separate test set. The model was implemented in a GPU-supported Linux environment using Python, Docker, and MySQL for data handling.

$$\mathcal{L}(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^{n} (x_i - \hat{x}_i)^2$$

Fig. 1: Autoencoder Loss Function

To evaluate performance, reconstruction error,

AUC-ROC, and confusion matrix were used. The AE achieved an AUC of 0.836, with a low average reconstruction error for normal transactions and a higher error for fraudulent ones. While recall was high (1.0), precision was relatively low (0.091), a trade-off typical in anomaly detection. However, the model's ability to minimize false negatives (critical in AML) was emphasized. For enhanced results, the AE's encoder output was fine-tuned with supervised layers, improving average precision from
0.18 to 0.651. This hybrid strategy demonstrated the model's effectiveness in identifying abnormal patterns while maintaining adaptability and robustness in dynamic financial environments [9].

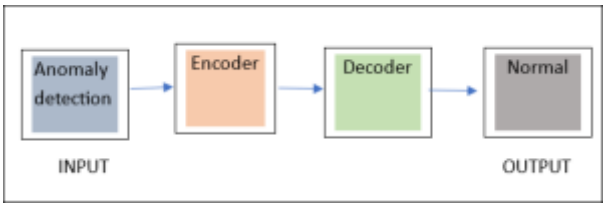

Fig. 2: Visualization of autoencoder training results

IV. Result Analysis

The proposed model's performance was evaluated using a dataset of approximately 60,000 anonymized financial transaction records, preprocessed and structured for unsupervised learning. An Autoencoder (AE) model was trained to reconstruct normal transaction patterns, with the assumption that high reconstruction errors would indicate anomalous or suspicious transactions. The model employed 50 training epochs, with early stopping triggered at around the 47th epoch to prevent over-fitting [11].

The visualization of the autoencoder training results clearly demonstrates the model's ability to differentiate between normal and abnormal trans- actions. Normal transactions showed minimal re- reconstruction error, while anomalous transactions,

which deviate from learned patterns, exhibited significantly higher errors. Specifically, the average reconstruction error for fraudulent transactions was 0.00183, compared to 0.000069 for normal transactions, highlighting the AE's effectiveness in anomaly separation [12].

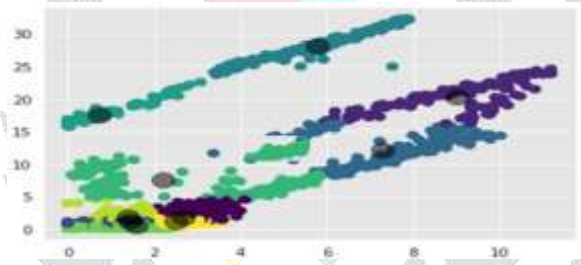

Fig. 3: Visualization of autoencoder training results

The model achieved an AUC-ROC score of 0.836, which indicates a strong overall ability to distinguish between normal and suspicious activities. Furthermore, performance metrics derived from the confusion matrix revealed a recall value of 1.0, ensuring that all true suspicious transactions were identified. Although the precision was lower (0.091) due to some false positives, this trade-off is acceptable in financial systems where it is more critical to catch all potential fraud than to minimize alerts[13]. Overall, the AE-based anomaly detection approach demonstrated robust performance in modeling transaction behavior[14]. The visualization graph supports the conclusion that the model effectively learned the underlying structure of normal transactions and was sensitive to deviations, making it suitable for real-time monitoring and internal control in financial anti-money laundering (AML) systems[15].

V. Conclusion

This study proposed a deep learning-based model using an autoencoder and Risk-Based Approach (RBA) to effectively detect suspicious financial transactions. By leveraging statistical methods, ex- pert input, and internal control indicators, the model demonstrated improved accuracy and adaptability compared to traditional rule-based systems. Despite its success, the model faces limitations, including challenges in optimal model design, data availability, and tuning complexity. Future improvements should focus on incorporating real-world transaction data, enhancing model interpretability, and evaluating performance using metrics beyond accuracy, such as computational efficiency. Additionally, expanding data diversity will be crucial for developing robust AML systems that can adapt to evolving financial crime tactics.

Acknowledgment

References

[1] Tadi, S. R. "Process Mining Driven by Deep Learning for Anomaly Detection in Intelligent Automation Systems." Journal of Scientific and Engineering Research 11.1 (2024): 317-329.
[2] Kaja, Alen. "Self-supervised learning with graphical context to effectively capture complex money laundering activities." (2023).
[3] G. Yang, X. Liu, and B. Li, "Anti-money laundering super- vision by intelligent algorithm," Computers Security, vol. 132, p. 103344, Sep. 2023, doi: 10.1016/j.cose.2023.103344.
[4] E. A. Akartuna et al., "Preventing the money laundering and terrorist financing risks of emerging technologies: An inter- national policy Delphi study," Technological Forecasting and Social Change, 2022, doi: 10.1016/j.techfore.2022.121155.
[5] A. I. Canhoto, "Leveraging machine learning in the global fight against money laundering and terrorism fi- nancing: An affordances perspective," Journal of

Busi- ness Research, vol. 131, pp. 441–452, Jul. 2021, doi: 10.1016/j.jbusres.2020.10.012.
[6] K. Singh and P. Best, "Anti-money laundering: Using data visualization to identify suspicious activity," Int. J. Account- ing Inf. Syst., vol. 34, Sep. 2019, Art. no. 100418.
[7] A. S. M. Irwin, K. R. Choo, and L. Liu, "An analysis of money laundering and terrorism financing typologies," J. Money Laundering Control, vol. 15, no. 1, pp. 85–111, Dec. 2011.
[8] J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, "Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis," J. King Saud Univ.-Comput. Inf. Sci., vol. 32, no. 6, pp. 647–657, Jul. 2020.
[9] C. J. Lee and J. C. Lee, "Experiences and methodology of Korea's anti-money laundering system deployment and development," in Proc. Knowl. Sharing Program, KSP Mod- ularization, 2013, pp. 38–42.
[10] G. Pavlidis, "The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards," J. Econ. Criminol., vol. 2, Dec. 2023, Art. no. 100040.

[11] K. Celik, "Impact of the FATF recommendations and their implementation on financial inclusion: Insights from mutual evaluations and national risk assessments," World Bank Group, USA, 2021.
[12] N. M. Labib, M. A. Rizka, and A. E. M. Shokry, "Survey of machine learning approaches of anti-money laundering techniques to counter terrorism finance," in Proc. Internet Things-Appl. Future (ITAF). Singapore : Springer, 2020, pp. 73–87.
[13] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," J. King Saud Univ.-Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, Jan. 2023.
[14] W. Fang, X. Li, P. Zhou, J. Yan, D. Jiang, and T. Zhou, "Deep learning anti-fraud model for Internet loan: Where we are going," IEEE Access, vol. 9, pp. 9777–9784, 2021.
[15] C. Dhasarathan, M. K. Hasan, S. Islam, S. Abdullah, U. A. Mokhtar, A. R. Javed, and S. Goundar, "COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach," Comput. Commun., vol. 199, pp. 87–97, Feb. 2023.