ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

AI POWERED PUBLIC WELFARE DISTRIBUTION FRAUD DETECTION SYSTEM

[1]Dr. D. Nagesh Babu,[2]V. Siva Mani Durga,[3]R. Yeswanth Kumar Reddy,[4]U. Sri Harshitha

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]U. G Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT- ***This project presents an AI-driven public welfare fraud detection system integrated with machine learning technology. The system enhances welfare transparency and accountability by identifying fraudulent transactions. It ensures efficiency, reliability, and intelligent decision-making through artificial intelligence. The system uses financial transaction data and machine learning techniques to identify fraudulent patterns and classify transactions accordingly. Suspicious transactions are detected, improving overall welfare distribution integrity. Traditional welfare monitoring systems rely on manual verification, periodic audits, which can be time-consuming, inconsistent, inaccurate, or inefficient, leading to financial irregularities. These systems also lack intelligent fraud detection and accurate analysis of suspicious transaction patterns. There is a need for an automated, reliable, and cost-effective public welfare fraud detection system that can accurately identify fraudulent transactions and support transparent distribution of welfare benefits using artificial intelligence.***

KEYWORDS: ***Artificial Intelligence (AI), Machine Learning (ML), Fraud Detection, Public Welfare Distribution, Financial Transaction Analysis, Classification, Predictive Analytics, Data Mining.***

INTRODUCTION

Public welfare distribution systems are designed to ensure that financial assistance reaches eligible beneficiaries efficiently and transparently. With advancements in Artificial Intelligence and Machine Learning, fraud detection has become an effective approach for identifying suspicious financial transactions. This project combines public welfare transaction analysis with AI-based machine learning to improve fraud detection

and distribution transparency. The proposed system not only improves the identification of fraudulent transactions but also adds an additional layer of intelligence by supporting accurate classification and better decision-making during welfare distribution.

LITERATURE SURVEY

Public welfare distribution systems have gained significant attention in recent years due to the increasing adoption of Artificial Intelligence and Machine Learning technologies. A public welfare fraud detection system is generally designed to analyze financial transaction data and identify suspicious activities that may affect the fair distribution of welfare benefits. The core concept of the proposed system revolves around intelligent transaction analysis and machine learning-based classification using historical financial transaction data to support accurate fraud detection and transparent welfare distribution.

RELATED WORK

Several researchers have contributed to the development of fraud detection systems with the aim of improving transparency, accountability, accuracy, and efficiency in public welfare distribution. Initial research in this domain focused on traditional fraud detection methods where suspicious transactions were identified through manual verification or conventional statistical techniques. These approaches relied on predefined conditions and historical analysis, offering limited adaptability and reduced effectiveness in identifying complex fraudulent transaction patterns.

EXISTING SYSTEM

The existing public welfare monitoring systems mostly depend on manual verification, periodic audits, or conventional fraud detection methods. Authorities must actively examine transaction records to identify suspicious activities and verify beneficiary details. Fraud detection is commonly performed using historical records or predefined procedures, which may overlook complex fraudulent patterns. These methods do not provide highly accurate identification of fraudulent transactions. Detection in current systems is often limited by manual effort and traditional analysis techniques. There is no intelligent mechanism to automatically classify transactions based on learned fraud patterns. Large transaction datasets require significant time and effort for analysis. Overall, the existing system lacks advanced intelligence,
accuracy, and efficient fraud detection capabilities.

PROPOSED SYSTEM

The proposed system implements an AI-driven machine learning model for detecting fraudulent transactions in public welfare distribution. It analyzes financial transaction data using trained machine learning algorithms to classify transactions as legitimate or fraudulent. Suspicious transactions are identified based on learned transaction patterns, helping improve transparency and accountability in welfare distribution. This approach enhances fraud detection accuracy and supports efficient analysis of large transaction datasets. The system eliminates the need for extensive manual verification, reducing time and human effort. A publicly available financial transaction dataset is used for model training and evaluation, minimizing data collection costs. The trained machine learning model is securely stored for reliable fraud prediction and classification.

SYSTEM ARCHITECTURE

The architecture of the AI-powered public welfare fraud detection system consists of five major components: a financial transaction dataset, a data preprocessing module, a machine learning model, a prediction module, and a reporting interface. Initially, the financial transaction dataset is collected and processed through the preprocessing module, where missing values are handled, unnecessary attributes are removed, and relevant features are selected for analysis. The processed data is then used to train the machine learning model, enabling it to learn patterns associated with legitimate and fraudulent transactions. During prediction, the trained model analyzes new transaction records and classifies them as either fraudulent or legitimate based on the learned patterns. The prediction results are displayed through the reporting interface, allowing users to view detected fraudulent transactions and classification outcomes in a clear format. This architecture provides an efficient and intelligent approach for analyzing large volumes of transaction data while improving the accuracy of fraud detection. The system supports transparent public welfare distribution by reducing manual effort and assisting authorities in identifying suspicious financial activities more effectively.

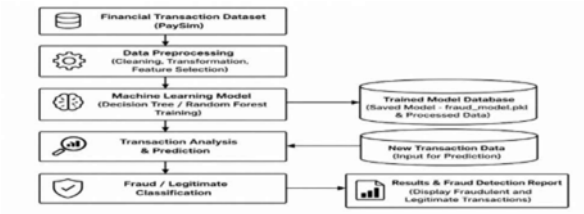

Fig 1: Block Diagram

METHODLOGY DESCRIPTION

The methodology of the AI-powered public welfare fraud detection system is designed to identify fraudulent transactions. The system follows a structured approach that includes data collection, data

preprocessing, model training, prediction, and result analysis. Financial transaction data is collected from a dataset and processed to remove inconsistencies and prepare it for analysis. The processed data is then used to train the machine learning model for identifying fraudulent transaction patterns. Based on the prediction results, the system classifies transactions as legitimate or fraudulent and displays the outcomes through the reporting interface.

RESULTS AND DISCUSSION

Fig2: Home page of Facial Recognition

The home page of the AI-powered public welfare fraud detection system serves as the main

interface through which users interact with the application.

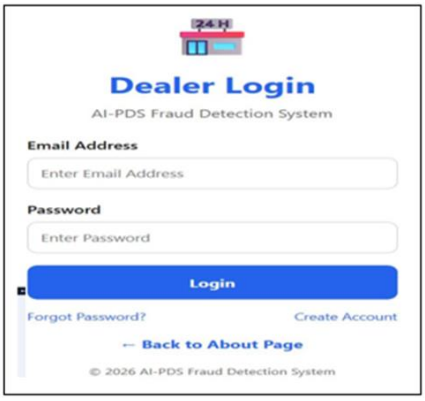

Fig 3: User Login Page

The User Login module enables registered users to securely access the system using their login credentials.

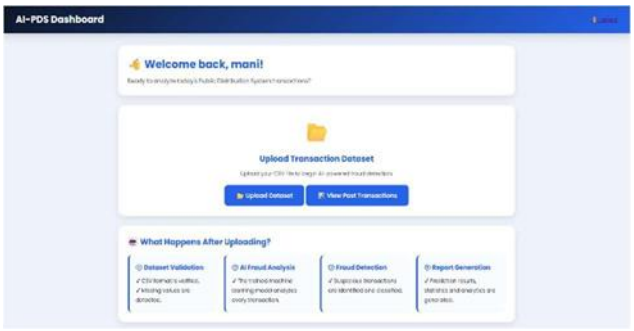

Fig 4: User Dashboard Page

The User Dashboard provides users with access to fraud prediction, transaction analysis, and other system functionalities

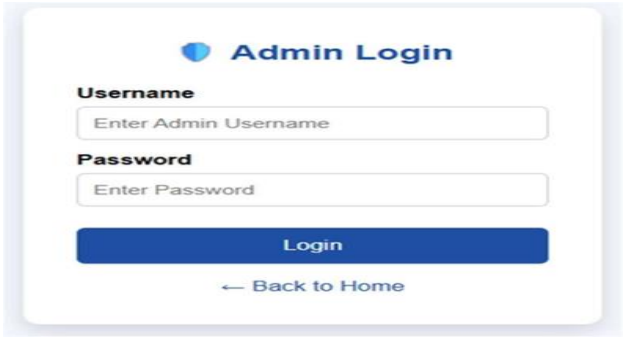

Fig5: Admin_login

The Admin Login module allows administrators to securely log in and access administrative functionalities.

Fig 6: Admin Dashboard Page

The Admin Dashboard displays system statistics, user details, and management options for monitoring the application.

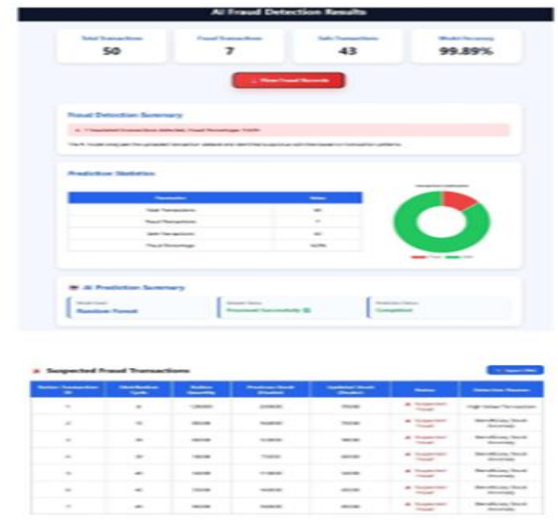

Fig 7: Predicted Fraud Transactions List

The Prediction Results module displays the classification outcome and highlights the detected fraudulent transactions.

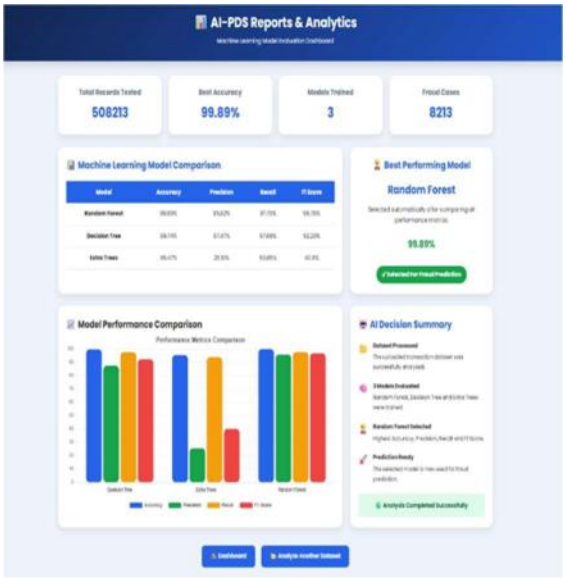

Fig. 8: Performance Analysis Module

The Performance Analysis module presents the machine learning model's performance using evaluation metrics and graphical analysis.

CONCLUSION

The AI-powered public welfare fraud detection system improves the efficiency and accuracy of fraud detection by identifying suspicious financial transactions using machine learning. By supporting transparent welfare distribution and reducing manual effort, the system provides a reliable and intelligent solution for detecting fraudulent activities.

FUTURE SCOPE

The proposed AI-powered public welfare fraud detection system can be further enhanced by integrating advanced machine learning and deep learning models to improve fraud detection accuracy.

Additional transaction features and larger datasets can be incorporated to increase the model's ability to identify complex fraudulent patterns. The system can be extended to support real-time transaction analysis for faster fraud detection and decision-making. Integration with cloud-based platforms can improve data storage, scalability, and accessibility. Furthermore, advanced data visualization and automated reporting features can be included to provide better insights into fraudulent activities and assist authorities in ensuring transparent and efficient public welfare distribution.

REFERENCES

[1] D. P. Harini, "Electronic Health Record Stage Identification using Principal Component Analysis," *Machine Intelligence Research,* vol. 18, no. 01, pp. 864- 873, 17 8 2024.

[2] D. P. Harini, "Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications," *International Journal of Engineering & Science Research,* vol. 3, no. 9, pp. 472-478, 2013.

[3] D. P. Harini, "Analyze and Predict of Human Cyber Attackers using Artificial Neural Network," *Journal of Basic Science and Engineering,* vol. 21, no. 1, pp. 1529 - 1536, 8 7 2024.

[4] Kattumuri, R. (2019). The Public Distribution System and Food Security in India. International Journal of Environmental Research and Public Health, 16(17), 3221.

[5] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data Mining for Credit Card Fraud: A Comparative Study. Decision Support Systems, 50(3), 602–613.

[6] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and Academic Review. Decision Support Systems, 50(3), 559–569.

[7] Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. Statistical Science, 17(3), 235–255.

[8] Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32.

[9] Quinlan, J. R. (1986). Induction of Decision Trees. Machine Learning, 1(1), 81–106.

[10] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys, 41(3).

[11] West, J., & Bhattacharya, M. (2016). Intelligent Financial Fraud Detection: A Comprehensive Review. Computers & Security, 57, 47–66.

[12] Kou, Y., Lu, C., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of Fraud Detection
Techniques. Proceedings of the IEEE International Conference on Networking, Sensing and Control.

[13] Han, J., Kamber, M., & Pei, J. (2012). Data Mining: Concepts and Techniques (3rd ed.). Morgan Kaufmann.

[14] Pedregosa, F., Varoquaux, G., Gramfort, A., et al. (2011). Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 12, 2825–2830.

[15] PaySim Dataset. (2016). PaySim: A Financial Mobile Money Transaction Dataset for Fraud Detection. Kaggle.