**SYNOPSIS**

**ON**

**“FACE ATTENDENCE RECOGNITION SYSTEM ”**

Submitted in

Partial Fulfillment of requirements for the Award of Degree

*of*

Bachelor of Technology

*In*

Information Technology By

**(Project Id : 24\_IT\_3B\_12)**

Suvansh Arora (2201640130113)

Saksham Pandey (2201640130093)

Yashna Singh (22016401300129)

Yash Raj (2201640130130)

Yuvraj Singh (2201640130131)

Under the supervision of **Ms. Sweta Sri Associate Professor**



**Pranveer Singh Institute of Technology**.

Kanpur - Agra - Delhi National Highway - 19 Bhauti -Kanpur - 209305.

(Affiliated to Dr. A.P.J. Abdul Kalam Technical University)

* **Introduction**

**A Face Attendance Recognition System** is an advanced technology that leverages facial recognition to automate the process of tracking and recording attendance. This system captures images or video of individuals, identifies them using biometric facial features, and then logs their attendance in a database, eliminating the need for traditional, manual methods like roll calls, punch cards, or RFID systems.

**Field of the Project:**

This project primarily focuses on using facial recognition technology to identify and verify individuals based on unique facial features. By leveraging **Machine Learning** and **Deep Learning** techniques, the system is trained to detect, extract, and compare facial data for accurate attendance tracking. This project integrates elements of image processing, pattern recognition, and automation, making it highly relevant in industries requiring efficient, secure, and contactless attendance management solutions.

**Special Technical Terms**:

* **Biometrics:** The measurement and statistical analysis of people's physical and behavioral characteristics for identification purposes.
* **Facial Recognition:** A biometric software application capable of identifying or verifying a person by analyzing patterns based on the person's facial features.
* **Face Detection:** The process of locating a human face within an image or video.
* Feature Extraction: Identifying and extracting key facial landmarks (e.g., eyes, nose, mouth) to create a unique facial signature.
* **Deep Learning:** A subset of machine learning involving neural networks, particularly Convolutional Neural Networks (CNNs), for training the system to recognize patterns in facial images.

**Project Objective**

The **UPI Fraud Detection** system aims to achieve the following objectives:

* **Real-Time Fraud Detection:**

Develop a system capable of identifying and preventing fraudulent UPI transactions in real-time, using machine learning algorithms to monitor transaction patterns and flag suspicious activities.

* **High Detection Accuracy:**

Aim for high accuracy in detecting fraudulent transactions while minimizing false positives and false negatives ensuring that legitimate transactions are not blocked unnecessarily.

* **User and Transaction Profiling**:

Build models that use user behaviour, transaction history, and risk assessment to detect anomalies and differentiate between normal and potentially fraudulent activities.

* **Efficient Data Management**:

Create a source and scalable system to manage transaction data, user profiles, and fraud

detection outcomes efficiently, ensuring data integrity and confidentiality.

* **Alert System for Suspicious Activity:**

Implement an alert system that notifies users and administrators when potentially fraudulent transactions are detected, allowing for quick intervention and blocking of transactions.

* **Adaptable Fraud Detection Model:**

Design the fraud detection algorithm to adapt to emerging fraud techniques by updating

models with new data, keeping the system effective against evolving threats.

* **Scalability for Growing Transaction Volume**:

Develop the system to handle an increasing number of transactions as UPI usage continues to grow, ensuring performance remains optimal as the user base expands.

* **Feasibility Study:**

The feasibility study evaluates whether the **UPI Fraud Detection** will succeed by assessing its practicality and analyzing the opportunities and threats associated with the proposed plan. The study will cover various types of feasibility: technical, operational, economic, schedule, and legal feasibility.

**Types of Feasibility:**

* **Technical Feasibility**:
* **Technology Requirements**: The project will use Python, Scikit-learn, and cloud computing services to build the fraud detection model.
* **System Compatibility**: The system will work with existing banking and financial

technologies, ensuring integration with UPI platforms.

* **Scalability**: The system architecture will support scalability for increased user numbers and data volume.
* **Operational Feasibility**:
* **User Acceptance**: The System will be user- fr iendly, with clear

notifications for both administrators and users during fraudulent events.

* **Seamless Integration**: Ensure that the fraud detection system can seamlessly integrate with existing UPI transaction systems, allowing real-time data exchange without disrupting ongoing operations.
* **Response Procedures**: Define clear response procedures for how to handle suspected fraudulent transactions, including investigation steps and resolution processes.
* **Economic Feasibility**:
* **Cost Analysis:** The costs associated with development include cloud services for data storage and machine learning model deployment. However, potential savings in fraud prevention can offset the expenses.
* **Investment (ROI)**: Estimate the potential savings achieved by reducing fraud losses, including avoided financial losses and administrative costs related to fraud investigations.
* **Budget Planning**: : Create a comprehensive budget that outlines all expected costs and potential revenues. This should include projections for the first few years of operation.
* **Schedule Feasibility**:
* **Project Timeline**: Outlining a project timeline that includes key phases: planning, development, testing, and deployment.
* **Milestones**: Setting specific milestones to track project progress and ensure timely completion.
* **Legal Feasibility**:
* **Data Protection Laws**: Ensure compliance with laws such as the General Data Protection Regulation (GDPR) if applicable, and India’s Information Technology Act. This includes obtaining necessary consent from users for data collection and processing.
* **Liability for Fraudulent Transactions**: Clarify the liability of the involved parties (e.g., banks, service providers) in cases where fraudulent transactions are not detected or acted upon in a timely manner.
* **Intellectual Property**: Assess the intellectual property rights related to the software, algorithms, and machine learning models used in the project to ensure that you have the right to use and modify them.
* **Methodology/ Planning of work**

. **1. Requirement Analysis:**

* Identify the data required for detecting fraud, including historical transaction data, user

profiles, and fraud reports.

* Define user roles, including Admins and Users.
* **System Design**
* **Architecture Design:**
* Input: UPI transaction data.
* Processing: Machine Learning Algorithms applied for detecting fraud.
* Output: Fraudulent transaction alerts.
* **DFD (Data Flow Diagram):**
* Users → Transaction Data → Detect Fraud → Fraud Alerts → Bank → Alert

→User.

* **Database Design:** Use MySQL for storing UPI transaction data, fraud reports and user profiles**.**
* **Module Development:**
* Train machine learning models such as Random Forest and Logistic Regression.
* Develop anomaly detection techniques for identifying unusual transaction patterns.
* **Data Processing:** Clean and preprocess transaction data for training and testing the model..
* **Testing and Validation**: Perform tests to ensure accuracy and minimize false positives,

and security tests to ensure reliability and compliance with data privacy regulations**.**

* **Deployment:** Deploy the system on cloud infrastructure for real-time fraud detection.
* **Maintenance:** Provide ongoing monitoring and updates to the fraud detection algorithm.
* **Tools/Technology Used:**
* **Minimum Hardware Requirements**

Hardware required for the development of the project.

* **CPU:** Intel i5 or Higher
* **RAM:** 8 GB or Higher
* **STORAGE:** 256 GB SSD or Higher

**5.2 Minimum Software Requirements**

For the development and execution of the project, the following software tools are required:

* Operating System: Windows 10 or above, or Linux (Ubuntu 18.04 or above)
* Programming Language: Python 3.x
* Libraries/Frameworks:
* Scikit-learn: For machine learning algorithms.
* Pandas: For data handling and exporting attendance records to Excel.
* MySQL: For database management.
* IDE/Editor: PyCharm, VS Code, or any Python-compatible IDE
* **References: [IEEE format]:**
* G. Brown and T. Hastie, "Machine Learning for Financial Fraud Detection."
* P. McKinney, "Data Structures for Machine Learning."
* L. Breiman, "Random Forests."