**AI-Driven Medical Fundraising Verification System to Detect and Prevent Fraudulent Treatment Requests**

**Abstract**

Medical Fund refers to financial assistance provided to individuals or families in need of support for medical treatments, surgeries, or emergencies. Such initiatives often rely on crowdfunding platforms, social media campaigns, or charitable organizations to raise funds. However, the rise of Medical Fund Fraud has become a significant challenge, where fraudsters fabricate treatment documents or bills to solicit donations deceitfully, undermining the trust of donors and affecting genuine beneficiaries. Existing fraud detection systems are often manual or semi-automated, requiring human verification of submitted documents. These processes are time-consuming, error-prone, and struggle to identify sophisticated fraudulent attempts. The lack of comprehensive and automated mechanisms further exacerbates the issue, leading to donor skepticism and reduced willingness to contribute. This project offers an AI-driven approach to detect and block fraudulent medical fund requests. It incorporates advanced YOLOv8 for detecting text regions in uploaded treatment bills and PaddleOCR for extracting and recognizing the text. The extracted information—such as hospital names, patient details, and treatment costs—is verified against a trusted hospital dataset using the Fuzzy Matching Algorithm, which measures the similarity between extracted text and stored records to identify discrepancies effectively. By automating text detection, recognition, and pattern matching, this system ensures accurate verification of medical fund requests, safeguarding donor contributions and fostering trust in medical crowdfunding efforts.

**Software Requirements**

* **Python 3.8 or above**: For implementing the application logic and integrating AI models
* **Flask**: For building the web application and handling the backend.
* **YOLOv8**: For text detection in uploaded medical treatment bills.
* **PaddleOCR**: For text recognition from detected text regions.
* **Fuzzywuzzy**: For implementing the Fuzzy Matching to verify document authenticity.
* **OpenCV**: For image preprocessing and manipulation.
* **MySQL Server**: For storing user and medical treatment data, and verified hospital datasets
* **WampServe**r: For hosting the database locally during development.

Aim

To develop an AI-powered system for detecting and preventing fraudulent medical fund requests by verifying treatment documents using advanced text detection, recognition, and pattern-matching techniques.

Objectives

To automate the verification of medical fund requests using AI-based fraud detection.

To integrate YOLOv8 for detecting text in treatment bills and PaddleOCR for text recognition.

To apply Fuzzy Matching Algorithm to compare extracted text with authentic hospital records.

To enhance donor trust by ensuring that only genuine medical fund requests are approved.

To minimize fraudulent activities in medical crowdfunding by providing a reliable and efficient verification system.

Existing System

raditional methods for verifying medical fund requests have relied on manual processes, third-party validation, and basic rule-based checks. While these methods have been used for years, they are slow, inefficient, and prone to errors. Fraudsters have found ways to bypass these verification steps, leading to a rise in medical fund fraud. Below are some of the commonly used traditional methods and their limitations.

* **Manual Document Verification**

In this method, hospitals, crowdfunding platforms, or donors manually review medical bills, prescriptions, and other supporting documents submitted by patients. They check for inconsistencies, formatting errors, and any signs of forgery. However, this process is highly **time-consuming**, relies on human expertise, and is prone to errors, especially with sophisticated fraudulent documents.

* **Phone or Email Verification**

Donors or fundraising platforms contact hospitals or doctors via phone or email to verify if a particular patient is undergoing treatment. While this method helps confirm details, it depends on the **responsiveness of hospitals** and can lead to delays in fund approvals. Additionally, fraudsters may provide fake contact details to deceive verifiers.

* **Third-Party Trust Networks**

Some crowdfunding platforms rely on NGOs, hospitals, or medical institutions to validate medical fund requests. These trusted third parties verify patient details before approving funds. While this method adds a layer of security, it **lacks scalability** and cannot handle a large number of requests efficiently. It also depends on the availability and cooperation of third-party organizations.

* **Pattern-Based Rule Engines**

Basic fraud detection systems use predefined rules to detect suspicious activities. For example, the system may flag requests with similar medical bills, repetitive content, or unusual donation patterns. However, fraudsters can easily **modify their tactics** to bypass these rules, making this approach **less effective against advanced forgery techniques**.

* **Community-Based Reporting**

Some platforms allow users or donors to report fraudulent medical fund requests. If multiple reports are received, the request undergoes additional verification or is removed. However, this method **relies on user awareness** and does not prevent fraud before funds are collected. Many fraudulent campaigns may go unnoticed if no one reports them in time.

**Existing Rule-Based Algorithms**

Rule-based algorithms are traditional approaches used in fraud detection systems, relying on predefined conditions to identify fraudulent activities. These methods operate on static rules that classify transactions or documents as genuine or fraudulent based on specified criteria. However, while effective in simple cases, rule-based approaches struggle with evolving fraud techniques and sophisticated forgeries. Below are some common rule-based algorithms used in fraud detection, along with their descriptions and limitations:

* **Regular Expression (Regex) Matching**

Regular Expression Matching is widely used to detect predefined patterns in medical invoices, receipts, and supporting documents. It checks for specific structures such as hospital names, patient details, and date formats.

**Example:** A rule might validate if a date follows the format DD-MM-YYYY or if a hospital name matches an approved list.

* **Keyword-Based Filtering**

This technique scans medical fund requests for specific keywords like "emergency," "ICU," "surgery," or "cancer treatment." If a request lacks these critical terms, it may be flagged as suspicious.

**Example:** A donation request for medical treatment should contain essential keywords like "hospital," "prescription," or "doctor." If these words are absent, the system raises a red flag.

* **Basic Pattern Matching**

Pattern Matching compares uploaded medical bills with a database of verified invoices to detect inconsistencies in structure, format, or content.

**Example:** If a fraudulent bill has an incorrect hospital logo, altered font styles, or mismatched invoice numbers, the system identifies the discrepancies.

**Drawbacks**

* **Time-Consuming:** Manual verification processes cause delays in fund approvals.
* **Prone to Human Errors:** Fraudulent documents may go undetected due to oversight.
* **Lack of Scalability:** Inefficient for handling large volumes of fund requests.
* **Easily Exploitable:** Fraudsters manipulate documents to bypass verification.
* **Delayed Fund Disbursement:** Genuine patients may suffer due to slow verification.
* Rigid and Static – Cannot adapt to evolving fraud techniques.
* High Error Rate – Leads to false positives and false negatives.
* Easy to Bypass – Simple modifications can evade detection.
* Limited Scalability – Requires frequent manual updates.
* Poor Handling of Complex Data – Struggles with unstructured data like images and handwritten documents.

**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.

* **AI-Based Fraud Detection**

The system employs **YOLOv8** for detecting text regions in medical bills and **PaddleOCR** for extracting textual information such as hospital names, patient details, and treatment costs. These extracted details are then analyzed to identify potential discrepancies.

* **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.

**Advantages**

* **Enhanced Fraud Detection** – Effectively identifies and blocks fake medical fund requests using AI-driven verification.
* **Automated Verification** – Eliminates manual document checking, reducing errors and improving efficiency.
* **Donor Confidence** – Ensures transparency, encouraging more donors to contribute without fear of fraud.
* **Real-Time Processing** – Quickly analyzes and verifies medical bills, preventing fraudulent requests instantly.
* **Secure Transactions** – Protects both donors and genuine beneficiaries by verifying fund requests before approval.
* **Scalability** – Can be expanded to support multiple hospitals, crowdfunding platforms, and NGOs.
* **Cost-Effective** – Reduces the need for manual fraud detection teams, saving operational costs.
* **User-Friendly Interface** – Simplifies the donation and verification process for both patients and donors.

**Modules**

1. Medical Fund Fraud Detector Web App

2. End User

2.1. Admin

2.2. Patient/Fund Requester

2.3. Donors

3. Hospital Database Integrator

4. Medical Fund Request

5. Fraud Detection

5.1. Preprocessing

5.2. Text Region Detection

5.3. Text Recognition

5.4. Pattern Matching

6. Fund Request Verification

7. Donor Payment Processing

8. Notification

**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. The project also integrates text recognition, pattern matching, and deep learning algorithms to enhance fraud detection accuracy. By combining AI-driven fraud analysis with hospital database verification, the system ensures that only genuine medical cases receive financial aid, minimizing scams and improving transparency in medical fundraising.

**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. This verification includes checking hospital stamps, doctor signatures, billing authenticity, and prescribed treatments. This module supports multiple hospital databases through secure APIs, encrypted data transfer protocols, and authentication mechanisms. It also implements real-time validation, where discrepancies between submitted documents and hospital records trigger alerts for further review by the admin. Additionally, this module is designed to comply with data privacy regulations, ensuring that sensitive patient information is handled securely and only used for verification purposes.

**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. The module also provides real-time tracking, allowing patients to view the status of their requests, whether it is under review, approved, flagged for verification, or rejected. If the request is flagged as suspicious, the system escalates it to the Admin for manual inspection. Once verified, the request is made available to registered fund donors who can review the case details and contribute financially. If a donation is made, the module ensures secure payment processing and updates the request status accordingly. This module ensures transparency, security, and efficiency, streamlining the process of receiving medical financial aid while mitigating fraudulent activities.

**5. Fraud Detection**

The Fraud Detection module is a critical component designed to ensure the authenticity of medical fund requests by analyzing submitted documents and identifying fraudulent activities. It employs a combination of deep learning, Optical Character Recognition (OCR), and pattern matching techniques to detect anomalies such as forged medical bills, fake hospital stamps, manipulated prescriptions, and duplicate requests. The module systematically processes uploaded documents through three key submodules:

**5.1. 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.

**5.2. 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.

**5.3. 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.

**6. 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. This feature allows system admins to manually inspect flagged fund requests, cross-check submitted documents, and make informed decisions regarding approval or rejection. Admins can override automated classifications in cases where the system might have incorrectly flagged a request. Another key feature of this module is the Trust Score Generation, which assigns a fraud probability score to each request. Using machine learning algorithms, the system evaluates factors such as document consistency, past request history, hospital validation checks, and detected anomalies to generate a score. The trust score helps admins and donors assess the reliability of a request before making a donation.

**7. 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.

To address fraudulent fund requests, the module includes a Refund Mechanism that handles reimbursement procedures in cases where a donation was made to a fraudulently flagged request. If a request is later identified as fraudulent, the system notifies the donor and initiates a refund process. The refund can be automatically processed or manually reviewed by admins, depending on the case. This mechanism builds trust among donors by assuring them that their contributions are safeguarded from misuse.

8. **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. The system automatically generates and sends email confirmations, SMS notifications, and in-app alerts based on the user's preferences. For example, a patient will be notified when their request is approved, a donor will receive a confirmation of their payment, and an admin will be alerted when a suspicious request is flagged.

**System Flow of the Project**

The system flow outlines how the **Medical Fund Fraud Detection System** operates, detailing each step from user interaction to fraud detection and fund disbursement. The following stages define the system’s workflow:

**1. User Registration & Authentication**

* **Patients, donors, and admins** must register by providing required details.
* **Authentication system** ensures secure login via email and password.

**2. Fund Request Submission**

* **Patient/Fund Requester** submits a request by uploading medical documents and entering required details.
* The system stores the request in the **database for verification**.

**3. Fraud Detection & Verification**

* **Preprocessing:** Uploaded documents are processed using image enhancement techniques.
* **Text Region Detection:** YOLOv8 detects and extracts text from medical documents.
* **Text Recognition:** OCR extracts the text from the detected regions.
* **Pattern Matching:** Extracted text is compared with a **hospital database** to verify legitimacy.
* **Decision System:** The system classifies requests as **"Valid," "Suspicious," or "Fraud."**
* **Admin Manual Review:** Flagged requests are manually reviewed before approval or rejection.

**4. Approval or Rejection of Fund Requests**

* If **verified**, the request moves to the **donation stage.**
* If **flagged as fraud**, the request is rejected, and the patient is notified.

**5. Donor Interaction & Payment Processing**

* **Donors log in**, view genuine fund requests, and make donations.
* Payment is processed via a **secure payment gateway** and logged in the database.

**6. Fund Disbursement & Notifications**

* If a donor makes a successful payment, the system transfers the amount to the verified patient.
* The **notification module** alerts users about approvals, payments, and flagged fraud cases.
* In case of fraudulent detection **after payment**, a **refund mechanism** is activated.

**7. Continuous Model Training & Improvement**

* The **fraud detection model** is continuously updated using newly identified fraud patterns.
* The admin can **train the YOLOv8 model** with new datasets to improve fraud detection accuracy.

**Project Overview**

The Medical Fund Fraud Detection System is designed to ensure transparency and security in medical fund requests by detecting fraudulent activities. This project leverages advanced technologies, including Python, Flask, MySQL, Wampserver, TensorFlow, Pandas, Scikit-Learn, Matplotlib, NumPy, Seaborn, Pillow, OpenCV, and Bootstrap, to analyze and verify fund requests. The system allows patients to submit medical fund requests, donors to contribute securely, and administrators to monitor and review transactions. A core component of this system is the fraud detection module, which utilizes YOLOv8 for text region detection and OCR for text recognition to analyze uploaded medical documents. The extracted data is cross-verified with a hospital database to identify inconsistencies using pattern-matching techniques and fuzzy logic algorithms. Requests are classified as valid, suspicious, or fraudulent, ensuring only genuine cases receive donations. Additionally, the system integrates a secure payment gateway, real-time notifications, and an admin review feature for flagged requests. This approach minimizes fraudulent transactions, enhances trust between donors and recipients, and streamlines the medical funding process with automated verification and real-time fraud detection.

**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.

**Future Enhancement**

* **Blockchain Integration for Security**

Implementing blockchain technology will ensure tamper-proof record-keeping for medical documents and transactions. Smart contracts can automate fund disbursement, ensuring that payments are released only after proper verification, reducing human errors and fraudulent claims.

* **Mobile Application for Accessibility**

Developing a mobile version of the system will allow patients, donors, and administrators to access and manage fund requests from anywhere. Real-time notifications, instant fund verification, and fraud alerts can improve usability and engagement.

* **Integration with Government and Insurance Databases**

To enhance verification accuracy, the system can be integrated with **government healthcare schemes and insurance company databases**. This will allow **real-time validation** of medical records and reduce fraudulent claims.