IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

A RISK-BASED SUSPICIOUS FINANCIAL TRANSACTION DETECTION MODEL USING AUTOENCODERS

[1]*Kuruva Naveen Kumar, MCA Student, Department of MCA*

[2] *H. Ateeq Ahmed, M.Tech, (Ph.D), Assistant Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

For many years, the financial sector has placed a high priority on identifying questionable financial transactions. Financial companies have historically used rule-based systems to spot possibly fraudulent activity. To identify suspicious activity, these systems use preset criteria and patterns, including big transactions or frequent deposits. Traditional techniques are somewhat successful, but they have several drawbacks. They often produce a high percentage of false positives, necessitating human evaluation of transactions that have been identified. Furthermore, these systems have trouble keeping up with changing fraud trends, which reduces their ability to identify complex financial crimes. Advanced detection systems are now more important than ever due to the increasing number and complexity of financial transactions in the digital age. The dynamic nature of financial fraud is not addressed by traditional solutions, which results in ineffective loss prevention. This makes the need for a more flexible, precise, and scalable method of identifying questionable transactions urgent. Traditional approaches' lack of flexibility and the serious financial and reputational consequences associated with undiscovered fraud highlight the need for a more reliable detection system. Enhancing the capacity to identify unusual patterns in financial data with a low number of false positives while preserving scalability and efficiency is the aim. The suggested system offers a novel approach that makes use of a risk-based evaluation method in conjunction with an autoencoder-based model. By identifying minute deviations from typical patterns in transaction data, this method seeks to identify questionable activity. By including a risk-based framework, the model is guaranteed to take contextual elements into account, minimising false alarms and giving high-risk transactions priority for further examination. By addressing the shortcomings of conventional techniques, this system offers a smart, flexible, and trustworthy instrument for preventing financial fraud.

I. INTRODUCTION

1.1 Introduction

In the financial sector, identifying suspicious financial transactions is crucial, especially when it comes to fighting fraud and money laundering. The earliest fraud detection systems, which relied on human inspections and simple software tools, were introduced in the 20th century, giving rise to the idea. The Reserve Bank of India (RBI) and financial institutions in India have been making a concerted effort to enhance fraud detection methods. The Financial Intelligence Unit of India (FIU-IND) indicates that the number of suspicious transaction notifications has significantly increased in recent years. More than 3.5 million complaints of questionable transactions were submitted in 2020 alone, demonstrating the nation's growing financial fraud problem. The intricacy of financial crimes, such as money laundering, phishing, and cyber fraud, was too great for traditional systems to handle. India has responded by using a number of technical innovations, including as machine learning techniques, to enhance detection. Digital banking, e-commerce, and the rise in financial transactions have increased the need for a more automated, precise, and scalable solution. The financial industry must adjust to these developments by putting in place

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

more advanced detection methods as the economy becomes more digitalised.

Problem Definition

Financial institutions mostly depended on rule-based systems to identify suspicious transactions prior to the incorporation of machine learning. Simple thresholds and patterns, such odd transaction amounts or certain transaction rates, served as the foundation for these systems. These methods did, however, have serious shortcomings. They often produced a high volume of false positives, which resulted in an inefficient use of resources for transaction reviews by hand. Furthermore, these systems were unable to adapt to changing fraud strategies, which resulted in the failure to identify sophisticated and novel fraud patterns. Instead of being proactive, fraud detection was reactive, concentrating on finding irregularities after they had already happened. Transactions with normal but unusual behaviour were highlighted needlessly due to the lack of contextual analysis. These restrictions raised the possibility of financial loss and caused delays in the detection of fraudulent activity. Consequently, it became clear that more sophisticated systems that could learn from data and adjust to emerging dangers were required. These persistent issues were addressed by machine learning, which has the capacity to identify patterns and identify abnormalities instantly.

Research Motivation

The limits of conventional fraud detection systems, which find it difficult to detect more complex fraudulent activity, are the driving force behind this study. The necessity for a more reliable and scalable detection method has been brought to light in India by the sharp increase in financial crimes and the quick expansion of digital transactions. Traditional approaches are no longer enough to handle the complexity of fraudulent operations including phishing, identity theft, and money laundering. By developing models that can identify minute, hidden patterns in transaction data, machine learning holds promise for increasing accuracy and lowering false positives. The goal of this project is to create a more efficient model that can learn from transaction data and adapt to new forms of fraud by using autoencoders and a risk-based approach. The potential of these cutting-edge methods to improve the effectiveness and security of financial systems, shielding institutions and customers from the growing risk of financial crime, serves as the driving force. Additionally, organisations can handle the growing amount of transactions while maintaining high detection accuracy thanks to the scalability of machine learning models.

II. LITERATURE SURVEY

Singh & Best [1] suggested a technique for identifying suspicious activity for anti-money laundering (AML) that makes use of data visualisation. They showed how data visualisation methods may be used to detect odd transaction patterns that could be signs of money laundering, providing a strong instrument for keeping an eye on financial systems and enhancing banking industry compliance protocols. The dangers of mobile money were investigated by Whisker & Lokanan [2] in relation to counterterrorism funding and anti-money laundering. They spoke about the difficulties that mobile money poses, such as its anonymity and the ease with which it might be used for illegal financial purposes, and they suggested ways to lessen these dangers. A sustainable paradigm for putting anti-money laundering policies in line with UN development objectives was provided by Dobrowolski & Sułkowski [3]. They put out an integrated strategy that tackles the difficulties of compliance in various regulatory contexts while highlighting sustainable financial systems and the contribution of AML to global economic stability and progress. In their analysis of money laundering and terrorist funding typologies, Irwin et al. [4] focused on the strategies and tactics employed to hide illegal financial activity. They looked at the

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

trends and traits of these illegal operations, giving a thorough rundown of how successful AML regulations can identify and stop them.

A swarm intelligence-based framework for inducing categorisation rules was presented by Uthayakumar et al. [5] and used in credit risk analysis and bankruptcy prediction. They demonstrated how machine learning methods, such as swarm intelligence, may be used to increase prediction accuracy in the banking industry, especially when it comes to identifying money laundering threats. The risk-based approach (RBA) criteria for counter-terrorism financing (CFT) and anti-money laundering (AML) in financial investment enterprises were introduced by KOFIU [6]. In order to maximise the utilisation of resources in the fight against financial crimes, this study demonstrated how financial institutions might utilise RBA to detect high-risk operations and adjust their compliance efforts appropriately. The techniques and experiences of Lee & Lee [7] in implementing and improving South Korea's anti-money laundering (AML) system were revealed. They spoke about how different regulatory frameworks may be integrated and the difficulties in developing a complete system that successfully stops money laundering while maintaining the stability of the financial system. The unforeseen implications of putting anti-money laundering standards—more especially, those established by the Financial Action Task Force (FATF)—into practice were discussed by Pavlidis [8]. The study looked at the potential drawbacks of the FATF's stringent compliance standards, including a rise in financial exclusion, and offered solutions. Using information from national risk assessments and mutual evaluations, Celik [9] investigated how the FATF's guidelines affected financial inclusion. The report highlighted the need to strike a balance between maintaining access to financial services and executing AML/CFT laws, especially for marginalised people.

According to the 2013 FATF methodology, Jayasekara [10] spoke about the difficulties in putting into practice an efficient risk-based supervisory strategy for AML and combating the funding of terrorism. The study offered suggestions to improve supervisory efficiency while concentrating on the challenges financial institutions have when implementing these complex systems. With an emphasis on adherence to the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws, Raghavan [11] investigated the incorporation of anti-money laundering procedures into corporate governance and finance activities. The research demonstrated how corporate governance is changing as a result of AML regulations, highlighting the need of more stringent internal controls to stop financial crimes. Raghavan [12] looked at how AML rules are affecting banking firms' corporate governance and finance departments. He spoke on how AML procedures may be incorporated into organisational structures and emphasised how compliance standards are always changing, especially in light of new financial crimes. Machine learning methods for counterterrorism finance and anti-money laundering (AML) strategies were reviewed by Labib et al. [13]. They went over a number of machine learning approaches and spoke about how they may be used to find possible money laundering operations, detect suspicious transactions, and increase the efficacy of AML in general.

A comprehensive study of disruptive technology-based credit card fraud detection techniques was carried out by Cherif et al. [14]. They focused on how developments in artificial intelligence (AI) and machine learning have greatly improved the precision of fraud detection systems, particularly when it comes to financial transactions, which are often the focus of money laundering operations. An AI-based method was presented by Senator et al. [15] to detect possible money laundering activities from reports of significant cash transactions. Their study highlighted the usefulness of AI in

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

automating the detection of financial crimes by introducing the Financial Crimes Enforcement Network's (FinCEN) AI system for identifying suspicious trends. A decision tree-based approach to assessing money laundering risks was presented by Wang & Yang [16]. By classifying transactions according to their risk levels using previous transaction data, their methodology made it possible to identify and stop money laundering operations more successfully. The use of data mining techniques in financial applications was examined by Zhang & Zhou [17], who concentrated on how these approaches might reveal hidden patterns in transaction data that can point to illegal activity like money laundering. They spoke about how data mining may improve financial monitoring systems and make it easier to spot financial crimes.

III. EXISTING SYSTEM

The existing system for anti-money laundering (AML) and counter-terrorism financing (CFT) heavily relies on traditional approaches such as rule-based algorithms, transaction monitoring systems, and manual auditing. These systems identify unusual patterns by matching transaction data against predefined rules or thresholds. Organizations often employ data visualization techniques, risk-based assessments, and typologies to detect money laundering activities. Financial institutions also implement compliance measures guided by international standards such as the FATF recommendations. Additionally, machine learning (ML) and artificial intelligence (AI) methods have been integrated into some systems to automate the detection of suspicious activities. However, despite these dvancements, the systems face several challenges, especially in handling evolving money laundering techniques and balancing regulatory compliance with financial inclusion.

DISADVANGES

High False Positives: Rule-based systems often generate a high number of false positives, which lead to inefficiencies and wasted resources during investigations.

Adaptability to Evolving Techniques: Traditional systems struggle to adapt to new and sophisticated money laundering schemes, which involve complex patterns and multi-layered transactions.

Lack of Scalability: Existing systems may fail to handle large-scale transaction data efficiently, especially in the era of digital and mobile banking.

Financial Exclusion: Strict compliance with FATF standards can inadvertently lead to financial exclusion, particularly for underserved communities.

Limited Integration of AI/ML: While some systems use AI/ML, their integration remains limited, resulting in suboptimal performance for predictive modeling and anomaly detection.

Data Privacy Concerns: AML systems often face challenges related to data sharing and privacy compliance, especially across international borders.

Resource-Intensive Supervision: Risk-based supervision approaches demand significant resources for proper implementation, making it difficult for smaller institutions to comply.

Unintended Consequences: Over-regulation can deter financial inclusion and innovation, and misaligned priorities may lead to ineffective implementation of AML measures.

IV. PROPOSED SYSTEM

In order to discover irregularities and stop financial losses, fraud detection in financial transactions is a crucial job that calls for a strong and methodical approach. This study describes a methodical approach to creating and comparing two machine learning models: a suggested Autoencoder-Random Forest (AERF) model and an existing Deep Neural Network (DNN) model. Preprocessing, model training, performance assessment, and dataset preparation are all steps in the process. The specific stages of this study are listed below.

First Step: Upload the dataset

Uploading the dataset is the initial step. Financial transaction data, including transaction type, amount, origin and destination

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

balances, and a target column indicating if the transaction is fraudulent (isFraud), is presumed to be included in the dataset utilised in this study.

A web-based interface created using Django is used to upload the dataset. Users may choose and upload a CSV file using this interface. After uploading, the dataset is analysed and momentarily saved for further examination. For the next stages to be successful, the dataset must be clean, organised, and formatted correctly. To avoid processing mistakes, a strong upload system verifies the file type and fundamental data integrity.

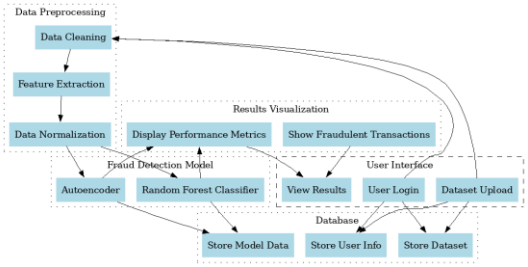

Fig.1: Architectural Block Diagram of The Proposed System.

V. SCREEN SHOTS

Results Description

The homepage is the first interface that administrators and users see. It offers navigation choices for a number of features, including dataset upload, login, and registration. An intuitive and user-friendly experience is guaranteed by the design. The registration page, which is a common form for administrators and users, is seen in figure 2. To establish a new account in the system, the page requests basic information such a username, password, and other identifying characteristics.

Fig 1: Home Page of the Financial Transaction Detection.

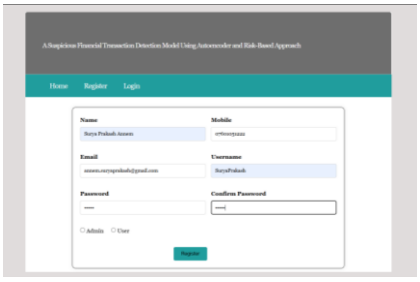

Fig 2: Common Registration for user and admin.

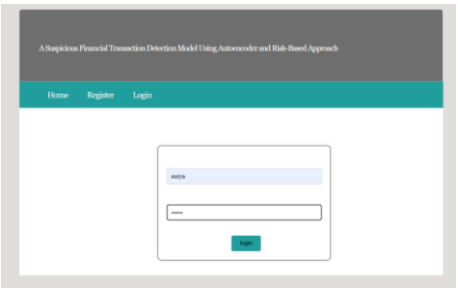

Fig 3: User login for using Transaction detection.

The fraud detection system is accessible to registered users via the user login page. It has spaces for inputting login information, such as a password and username. Users may use the system's functions, such uploading datasets for fraud detection, after successfully logging in.

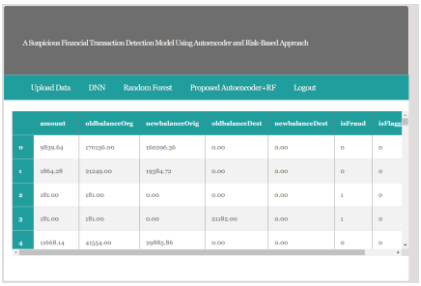

Fig 4: Sample Fraud Transaction Uploaded Dataset.

A sample of the dataset that users or administrators have uploaded is shown in this image. In order to analyse and identify fraudulent activity, it includes financial transaction information, including features like transaction step, type, source and destination balances, fraud indications, etc.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

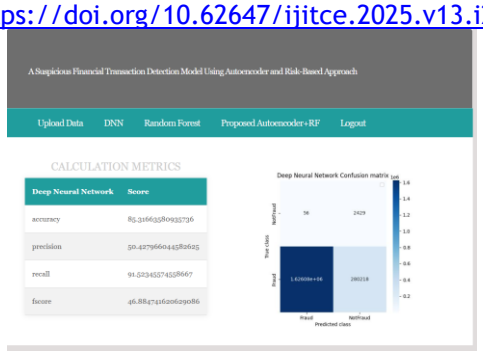

Fig 5: Performance metrics of the Existing DNN model.

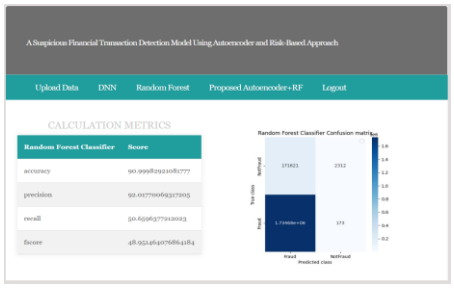

Fig 6: Performance metrics of the Existing RFC model.

The RFC model is more accurate and precise than DNN, which makes it more dependable for accurately detecting fraudulent transactions.

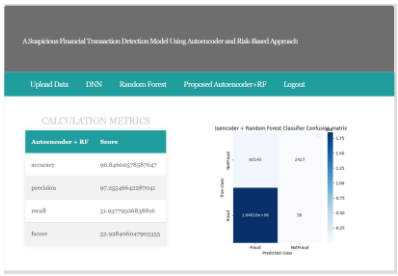

Fig 7: Performance metrics of the Proposed Auto Encoder + RFC model.

The suggested model exhibits significant gains in identifying fraudulent transactions while preserving a balanced F1-score, achieving the best accuracy and precision.

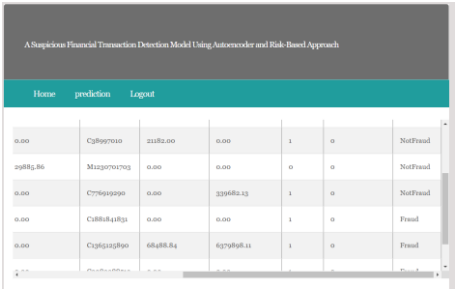

Fig 8: Proposed model prediction on user uploaded test data.

The predictions made by the suggested model on a test dataset that was provided by a user are shown in this image. The Autoencoder + RFC model demonstrates its relevance to real-world datasets by successfully identifying fraudulent transactions.

VI. CONCLUSION AND FUTURE SCOPE

Conclusion:

To identify fraudulent transactions in financial datasets, the research combines the strong classification capabilities of the Random Forest Classifier (RFC) with the feature extraction and dimensionality reduction capabilities of autoencoders. This hybrid method makes use of RFC's excellent accuracy and interpretability for classification tasks while using Autoencoders' unsupervised learning capabilities to uncover hidden patterns and abnormalities in transaction data. The design of the system addresses the difficulties brought on by unbalanced datasets and intricate transactional behaviours, guaranteeing scalability, efficiency, and accuracy in fraud detection. The initiative makes a substantial contribution to lowering financial losses and boosting confidence in financial institutions.

Future Scope:

1. Integration with Real-Time Systems: To identify fraud in real time and enable prompt reactions to questionable activity, the model may be included into live transaction monitoring systems.
2. Improving Model Performance: To further increase prediction accuracy and computing efficiency, sophisticated methods such as ensemble learning using gradient-boosted models or transformers might be investigated.
3. Explainability and Interpretability: By using explainable AI (XAI) methodologies, stakeholders may better understand and trust the system

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025
https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

by seeing how transparent the fraud detection judgements are.

4. Application to Multimodal Data: The model's capacity to detect fraudulent transactions may be improved by using data from other sources, such as device information, geolocation, and user behavioural patterns.
5. Domain Adaptation: Using the system to identify fraud in billing and claims data in other sectors, like insurance or healthcare.
6. Adaptation to Emerging Threats: As fraud strategies and patterns change, the system is updated often utilising continuous learning approaches.

REFERENCES

[1] Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. International Journal of Accounting Information Systems, 34, 100418.

[2] Whisker, J., & Lokanan, M. E. (2019). Anti-money laundering and counter-terrorist financing threats posed by mobile money. Journal of Money Laundering Control, 22(1), 158-172.

[3] Dobrowolski, Z., & Sułkowski, Ł. (2019). Implementing a sustainable model for anti-money laundering in the United Nations development goals. Sustainability, 12(1), 244.

[4] Samantha Maitland Irwin, A., Raymond Choo, K. K., & Liu, L. (2011). An analysis of money laundering and terrorism financing typologies. Journal of Money Laundering Control, 15(1), 85-111.

[5] Uthayakumar, J., Vengattaraman, & Dhavachelvan, T. P. (2022). Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis. Journal of King Saud University - Computer and Information Sciences, 32(6), 647-657.

[6] KOFIU. (2017). Risk-Based Approach (RBA) Processing Standards for AML/CFT in Financial Investment Businesses. Institutional Operations Division, Financial Intelligence Unit.

[7] Lee, C.-J., & Lee, J.-C. (2013). Experiences and methodology of Korea's anti-money laundering system deployment and development. Knowledge Sharing Program: KSP Modularization.

[8] Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards. Journal of Economic Criminology, 100040.

[9] Celik, K. (2021). Impact of the FATF Recommendations and their Implementation on Financial Inclusion: Insights from Mutual Evaluations and National Risk Assessments.

[10] Jayasekara, S. D. (2018). Challenges of implementing an effective risk-based supervision on anti-money laundering and countering the financing of terrorism under the 2013 FATF methodology. Journal of Money Laundering Control, 21(4), 601-615.

[11] Raghavan, K. R. (2006). Integrating anti-money laundering into the compliance structure: How the requirements for compliance with BSA/AML are changing the emphasis of corporate governance and finance functions. Bank Accounting & Finance, 19(6), 29-37.

[12] Raghavan, K. R. (2006). Integrating anti-money laundering into the compliance structure: How the requirements for compliance with BSA/AML are changing the emphasis of corporate governance and finance functions. Bank Accounting & Finance, 19(6), 29-37.

[13] Labib, N. M., Rizka, M. A., & Shokry, A. E. M. (2020). Survey of machine learning approaches of anti-money

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

https://doi.org/10.62647/ijitce.2025.v13.i2.pp872-879

laundering techniques to counter terrorism finance. In Internet of Things—Applications and Future: Proceedings of ITAF 2019 (pp. 73-87). Springer.

[14] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review, Journal of King Saud University - Computer and Information Sciences, 35(1), 145-174.