International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-Powered Fraud Prevention in Medical Treatment Fundraising

***MR.M.Ramu*[1]*,Kishorkumar.K*[2]*,Krishnamoorthi.S*[3]*,Praveenbalaji.C*[4]**

[1]Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu, India.
[2,3,4] UG- Department of Information Technology, Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu, India.

ABSTRACT:

Medical Funds offer essential financial support for individuals and families needing assistance with treatments, surgeries, or emergencies, often through crowdfunding platforms, social media, and charitable organizations. However, the growing problem of Medical Fund Fraud, where fraudsters submit fake treatment documents and bills, undermines donor trust and impacts genuine beneficiaries. Existing fraud detection systems are typically manual or semi-automated, making the verification process slow, error-prone, and less effective against sophisticated fraudulent attempts. This project presents an AI-driven system designed to detect and block fraudulent medical fund requests. It integrates YOLOv8 to detect text regions on uploaded treatment bills and PaddleOCR to extract and recognize the content accurately. Key details such as hospital names, patient information, and treatment costs are then cross-verified against a trusted hospital database using a Fuzzy Matching Algorithm, which measures the similarity between extracted data and stored records to detect inconsistencies. By automating the processes of text detection, extraction, and verification, this system significantly improves the speed and accuracy of fraud detection. The solution ultimately aims to protect donor contributions, enhance transparency, and rebuild trust in medical crowdfunding platforms.

Keywords: Yolov8,Fuzzy Matching, Paddleocr

1. INTRODUCTION

Medical fundraising is the process of raising financial support for individuals who need funds for medical treatments, surgeries, or ongoing healthcare expenses. It is commonly done through crowdfunding platforms, charitable organizations, NGOs, and community-driven efforts. People create campaigns, share their medical conditions, and request donations from the public, friends, family, or corporate sponsors.With the rise of online fundraising platforms, individuals can share their medical fund requests through social media, websites, and donation portals. However, the lack of proper verification mechanisms has led to fraudulent activities where scammers create fake medical bills to exploit donors. Hence, advanced fraud detection systems using AI and pattern-matching algorithms are essential to ensure transparency and authenticity in medical fundraising.

2. Proposed system

The proposed system aims to enhance the detection and prevention of fraudulent medical fund requests by integrating AI-driven technologies. It automates the verification process, ensuring accuracy and efficiency while minimizing human intervention.

- **Pattern Matching for Verification**

To ensure authenticity, the system utilizes the Fuzzy Matching Algorithm, which compares extracted text with a trusted hospital dataset. This method effectively measures similarity and detects inconsistencies in treatment details, preventing fraudulent fund requests.

- **Automated Document Processing**

Unlike traditional manual verification methods, the proposed system automates document processing, significantly reducing the time required for fraud detection. It eliminates human errors and ensures consistency in identifying fake medical fund requests.

- **Secure and Transparent Donation Process**

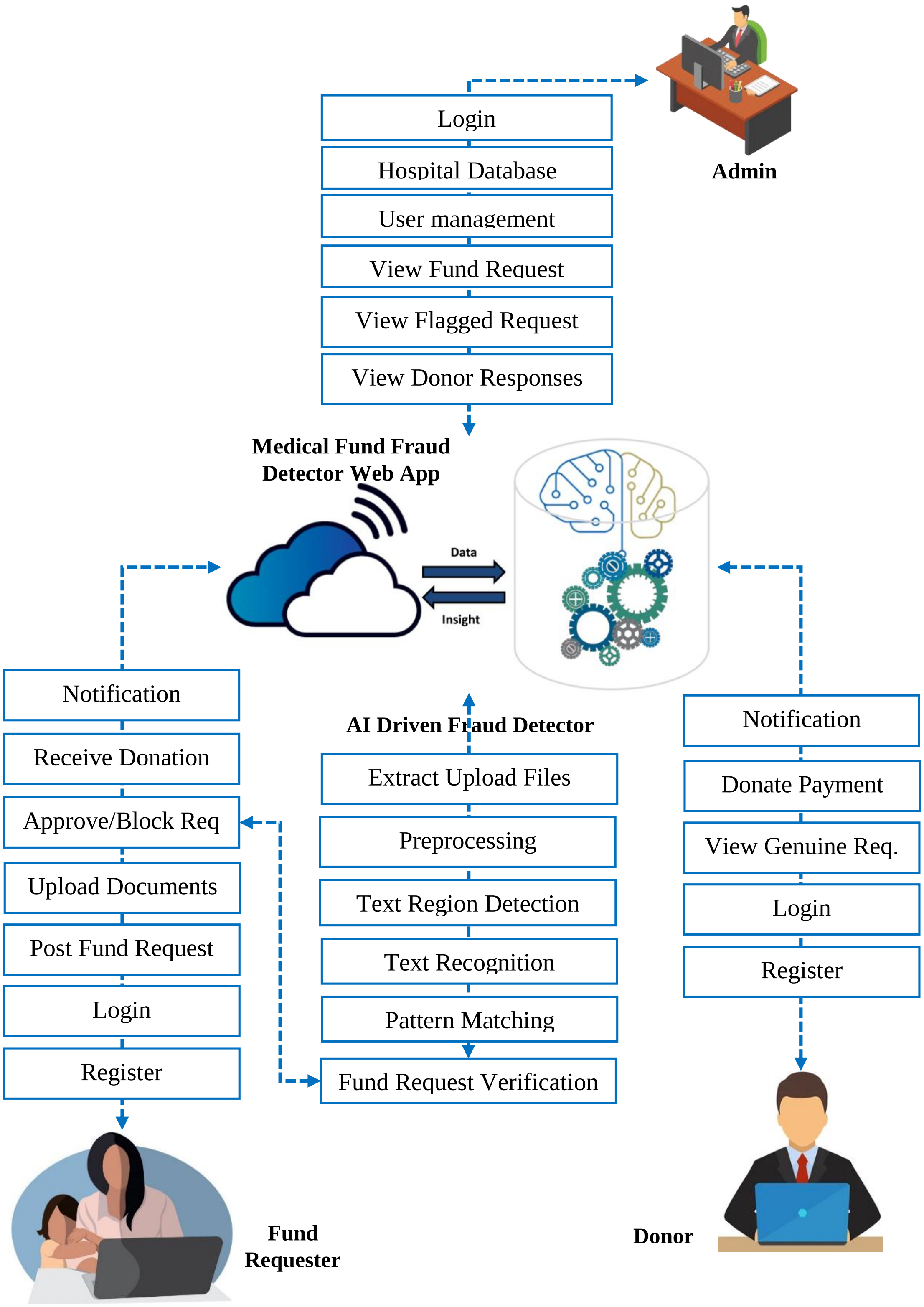
The system enhances donor confidence by providing a transparent verification process. Only verified medical fund requests are displayed to potential donors, ensuring that contributions reach genuine beneficiaries.

2.1 Advantage

- Effectively identifies and blocks fake medical fund requests using AI-driven verification
- Eliminates manual document checking, reducing errors and improving efficiency
- Ensures transparency, encouraging more donors to contribute without fear of fraud
- Quickly analyzes and verifies medical bills, preventing fraudulent requests instantly
- Protects both donors and genuine beneficiaries by verifying fund requests before approval
- Can be expanded to support multiple hospitals, crowdfunding platforms, and NGOs

- Reduces the need for manual fraud detection teams, saving operational costs
- Simplifies the donation and verification process for both patients and donors

2.2 system architecture



1. Medical Fund Fraud Detector Web App

The Medical Fund Fraud Detection System is developed to ensure transparency and authenticity in medical fund requests by leveraging Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning techniques. This project is built using Python, Flask, MySQL, WampServer, TensorFlow, Pandas, Scikit-Learn, Matplotlib, NumPy, Seaborn, Pillow, OpenCV, and Bootstrap, making it a robust web-based application. The system integrates fraud detection models with document verification to identify and prevent fraudulent medical fund requests. Flask serves as the backend framework, handling requests, authentication, and communication with the database. MySQL is used to store user information, fund request details, and fraud verification results, while WampServer provides a local environment for testing and database management. TensorFlow, Scikit-Learn, and OpenCV power the fraud detection system by processing medical documents and identifying manipulated elements such as forged signatures, tampered invoices, and duplicate requests. The YOLOv8 object detection model plays a crucial role in detecting fraud patterns in medical bills and hospital stamps. The frontend is designed using Bootstrap, ensuring a responsive and user-friendly interface. Patients can submit fund requests, upload supporting documents, and track verification results. Administrators oversee fraud detection, manage users, and train the AI model. Donors can browse verified fund requests and contribute with confidence.

2. End User

The End User Module is designed to facilitate interaction between different stakeholders of the system, ensuring seamless and secure fund transactions while preventing fraudulent activities. It consists of three primary user roles: Admin, Patient/Fund Requester, and Fund Donor, each having distinct functionalities.

2.1 Admin

The Admin plays a crucial role in managing the system by overseeing fund requests, fraud detection, and user management. The Admin Dashboard allows administrators to log in securely and perform various tasks such as training the fraud detection model, adding or removing users, and verifying fund requests. The model training process involves feeding the system with datasets of fraudulent and genuine medical documents to enhance accuracy in fraud detection. Admins can review flagged fund requests that the AI system detects as potentially fraudulent and take necessary actions. Additionally, they have access to detailed fund request and response records, ensuring transparency and accountability in financial transactions.

2.2 Patient/Fund Requester

The Patient or Fund Requester is an individual seeking financial assistance for medical treatment. They begin by registering and logging into the system. Once authenticated, they can post a fund request by providing details about their medical condition, required treatment, and uploading relevant medical documents such as bills, prescriptions, and hospital reports. After submission, the system analyzes and verifies the request using fraud detection techniques, and the requester can view the verification results. If the request is approved and donors contribute to the cause, the patient receives payment from the donor directly, ensuring a secure and transparent process.

2.3 Fund Donor

The Fund Donor is an individual or organization willing to provide financial assistance to verified medical fund requests. After registering and logging in, the donor gains access to a list of genuine and verified fund requests, ensuring that their contributions go to legitimate cases. The donor can browse patient requests, review supporting documents, and make an informed decision before donating securely through the system. This ensures a trustworthy donation process, preventing fraudulent transactions and encouraging more donors to participate.

This module establishes a secure and transparent platform where fund requests are authenticated, and donations reach the intended recipients without manipulation or fraud.

3. Hospital Database Integrator

This module is designed to establish a secure and efficient connection between the system and hospital databases. Its primary function is to validate medical fund requests by cross-referencing submitted medical documents, prescriptions, and hospital bills with the respective healthcare providers' records. This module enhances the accuracy and credibility of the verification process, reducing fraudulent claims. The integration process begins by fetching hospital data from authorized healthcare institutions, including details such as patient records, treatment history, hospital registration, and billing information. When a patient submits a fund request, the system automatically retrieves relevant details from the linked hospital database to verify the authenticity of the provided documents.

4. Medical Fund Request

The Medical Fund Request module serves as the core functionality for patients seeking financial assistance for medical treatments. This module enables patients (fund requesters) to submit requests for funding by providing necessary details, including personal information, medical condition, hospital details, treatment cost, and supporting documents such as medical prescriptions, hospital bills, and test reports. Upon submission, the system processes the request through multiple verification layers. The uploaded documents undergo preprocessing, text extraction, and fraud detection mechanisms to ensure authenticity. The module integrates with the Hospital Database Integrator to cross-verify the submitted medical records with the respective hospitals, checking for duplicate requests, forged documents, and manipulated information. Each fund request is assigned a unique reference ID and categorized based on urgency, severity of the medical condition, and required treatment cost.

4.1. Text Region Detection

This step involves identifying the areas within an uploaded document that contain textual information. Using YOLOv8, a powerful object detection model, the system scans and detects text regions in medical bills, prescriptions, and hospital documents. YOLOv8 is trained to recognize specific document attributes such as hospital names, patient details, payment sections, and diagnostic information. By isolating these text regions, the system ensures that only relevant portions of the document are processed for further analysis.

4.2. Text Recognition

Once text regions are detected, the system extracts the textual content using Optical Character Recognition (OCR) techniques, primarily leveraging Tesseract OCR. This step converts printed and handwritten text into machine-readable format, allowing for further processing. The extracted text is preprocessed to remove noise, distortions, and irregular font styles, ensuring higher accuracy in subsequent verification processes. This phase enables the system to retrieve critical data such as patient names, medical conditions, treatment costs, and hospital details for fraud analysis.

4.3. Pattern Matching

The extracted text is then analyzed to detect inconsistencies and fraudulent patterns. This is achieved through pattern matching techniques, where the text is compared against a verified hospital database to identify anomalies. The system employs fuzzy logic algorithms to detect inconsistencies such as:

- Fake or manipulated medical reports where hospital names, patient details, or treatment costs do not match official records.
- Duplicate fund requests submitted under different names but with identical medical details.
- Mismatched hospital stamps and signatures that deviate from authentic hospital documentation.

By combining machine learning, OCR, and database verification, the Fraud Detection module enhances the reliability of the system, ensuring that only genuine medical cases receive financial aid while fraudulent requests are flagged for review.

5. Fund Request Approve /Decline

The Fund Request Verification module is responsible for assessing the authenticity of submitted medical fund requests before they are approved for donor contributions. This module integrates an intelligent decision-making system that categorizes each request based on its credibility, allowing for efficient fraud prevention and transparency. The Decision System is the core of this module, automatically classifying fund requests into three categories: "Valid," "Suspicious," or "Fraud." The classification is based on various factors, including document authenticity, consistency in patient details, verification against the hospital database, and fraud detection algorithms. If a request is deemed valid, it is immediately made available for potential donors. If marked suspicious, it undergoes further review, while requests flagged as fraudulent are rejected from the system. To ensure a thorough verification process, the module includes a Manual Review Option for administrators.

6. Donor Payment Processing

The Donor Payment Processing module is responsible for handling financial transactions between donors and verified fund requesters in a secure and transparent manner. This module ensures that donations reach genuine beneficiaries while maintaining a seamless and fraud-resistant transaction system.A key component of this module is Secure Payment Gateway Integration, which ensures that all financial transactions are conducted safely. The system integrates trusted payment gateways to facilitate donations using multiple payment methods, such as credit/debit cards, online banking, and digital wallets. Advanced encryption techniques and multi-layer authentication mechanisms are implemented to protect donor information from unauthorized access and cyber threats.The module also features Transaction Tracking, which records and logs every donation transaction in a secure database. Each transaction is linked to the respective donor, patient, and fund request ID, ensuring full traceability. Donors can access their donation history, check the status of their contributions, and receive automated receipts for tax or record-keeping purposes. Admins can also monitor transaction logs to detect any irregularities or potential fraud attempts.

7.Notification Module

The Notification Module is designed to provide real-time updates and alerts to all users involved in the fund request and donation process. This module ensures that administrators, fund requesters (patients), and donors are kept informed about important events, such as fund request approvals, rejections, flagged fraud cases, and donation payments. A core feature of this module is Real-time Alerts, which instantly notify users of critical updates. When a fund request is submitted, processed, or reviewed, the system sends immediate notifications to both the fund requester and the admin. Donors also receive alerts when their donations are successfully processed or when a refund is issued in cases of fraudulent fund requests. To maximize communication efficiency, the Email & SMS Integration feature ensures that users receive updates across multiple communication channels.

3. CONCLUSION

Medical fund fraud is a growing issue where individuals or organizations submit fake, manipulated, or duplicate medical documents to unlawfully claim financial aid. This fraudulent activity results in misuse of resources, financial losses, and delays in assistance for genuine patients in need. Traditional systems for fund distribution often rely on manual verification, which is time-consuming, prone to human error, and lacks real-time fraud detection mechanisms. These existing methods fail to efficiently identify forged documents or repetitive claims, leading to ineffective fund allocation and donor distrust. To overcome these challenges, our project introduces an intelligent, automated Medical Fund Verification System that integrates YOLOv8 object detection, Optical Character Recognition (OCR), machine learning algorithms, and secure payment gateways. The system effectively detects forged bills, manipulated documents, and fake hospital stamps, ensuring that only genuine requests receive funding. Key features include automated fraud detection, a trust score system, a real-time notification module, and a secure donor payment processing system. The project not only enhances accuracy and efficiency in fund verification but also reduces fraud risks and improves transparency in medical fund distribution. With its robust fraud detection capabilities, this system increases donor confidence, ensures fair fund allocation, and streamlines the financial aid process, making it a reliable and impactful solution for combating medical fund fraud.

Acknowledgements

Let me take this opportunity to thank everyone that aided and guided me while working on my project “AI-Powered Fraud Prevention in Medical Treatment Fundraising.”

I wish to thank Ramu.M especially for their insight and encouragement which made this idea possible. I appreciate the rest of my peers, friends, and family for their support and motivation.

As AI technology matures and becomes increasingly accessible, powering it with the right technology will ensure trust and transparency in medical fundraising. I hope that my contribution will effectively augment the fight against fraud.

REFERENCES

Deng, Y., & Liu, L. (2021). “PaddleOCR: An Open-Source Optical Character Recognition (OCR) Toolkit.” arXiv preprint arXiv:2104.01932. DOI: 10.48550/arXiv.2104.01932

Detection in Healthcare Systems.” International Journal of Engineering and AdvanSahu, S., & Nayak, R. (2020). “Medical Fraud Detection using Machine Learning Techniques.” Journal of Healthcare Engineering, 2020. DOI: 10.1155/2020/3281564

Jha, A., & Verma, S. (2020). “Blockchain-Based Transparent Fundraising for Medical Applications.” Future Generation Computer Systems, 108, 791-800. DOI: 10.1016/j.future.2020.03.001

Koo, D., & Jeong, S. (2020). “Deep Learning for Medical Fraud Detection.” Computers in Biology and Medicine, 123, 103894. DOI: 10.1016/j.compbiomed.2020.103894

Kshetri, N. (2018). “1 Blockchain and Healthcare Fraud Detection: An Overview.” Computers, Privacy, and Security Issues in Healthcare, 1, 19-34. DOI: 10.1007/978-3-319-77627-1_2

kshmi, A., & Rajendran, S. (2019). “Fuzzy Matching Algorithm for Fraudulent Data

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). “You Only Look Once: Unified, Real-Time Object Detection.” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 779-788. DOI: 10.1109/CVPR.2016.91

Rid, A., & Laskowski, A. (2016). “Ethical Issues in Crowdfunding for Medical Expenses.” JAMA Internal Medicine, 176(5), 681-686. DOI: 10.1001/jamainternmed.2016.1087

Vijayalaced Technology, 8(6), 198-203. DOI: 10.35940/ijeat.F8325.088619

Flask – Grinberg, M. "Flask Web Development: Developing Web Applications with Python", O'Reilly Media.