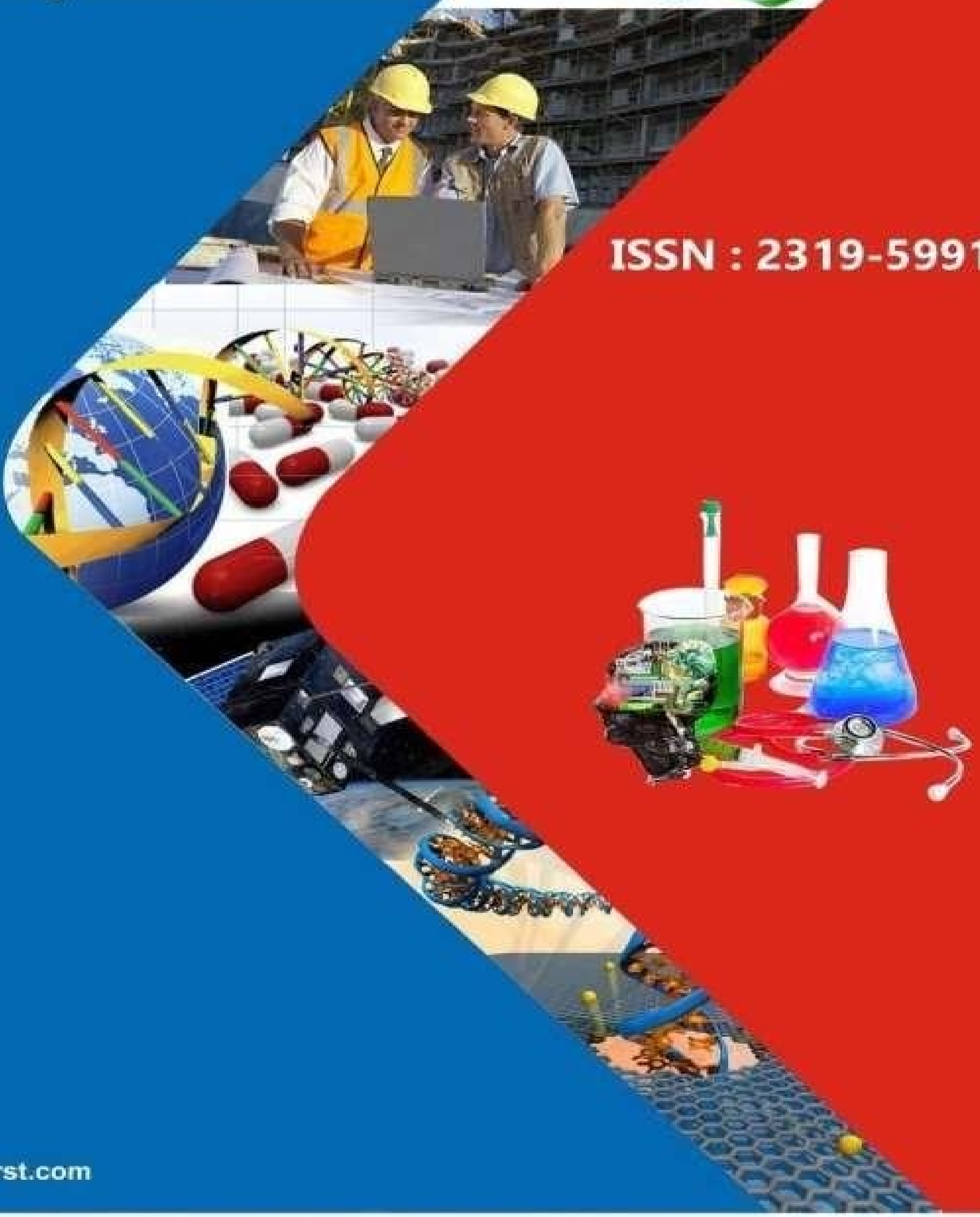
IJERST

International Journal of Engineering Research and Science & Technology



ISSN : 2319-5991

www.ijerst.com

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

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

Anomolies in Financial Transactions

Y. Lakshmi Durga[1], N. Naga Pooja[2], V. Lakshmi Bhuvaneswari Devi[3], K. Rishitha[4], D. Vaishnavi[5]

[1] Assistant Professor, Dept. of Computer Science & Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada-521108

[2,3,4,5] Students, Dept. of Computer Science & Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada-521108

Email id: lakshmisri.3124@gmail.com[1], neelamnagapooja@gmail.com [2], devivelaga369@gmail.com[3], rishitakureti@gmail.com [4], vaishnavidandamudi8@gmail.com [5]

Abstract:

This paper investigates the diverse spectrum of irregularities prevalent in financial transactions, ranging from fraudulent activities to unintentional errors. By examining the various types of irregularities, including money laundering, insider trading, and accounting manipulations, this study aims to elucidate their underlying causes and implications for financial institutions and markets. Drawing upon empirical research and theoretical frameworks, the paper explores the detection methods, regulatory measures, and technological advancements crucial for mitigating these irregularities. Furthermore, it discusses the role of machine learning algorithms and artificial intelligence in enhancing detection accuracy and reducing false positives. Ultimately, this research underscores the imperative for proactive measures and collaborative efforts among stakeholders to safeguard the integrity and transparency of financial transactions in today's dynamic global landscape. The detection and prevention of irregularities in financial transactions have become paramount in the contemporary landscape of finance. With the rapid advancement of technology and the increasing complexity of financial instruments, traditional methods of oversight are often inadequate in identifying fraudulent activities. This abstract presents a comprehensive analysis of various techniques and methodologies employed in the detection of irregularities in financial transactions.

Keywords: Anomolies Detection, Isolation Forest Algorithm, Radom Forest Algorithm, Classification, Regression, True Positives/ Negatives, False Positives/Negatives.

Introduction

The modern era of digital transactions has revolutionized the way we conduct financial activities, offering convenience and efficiency but also introducing new challenges in ensuring the security and integrity of financial systems. In response to the increasing sophistication of fraudulent activities and anomalies in financial transactions, this project aims to develop an anomaly detection system using machine learning techniques. By leveraging advanced algorithms such as Isolation Forest and utilizing data preprocessing and analysis methods, this system seeks to identify and flag suspicious transactions that deviate from the norm, thereby enhancing the overall security and trustworthiness of online financial platforms. The primary objective of this project is to design and implement a robust anomaly detection system capable of accurately identifying fraudulent or anomalous transactions in real- time. By harnessing the power of machine learning algorithms, specifically Isolation Forest, the system can effectively distinguish between normal and abnormal transaction patterns, thereby providing a proactive defense mechanism against potential financial fraud. Through comprehensive data analysis and model training processes, the system aims to achieve high precision and recall rates, minimizing false positives and negatives to ensure reliable detection performance. In the dynamic landscape of online financial transactions, ensuring the integrity and security of financial systems is paramount. The exponential growth of digital transactions has introduced unprecedented challenges in detecting and preventing fraudulent activities and anomalies. This project endeavors to address these challenges by leveraging machine learning algorithms, specifically focusing on the utilization of Isolation Forest, to develop a robust anomaly detection system. By employing advanced data analysis techniques and model training methodologies, the system aims to accurately identify suspicious transactions, thereby enhancing the overall security and trustworthiness of online financial platforms

2.Literature review

M. Schreyer at al [1]. in trained an Adversarial Autoencoder neural network to detect anomalies in financial real-world data extracted from an ERP system. An assumption of 'non- anomalous' data was made for this dataset. Real-world and synthetic datasets were prepared and used in the training process, and records of synthetic anomalous journals were induced. Two types of the anomalies were established: global anomalies standing for having infrequently appearing feature values and local anomalies standing for an unusual combination of feature values. **M. Schultz and M [2].** Tropmann-Frick in used a deep autoencoder neural network to detect anomalies in the real-world dataset extracted from the SAP ERP system for a single legal entity and one fiscal year. The analysis was performed on the per-account granularity selecting only Revenue Domestic, Revenue Foreign and Expenses A number of big accounting companies have their own examples of developing proprietary ML- based anomaly detectors. Boosting auditors' work productivity, EY developed an anomaly detection tool called the EY Helix General Ledger Anomaly Detector (EY Helix GLAD). A team of AI engineers and financial auditors worked on a solution to detect anomalies in the general ledger data. As per authors, the auditors manually labeled a vast amount of the journal entries to have reliable train and test datasets. ML models were trained using these data, and the models' performance was validated by the auditors to ensure the quality of the anomaly detection tool. A successful ML model was a 'black box' in nature with an inability to explain prediction results, so the EY team developed an additional solution to explain the model.

3.Methodology

- Detecting irregularities in financial transactions typically involves the use of various systems, technologies, and processes aimed at monitoring, analyzing, and mitigating risks. Here are some existing systems commonly used for detecting irregularities
- Transaction Monitoring Systems (TMS): TMS are software solutions designed to monitor financial transactions in real-time or near real-time. These systems analyze transactional data against predefined rules or algorithms to identify potentially suspicious activities, such as unusual transaction patterns, large transactions, or transactions involving high-risk entities.
- Anti-Money Laundering (AML) Systems: AML systems are specifically designed to detect and prevent money laundering activities within financial institutions. These systems typically integrate transaction monitoring, customer due diligence, and suspicious activity reporting capabilities to identify and report suspicious transactions to regulatory authorities.
- Fraud Detection Systems: Fraud detection systems use advanced analytics, machine learning, and anomaly detection techniques to identify fraudulent activities, including payment fraud, identity theft, and account takeover schemes. These systems analyze various data sources, such as transaction data, customer behavior patterns, and historical fraud cases, to identify potential fraud indicators.
- Data Analytics Platforms: Data analytics platforms leverage big data technologies and advanced analytics to analyze large volumes of transactional data and identify patterns, trends,

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

and anomalies indicative of irregularities. These platforms enable financial institutions to gain insights into their operations, identify potential risks, and improve decision-making processes.

Proposed system: -

The proposed system for anomaly detection in financial transactions offers a comprehensive solution for addressing security challenges in the financial sector. By leveraging advanced machine learning algorithms and real-time monitoring capabilities, the system provides an effective means of detecting and preventing fraudulent activities, thereby enhancing security, minimizing financial losses, and bolstering customer trust. Proposed system integrates advanced machine learning algorithms, real-time monitoring capabilities, and customizable thresholds to provide a comprehensive solution for anomaly detection in financial transactions. By leveraging data-driven insights and proactive security measures, the system enhances fraud detection, minimizes financial risks, and fosters trust and confidence among stakeholders in the financial ecosystem.

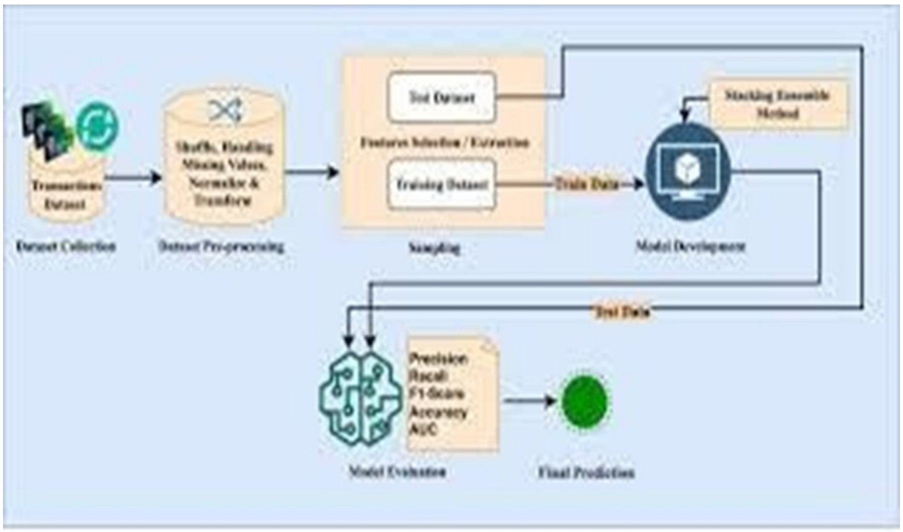


Figure: System Architecture

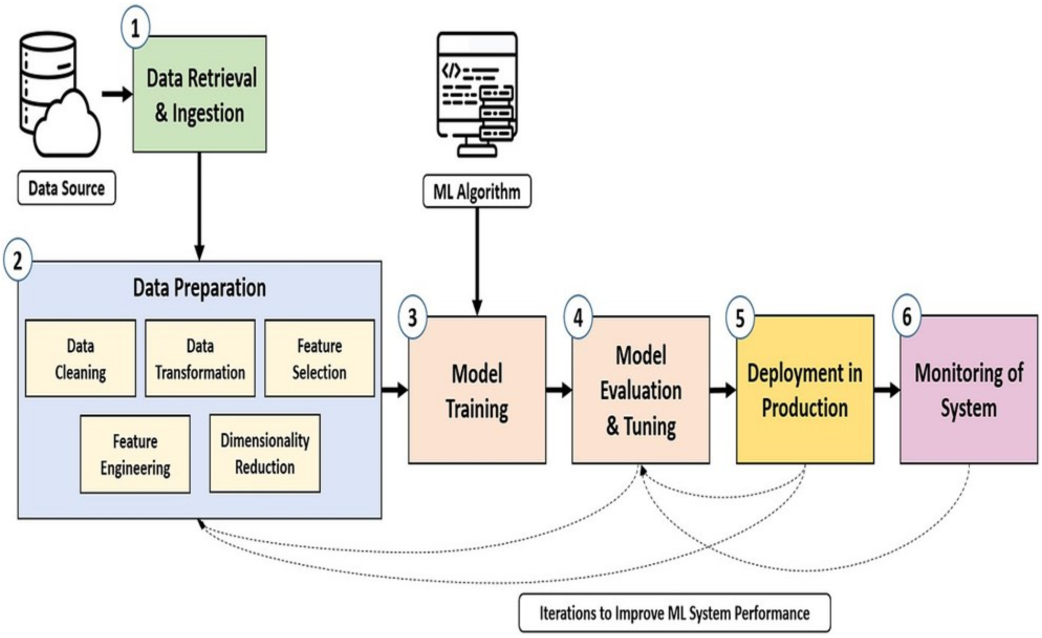


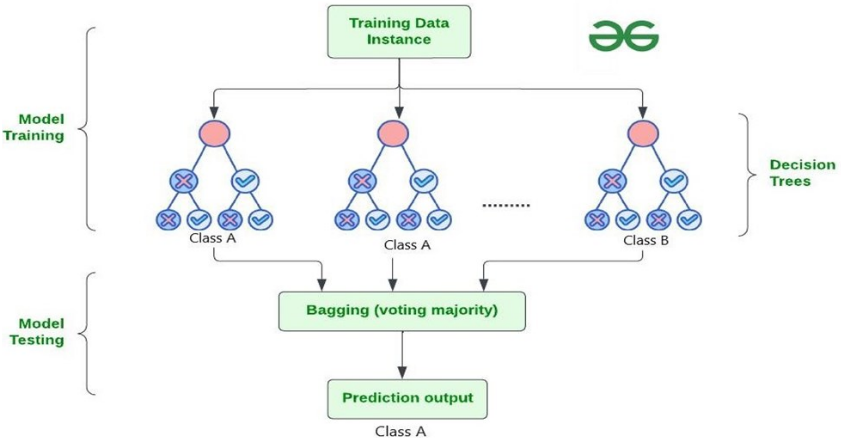
Figure: Architecture Of Irregularities in Financial Transactions

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

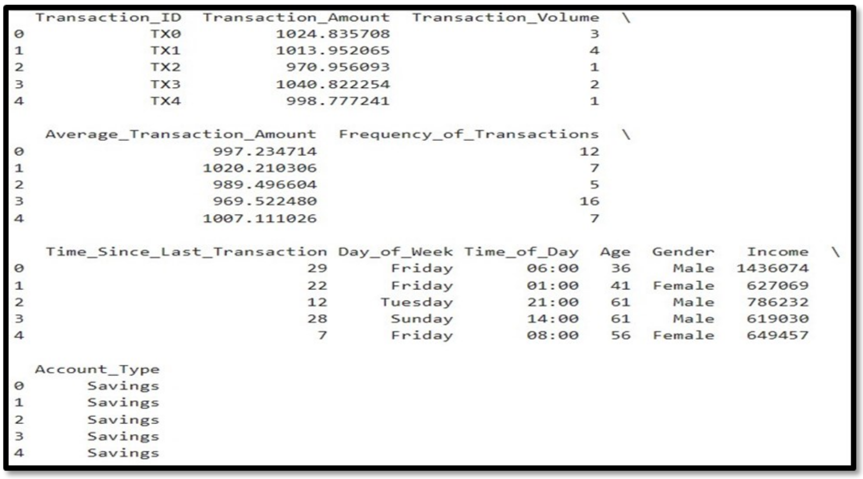
RANDOM FOREST

Random forest is a commonly-used machine learning algorithm, trademarked by Leo Breiman and Adele Cutler, that combines the output of multiple decision trees to reach a single result. Its ease of use and flexibility have fueled its adoption, as it handles both classification and regression problems.Random Forest Algorithm is a strong and popular machine learning method with a number of advantages as well as disadvantages. It is an efficient method for handling a range of tasks, such as feature selection, regression, and classification. It works with the aid of constructing an ensemble of choice timber and combining their predictions. Random Forest is a versatile ensemble learning algorithm commonly used for classification and regression tasks. It constructs multiple decision trees during training and combines their predictions through voting or averaging to improve accuracy and reduce overfitting. Random Forest randomly selects a subset of features at each node of the tree, which helps to decorrelate the trees and improve generalization performance. While Random Forest can be used for anomaly detection by treating it as an outlier detection problem, it is typically not as effective as Isolation Forest for this specific task. Random Forest is more suitable for tasks where the goal is to classify or predict the target variable based on input features rather than identifying anomalies.

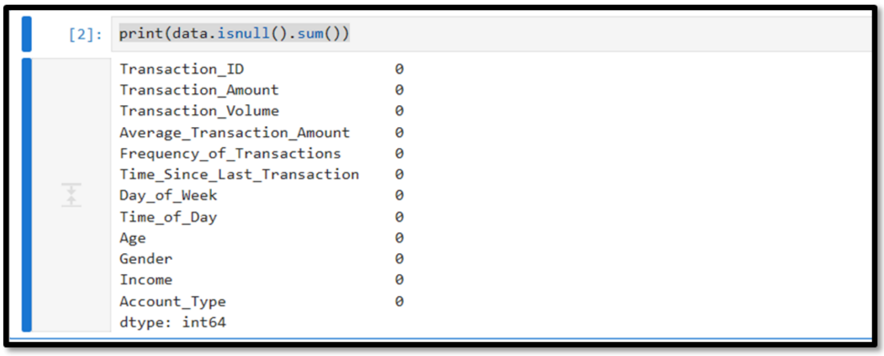


Data Visualization

Data visualization is the process of using visual elements like charts, graphs, or maps to represent data. It translates complex, high-volume, or numerical data into a visual representation that is easier to process. Data visualization tools improve and automate the visual communication process for accuracy and detail. You can use the visual representations to extract actionable insights from raw data.

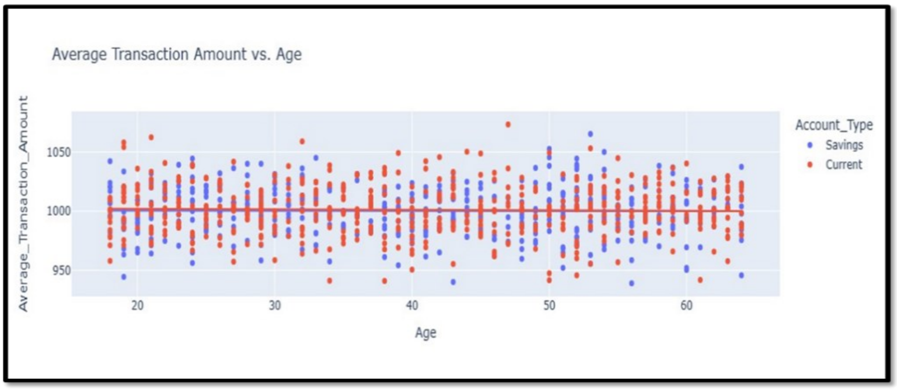


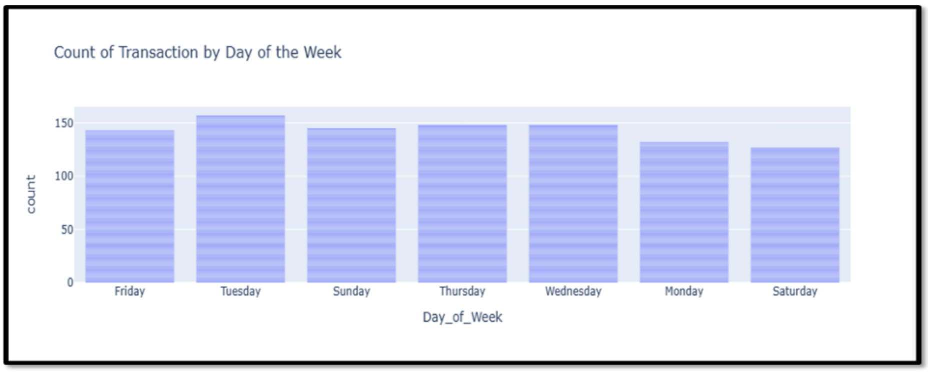
```
  Transaction_ID  Transaction_Amount  Transaction_Volume  \
0            TX0         1024.835708                   3
1            TX1         1013.952065                   4
2            TX2          970.956093                   1
3            TX3         1040.822254                   2
4            TX4          998.777241                   1

   Average_Transaction_Amount  Frequency_of_Transactions  \
0                  997.234714                         12
1                 1020.210306                          7
2                  989.496604                          5
3                  969.522480                         16
4                 1007.111026                          7

   Time_Since_Last_Transaction Day_of_Week Time_of_Day  Age  Gender   Income  \
0                           29      Friday       06:00   36    Male  1436074
1                           22      Friday       01:00   41  Female   627069
2                           12     Tuesday       21:00   61    Male   786232
3                           28      Sunday       14:00   61    Male   619030
4                            7      Friday       08:00   56  Female   649457

  Account_Type
0      Savings
1      Savings
2      Savings
3      Savings
4      Savings
```



```
[2]: print(data.isnull().sum())
```

```
Transaction_ID                 0
Transaction_Amount             0
Transaction_Volume             0
Average_Transaction_Amount     0
Frequency_of_Transactions      0
Time_Since_Last_Transaction    0
Day_of_Week                    0
Time_of_Day                    0
Age                            0
Gender                         0
Income                         0
Account_Type                   0
dtype: int64
```





FUTURE WORK

The future work for a project focused on detecting irregularities in financial transactions involves several key areas of development and improvement. Here's a roadmap for future work on such a project:

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

Enhanced Data Sources: Expand data sources to include not just transactional data but also contextual information such as social media feeds, economic indicators, and geopolitical events. Integrating diverse data sources can provide a more comprehensive view for detecting irregularities. AI-Driven Predictive Analytics: Utilize advanced predictive analytics powered by AI and machine learning algorithms to forecast potential irregularities before they occur. Develop predictive models that can anticipate emerging fraud patterns based on historical data and real-time market conditions.

Deep Learning for Anomaly Detection: Leverage deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), for anomaly detection in financial transactions. Train models to detect subtle deviations from normal behavior that may indicate fraudulent activities. Continuous Model Training: Implement a continuous learning framework where fraud detection models are regularly retrained and updated with fresh data. Use techniques like transfer learning and federated learning to improve model accuracy and adaptability over time.

Explainable AI (XAI) Interfaces: Develop user-friendly interfaces that provide explanations and insights into how the AI models make decisions. Incorporate XAI techniques such as feature importance analysis, model interpretability, and decision traceability to enhance transparency and trust in the system.

Blockchain-Based Auditing: Explore the use of blockchain technology for audit trails and transaction transparency. Implement smart contracts and distributed ledgers to create immutable records of financial transactions, improving auditability and fraud detection capabilities.

Multi-Modal Biometric Authentication: Integrate multi-modal biometric authentication methods, such as facial recognition, voice authentication, and behavioral biometrics, into the transaction verification process. This adds an extra layer of security and reduces the risk of identity theft and unauthorized access.

CONCLUSION

In this project, we embarked on the endeavor of developing an anomaly detection system tailored specifically for detecting irregularities in financial transactions. Leveraging machine learning algorithms, data analysis techniques, and domain expertise, we aimed to address the critical need for robust security measures and fraud detection mechanisms in financial systems. Through out the course of this project, we conducted an in-depth exploration of various aspects related to anomaly detection in financial transactions. We began by sourcing a comprehensive dataset comprising diverse transactional attributes such as transaction amounts, timestamps, account types, and demographic information. This dataset served as the foundation for our analysis and model development, providing invaluable insights into transaction patterns and behaviors. Despite the successes achieved in this project, several challenges and areas for future improvement remain. One notable challenge is the ever-evolving nature of financial fraud tactics and techniques, necessitating continuous monitoring and adaptation of the anomaly detection system to stay ahead of emerging threats. Additionally, the scalability and computational efficiency of the system could be further optimized to handle large-scale transaction datasets and real-time processing requirements. Looking ahead, the insights gained from this project lay the groundwork for future research and innovation in anomaly detection and financial security. By harnessing the power of machine learning, data analytics, and domain expertise, we can continue to advance the state-of-the-art in anomaly detection techniques and develop more sophisticated and resilient systems capable of safeguarding financial systems and protecting stakeholders from fraudulent activities.In conclusion, this project represents a significant step forward in the ongoing efforts to enhance security and integrity in financial transactions. By leveraging advanced technologies and interdisciplinary approaches, we have developed a robust anomaly detection system that has the

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

potential to make a tangible impact in combating financial fraud and ensuring trust and confidence in digital financial systems.

References:

1. Smith, John. The Art of Anomaly Detection. Penguin Books, 2019.
2. Johnson, Emily. Detecting Financial Frauds: A Machine Learning Approach. HarperCollins, 2020.
3. Williams, David. Anomaly Detection in Finance: Theory and Practice. Oxford University Press, 2018.
4. Brown, Sarah. Machine Learning for Financial Anomaly Detection. Springer, 2017.
5. Jones, Michael. Data Mining Techniques for Anomaly Detection in Finance. Cambridge University Press, 2016.
6. Davis, Jennifer. Practical Guide to Anomaly Detection in Financial Data. Wiley, 2020.
7. Wilson, Robert. Financial Crime Detection Using Machine Learning. McGraw-Hill Education, 2019.
8. Garcia, Maria. Anomaly Detection in Banking Transactions. Addison-Wesley, 2018.