Comprehensive Design and Analysis Project

Design Document

IT16158764 B.M.C.S. Basnayake

IT16120280 N.P. Seneviratne

IT16129740 Y.C. Tittagalla

IT16160330 U.P.A.S.D. Amarasinghe

Fraud Detection Based on Human Behavioral Patterns

Bachelor of Science (Honors) in Information Technology

Department of Software Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

May 2019

Contents

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Purpose

The purpose of this DD (Design Document) is to provide a detailed description about how we can identify fraudsters using human behavior patterns and how we have incorporated this with machine learning to identify fraudsters in real time. There are four major components in this system and in section 2 of this document will explain how each of these components are working and finally how these components will come together to give a final result.

This document includes system interfaces, hardware interfaces, site adaptation requirements and constraints which are imposed on the system. This design document also will indicate all the functional and non-functional requirements of each component and will compare it with the systems that are currently available in the market and if no such system exist then a comparison will be done with the researches that have been done up to date. Also, this document will describe about the indented goals to be achieved and the benefits and objectives of this study which will explain the expectations and purpose of this research.

The main intended audience of this DD are mainly researchers and developers who would like to know more about how this system works and what are the requirements that are needed to run a system that functions similar to this. This will also give a high-level overview/architecture of the system.

1.2 Scope

This document will contain the abstracts and details of the four modules named fraud detection by micro facial expressions, voice detection, body movements and transaction details. The main functional requirement of this system is to detect fraud as early as possible. It is done by using four unique methods stated above.

- Facial expressions module – identifies the crucial expressions of a human face and interprets the meaning of those expression according to theories.
- Voice module – detects the voice of the customer and separate the noise from the actual data and analyze for suspicious elements of the voice.

- Behavior module – body movements of the humans will be examined thoroughly and analyzed to detect abnormalities.
- Transaction module – get the details of the real time transactions and analyze with known patterns and rules to detect an abnormality.

This document will compare our modules with the other competing systems in the market and also the researches that have been done before. User interfaces, hardware interfaces and communication interfaces will be discussed along. How the deployment environment should be adapted to match with our needs will also be addressed in the document. The functions of the modules will be deeply discussed.

The system only gives a possibility of a fraud attack. Rules, patterns will be used by the machine learning models to predict the frauds. One of the main requirements of the system is to give the most accurate results as possible. Because the bank depends on this system to detect frauds. If an error happens, the loss will be very high. So, reliability, accuracy and efficiency are key non-functional requirements in the system.

By using this system for the protection of a bank, it will save lots of human power, money. In a regular banking system, personnel try to identify fraudulent behaviors using their own knowledge. It is not efficient and not accurate as well. And the human power is wasted for tasks they are not prepared for. Our solution will be a four in one package that will resolve all these issues faced by a traditional bank.

1.3 Definitions, Acronyms, and Abbreviations

UI	User Interface
LAN	Local Area Network
ML	Machine Learning
POS	Point Of Service
ATM	Automatic Teller Machine
CCTV	Closed-Circuit Television Camera
BLOB	Binary Large Object
ML	Machine Learning
DD	Design Document
3D	3 Dimensional
PCA	Principal Component Analysis
DVR	Digital Video Recorder
FOV	Field Of View
GPU	Graphics Processing Unit
RAM	Random Access Memory
PCI	Peripheral Component Interconnect
SSD	Solid State Drive
CPU	Central Processing Unit
LAN	Local Area Network
WAN	Wide Area Network

Table 1:Abbreviations

1.4 Overview

The main goal of this system is to identify fraudsters using behavior patterns and in this DD we will describe what ate the major components of this systems, how we will achieve this by using Machine Learning (ML) and what are the future plans for this system.

In the 1st section of this DD contains the purpose which will describe about preparing the DD and scope of the system which will give a description about the benefits, goals and objective that we will achieve by implementing this fraud detection system. This section will also cover how the DD is organized in to main three parts and what are the rest of the document contains.

In the 2nd section overall description will include the product perspective that will compare the application with the other competitive products, systems, users, hardware, software, researches. This will also provide the reader of this document summary of the main functions in the system and the characteristics that describe what kind user(s) will use the system and what kind of knowledge will they need to operate the system. Constraints that describe all the conditions that may limit developers' options and also this section will include the assumptions and dependencies that will affect the development of the system.

The 3rd section contains the specific requirements describes the design characteristics and external behaviors of the system in technical terms and in a more detailed manner than in the section two. user interfaces in detail and hardware, software interfaces and explains the functional requirements of the system.

2 OVERALL DESCRIPTIONS

Comment: Overall description of software - more detailed than in 1.5. This should be general enough so that it is unlikely to change much in future versions. Avoid statements that are repeated in later sections.

2.1 Product perspective

There are no existing working commercial systems that are built with this kind of combination of components there are some fraud detection software that are built around only one of the components in our system.

Fraud Labs Pro this software is a commercially used software for fraud detection using transaction patterns so there is a high risk of single point of failure in the product. In comparison our product will have three more components to backup this result.

Polygraphs machine is one of similar device, but purpose of polygraph machine is to detect lies on criminal activities. Polygraphs machine can only be able to use with single person and covered environment without any background noises. This fraud

detecting product is all about finding frauds before it happens and this product is mostly focusing crowded environments. **(Polygraphs machine)**

X13-VSA is the closest publicly available product found on internet. This system only analyzing the voices stress level to detect the lies. although this system is analyzing voice with algorithms. And this product also focusing one person in a crowded environment this product also will not works. (X13-VSA Reference)

Riskified - A fraud prevention system

Riskified is a fraud prevention, competitive application that is in the current market. They have a ecosystem which consists of billions of transaction recorded. A lot of information will be recorded such as names, emails, shipping, billing addresses. For each transaction, they will run an elastic query to get a list of similar historical orders. This will help to categorize legitimate and fraud transactions.

The above stated functionality of *Riskify* will be implemented in this research's transaction module too. All the historical data will be used for learning purposes of the machine learning model.

In most of the research that have been carried out in the video based anomaly detection only focus on one or two human behavior patterns to distinguish normal behaviors from abnormal behaviors in [28] they used a BLOB to identify humans but in it they also differentiate the foreground and the background of the footage they receive but the problem was the images it was hard to identify every single anomaly. The researchers used human part segmentation and PCA (Principle Component Analysis) to choose the most suitable feature in the scene. This modeling approach for unusual events' detection is good only if these abnormal events are well defined and there are enough training data.

In [29] it reviews a list of most popular methods that are currently used in human anomaly detection. Most of the research that are reviewed does not take account the 3D space around human so it cannot identify those movements but, in this research,, we will be using dense-pose [30] to create surface-based representation of the human body to represent 3D space.

2.1.1 System interfaces

- The Windows or Linux application installed in the administrator's personal computer.
- The database which stores the transaction information of the counters and the teller machines.
- The database to store all the predicted values of the transactions.

2.1.2 User interfaces

Below are the sketches of user interfaces used by this software module. They will be described in details in section 3.

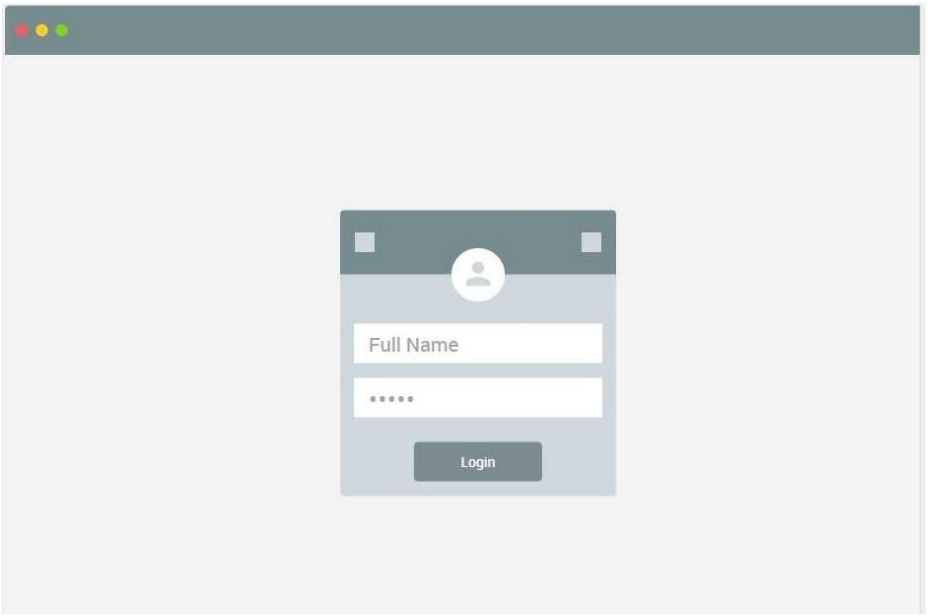


Figure 1: Login Page

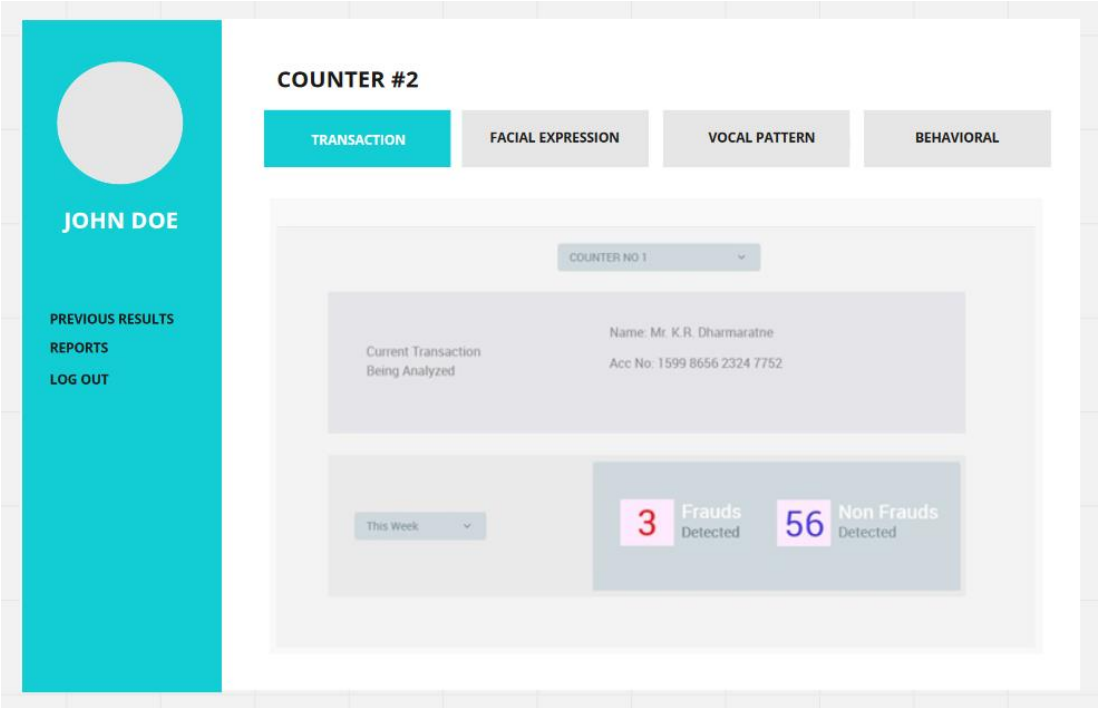


Figure 2: Transaction Analyzing Dashboard

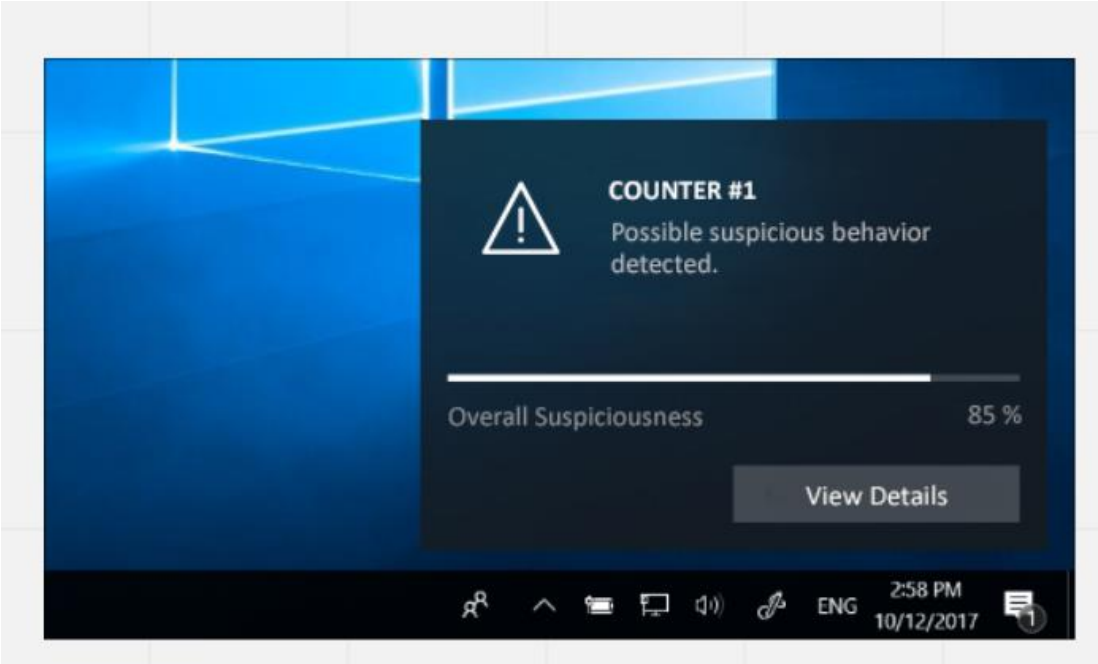


Figure 3: Windows Notification.

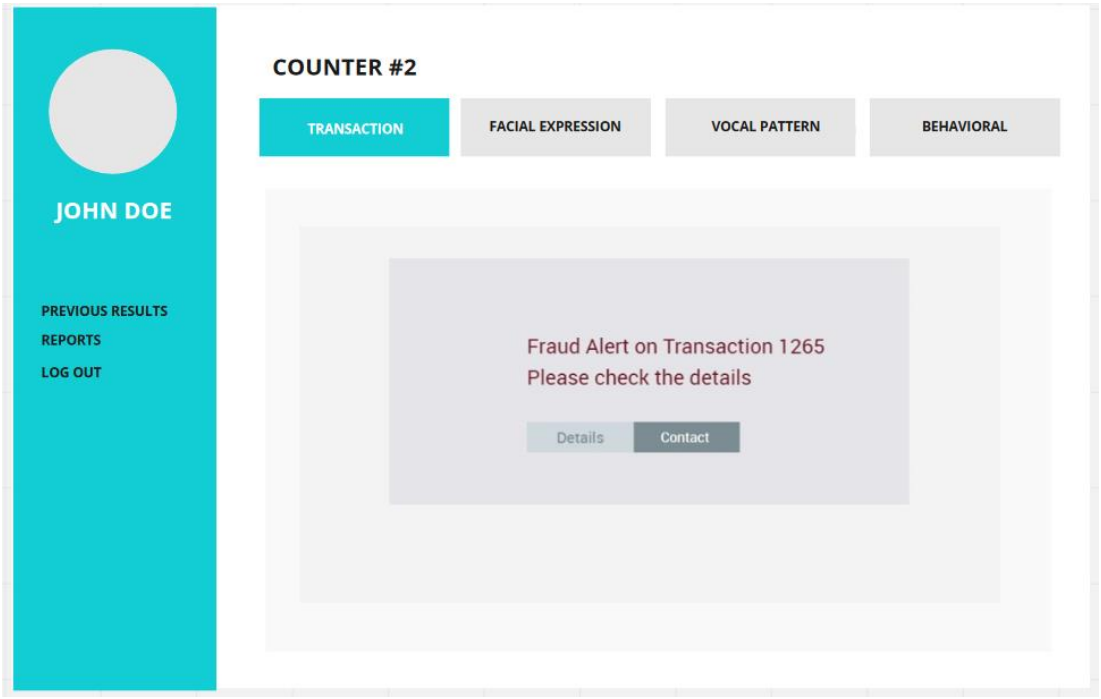


Figure 4: Alert Popup

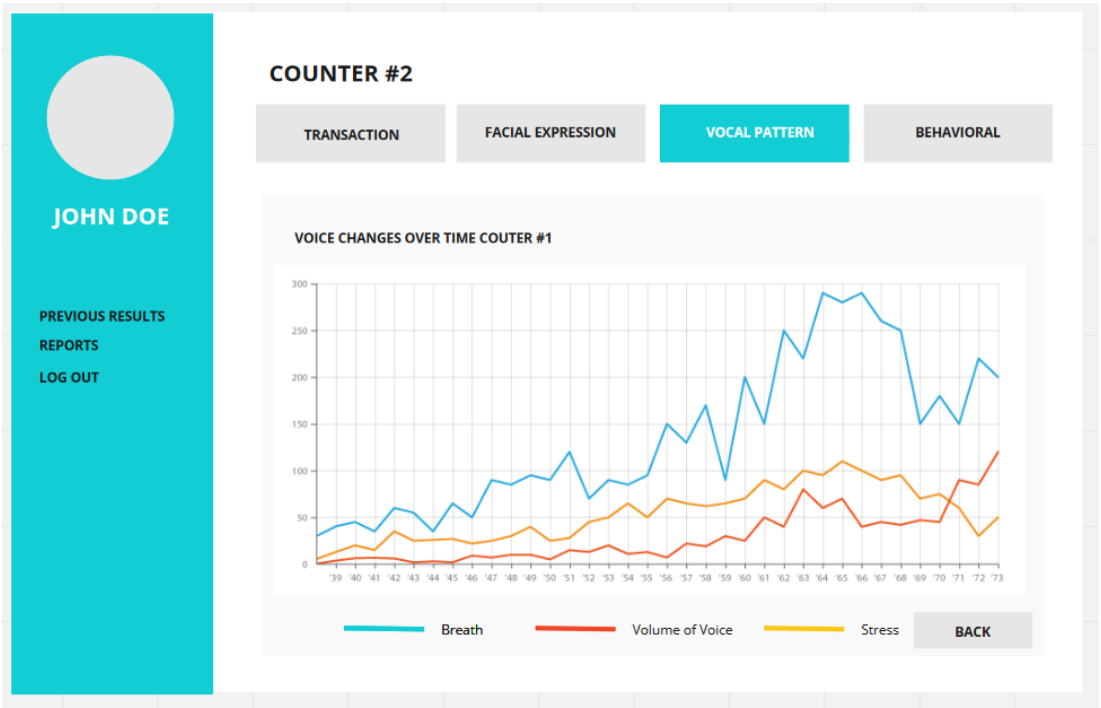


Figure 5: Voice Analyzed Details Dashboard

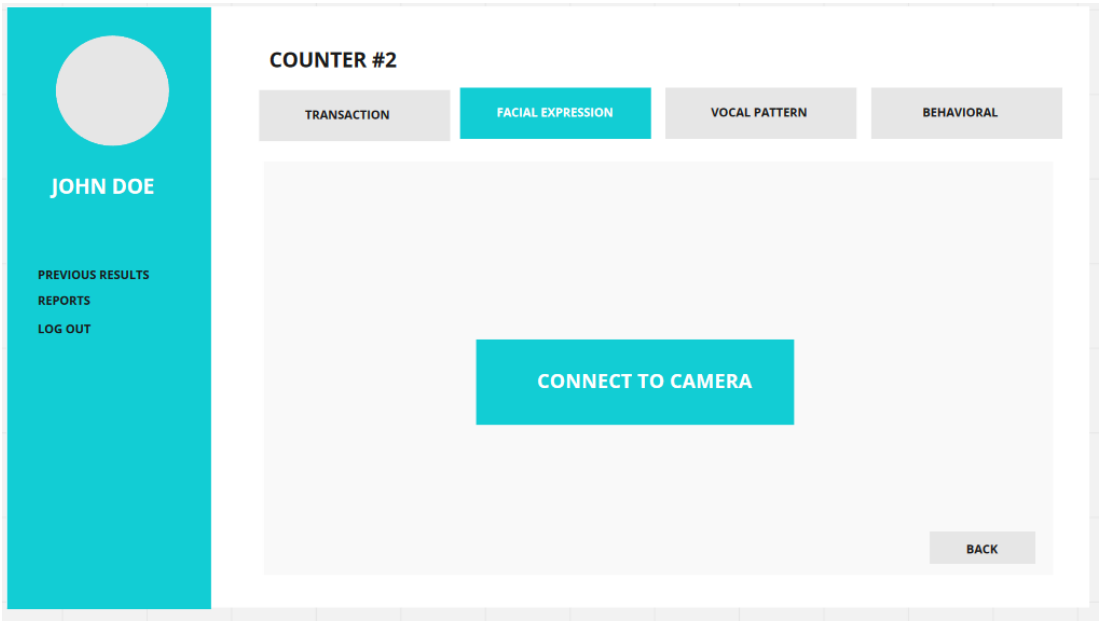


Figure 6: UI For Connect Camera.

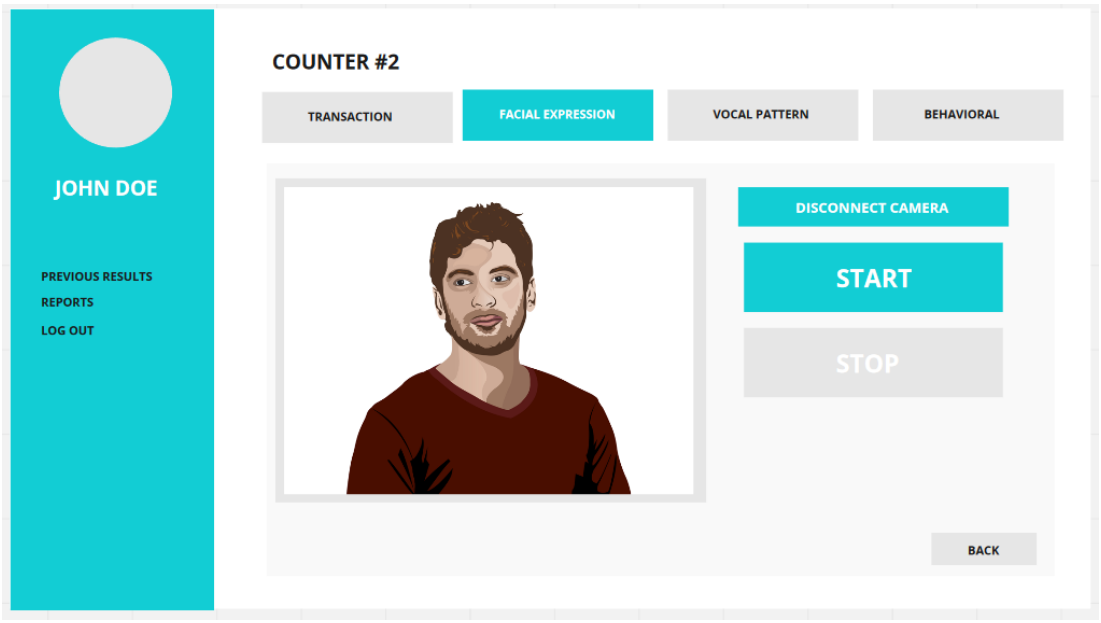


Figure 7: UI to Start Detecting

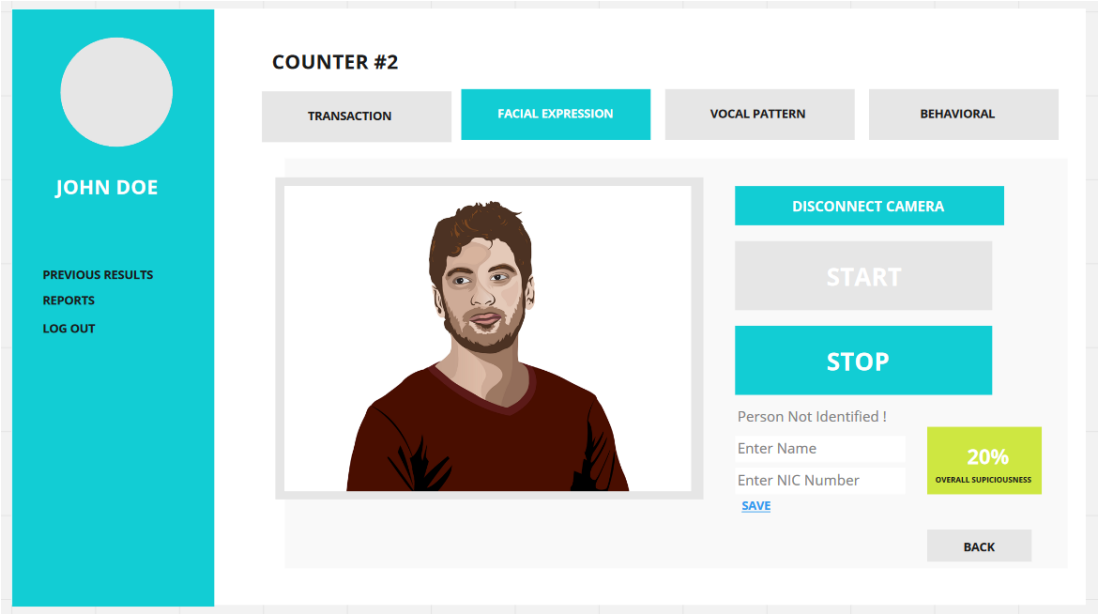


Figure 8: UI for Unidentified with Ordinary Behaving Person.

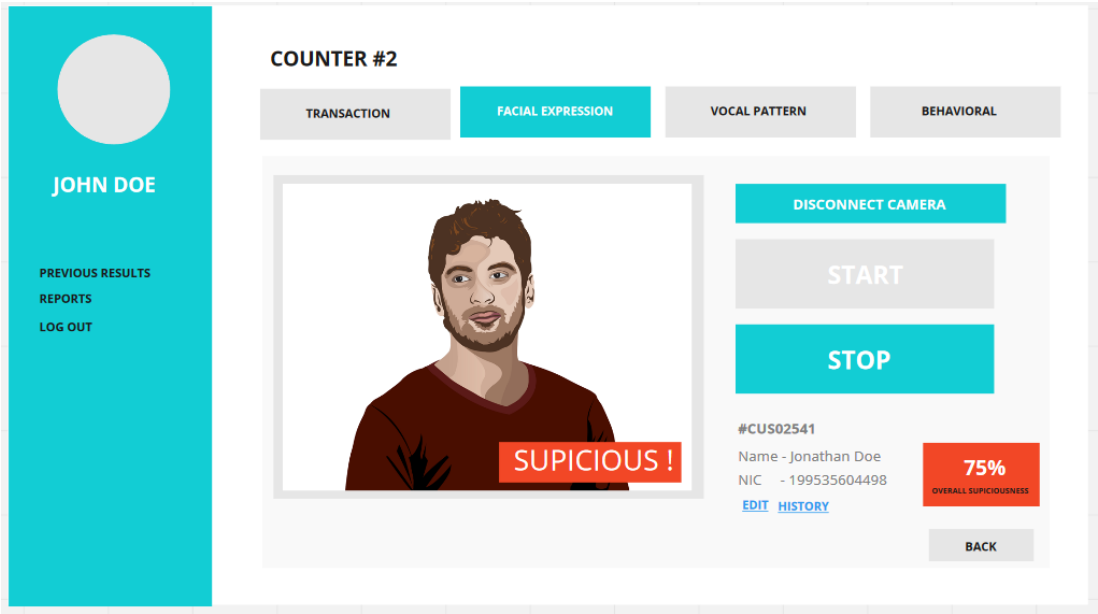


Figure 9: UI of Suspicious person detecting.

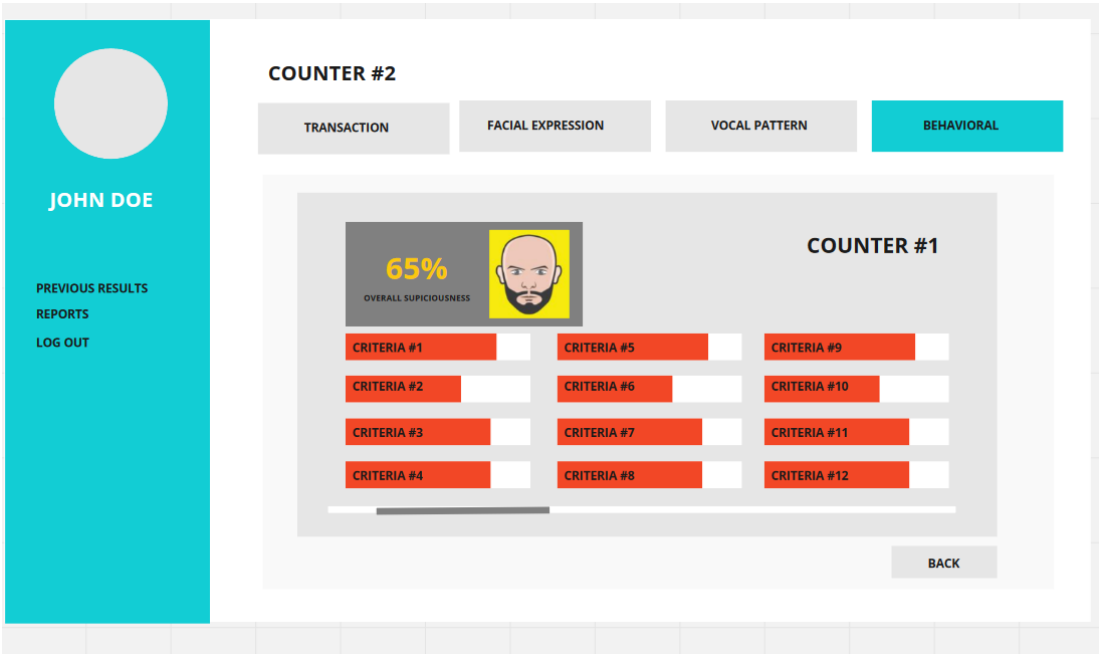


Figure 10: Behavior Analyzed Details Dashboard

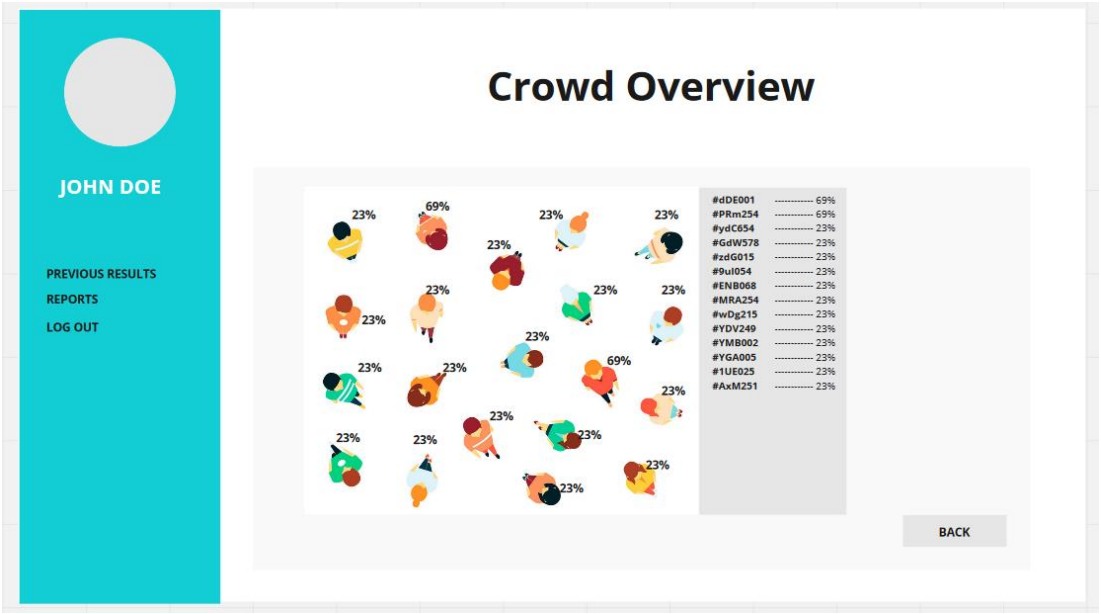


Figure 11: Crowd Overview Dashboard

2.1.3 Hardware interfaces

2.1.3.1 Facial Pattern based fraud detection module

Camera to get facial data

We need to digital camera with good quality in order to identify person's face and expressions.

Windows PC

Need a Windows PC to connect the camera and send processed data to servers.

2.1.3.2 Voice Based Fraud Detection Module

There are few main required hardware interfaces involving for voice-based fraud detection module. Microphones is the main device which is using to captures the voice of the current customer. Since there are several counters this all microphone should have to connect to one single system. So, USB Hub require to achieve this problem.

2.1.3.3 Transaction Module

Specific hardware devices will not be needed for this module of the system since it is based on analyzing transaction details. But a functioning system unit is required to use the deploy the system and to monitor it. Other modules of this system will need specific hardware devices to detect and analyze human behavioral patterns to identify the fraud patterns.

2.1.3.4 Body Language Module

CCTV Cameras will be needed to take the input of the surveillance video into the component and if the site contains multiple cameras, we need to send them streamlined for the we can use DVR.

2.1.4 Software interfaces

The machine learning models will be trained by using TensorFlow framework. And the web application (UI) will be developed using the Angular framework. Since both frameworks are google products and since they are tailored to be used together, it is a good combination. The customer information will be directly communicated to the TensorFlow model, while the dashboard users (personnel who control the software) would access the web application UI panel from the Angular driven dashboard.

For customer tracking purposes, we may need a small scaled data base service which will be a Mongo DB service - a document-oriented database.

Fraud detection using Facial and emotions.

Mainly there are two sub-systems in this sub-module.

- Cashier counter application
- Server-side application

Cashier counter application

This application is the face of this sub-module. This application is responsible for,

- Connect with camera.
- Send processed data to the server to further processing.
- Show result to the end user.
- Show old result about this customer.

This application is not sending data to server until it detects face. This process will reduce unnecessary server processing and bandwidth. Once it detects a face it starts recording and recorded video will send to the server as photos stream. These photos are compressed, so they are small in size.

It needs windows PC to run the application. Thus, most of the cashiers have a PC anyway to do their transactions.

Server-side application

This is brain of this application. Responsible for,

- Identify User.
- Detect facial behaviors.
    - Emotions.
    - Expressions.
    - Facial landmarks.

Server accept stream of photos. When stream of photos came to the server side first it identifies the user using cognitive services [1]. Then application process photos and put facial landmarks on the photo stream's faces. For that we **dlib** and **OpenCV** python libraries.

Using those Facial landmarks, we can calculate, emotions and expressions of the user. Using those data with the key points we can predict/ decide how suspicious the person is.

2.1.5 Communication interfaces

This system functions in a LAN of the bank environment. It does not essentially need Wide Area Network (WAN) to function. Since the whole system and the machine learning algorithms are deployed in the local machine, the whole process is done by a single system unit. The communication part is needed after a *high* probability of fraud activity is detected. The user may have setup automatic calls to respective personnel to act against the fraudster, or the user may manually enter personnel to be contacted. Anyways, this scenario needs a proper, reliable communication system. If the LAN fails, a crucial part of the module will fail, hence failing the whole system

Server is always communicating with the cognitive services. So, for that it need internet to communicate. This part is responsible for user identification.

2.1.6 Memory constraints

External memory: Most of the model's functionality will depend on the training data. Training data will be only needed in the training phase. So, in the production environment there will be no huge external memory constraints. Since we would have a web application interface, there will be no need for setting up applications too.

Internal memory: Machine learning model will require a notable amount of internal memory since the processed data from the GPU needed to store for ease analyzing process and needs a considerable memory power. A minimum 8GB RAM will be sufficient for the prediction and presentation purposes.

Cashier counter PC:

- In order to run camera app correctly PC need 8GB RAM
- And 4GB space recommended.

2.1.7 Operations

- User will need a login system to prove his identity to the system.
- User (admin personnel) will need a web portal (dashboard) to manage the machine learning modules.
- When user clicks on facial fraud detection module user able to view current counters and person's facial patterns and emotions in real time.
- When user clicks on facial fraud detection module user able to view current counters and person's history.
- When the user clicks on voice-based fraud detection module icon user able to view the current user's voice analyzed information graph which shows how customer voice suspicious level change over time.
- When the use clicks on the transaction-based fraud detection module icon, the user could see the currently ongoing operation on each and every POS (Point Of Service), ATM (Automatic Teller machine).
- All the operations in this body language component are unattended operations which means that after installing this component it'll run automatically

without any user interactions and this operation will run until the system is shutdown or until CCTV footage are fed into the component.

- If the footage we get is too noisy we can use denoising auto encoders to clear up the footage this can only achieve clarity for some extent only.
- There are no backup operations in this body language analyzing component but most of the CCTV footages are backup by the companies for various security reasons so we can even analyze the footage that is not in real-time.

Cashier counter application

- Connect/ Disconnect camera.
- Start/ Stop detection process.
- Assign/ Merge data to the detected customer.
- See Customer history.

2.1.8 Site adaptation requirements

To gather facial data from cashier counters,

- All the counters that require this component should have digital cameras installed in each cashier counter and system should be able to access these footages.
- Need a capable cashier counter PC in order run the client application.
- Need a centralized server with good internet connection and performance.

Microphones deploying on a cashier point might become an issue. For this issue we are going to use some of tiny microphones available in the market which are hardly noticeable to the customers. With this solution we will able this product's microphone adopts with the current site.

All the sites that require this human body language identification component should have digital CCTV cameras installed in the site and system should be able to access these footage.

Need to have machine that is able to run the system.

Since this application deals with sensitive client information, there should be high security measure taken. Other than that, there are no site-specific requirements for this application.

2.2 Product functions

Login and security

This application's data is confidential. If it gets leaked, there may be unnecessary problems. Due to this, we have to ensure a good security protocol to be followed throughout this system which will only allow the desired personnel to look at the data collected and the information passed.

Transaction module dashboard / portal

The dashboard will show some information that can be used to identify what is going on quickly. Information about the current transaction being analyzed, it's details, percentage of analyze, percentage of being a fraud up to now will be some quick tips. Below the current transaction display, there will be some overall information with graphs and charts which will depict the functionality of the module in the past week / month / year.

Underlying machine learning algorithm

This is the heart of this module. Prediction of the fraudulent transactions is solely done by it. Required data will be gathered from the counters and the teller machines and they will be fed into the algorithm. ML model will predict the fraudulent behaviors of the transaction while learning new patterns and analyzing already learned patterns.

Body Language Component

One of the major functions in body language is analyzing CCTV footage in real time. This part of the system is and internal component users does not need to interact with this component other than to feed data into it data also fed automatically after a secure link is established between the system and the CCTV camera network.

In this component users will also be tracked between cameras so if we start analyzing a user and he went out of fov (Field of vision) of the camera that he is being currently tracked and appeared in another cameras fov then the system will recognize that this is the same user as before and continue with its scanning.

Cashier counter application

Connect/ Disconnect camera

Cashier counter PC allow user to connect and disconnect from cameras that retrieving customer facial data.

Start/ Stop detection process

Cashier can Start or stop the process any given time.

Assign data to the detected customer

If there's new customer, then cashier can assign data to the customer or merge with other customer data.

See customer data history

This functionality allows to see the cashier, when customer came before and what are the old suspicious ratings.

2.3 User characteristics

The typical user will be a bank customer who will be doing a transaction. Basically, this can be any type of adult person since almost all the people use bank account these days. Educated, professional or poorly educated people will be using this system module. But we do not need to make the user interface easily understandable and user friendly since our system will not be directly accessible by these users. Since it is an underlying system of the main transaction system of the bank, typical user will not even notice this system.

Even though the transaction system is used by a typical user, the dashboard of the underlying system will be used be specific bank personnel. They will be normal employees with an elevated literacy level.

Cashier counter application will only be use by cashiers who has training and experience in computer usage.

Web Application/ Dashboard will be use by Management who have experience in computer usage, but we need good UX.

2.4 Constraints

- The system should be modular so the system should work without having all the components, user(s) can buy the components that they think are valuable for their environment and system should give the output based on those components.
- Each cashier counter needs a camera and PC with required specifications.
- Server also need good performance in order to handle concurrent accesses and processing.
- Good connection from client to sever and server to cognitive services.

2.5 Assumptions and dependencies

This application will be a web based one. That will remove most of the dependencies found in a normal application since it is separated from the operating system, and other services.

Assume that one server can handle all the customers in a peak hour.

Assume that fraudsters are not highly trained to hide their body language and emotions.

Assume we have clear analyzable footage from CCTV

2.6 Apportioning of requirements

Machine learning model should be the highest priority task. It should be implemented using TensorFlow.

Then the Data should be fed to the model. After that the model will be trained.

User interface is the least prioritized task. It will be needed for the bank personnel.

specifications of this component. In the 3rd section the functional and non-functional requirements are mentioned in detail. If any major defects are found according to the requirements the testing will be done and defects will be corrected. Application will be implemented by the developers in horizontal manner and no function will be completed at the middle of the development.

Essential requirements of this system are,

- Identify face of a person.
- Identify person by face
- Cashier counter application
- Mark facial landmarks
- Get emotional data from facial landmarks
- Mapping humans into 3D space.
- Identifying anomalies in human behavior.
- Tracking person.
- Background noise reduction.

- Isolating speakers voice.
- Identify voice-based lie detecting rules.
- Collection Transaction information.
- Check the collected data for transaction rules.
- Classify Transactions according to the algorithm.
- Geometrical Mapping face into a 3D space.
- Analyze micro facial expressions

Desirable requirements of this system are,

- Classification of persons according to the level of suspiciousness.
- Learning from previous findings.
- Getting a heat signature map of the person.
- Show in the interface how many rules were passed by a transaction.
- Get person's facial micro-expressions to the calculations.
- Getting a heat signature map of the person's face.

3 SPECIFIC REQUIREMENTS

3.1 External interface requirements

3.1.1 User interfaces

Login Page

Pre-determined personnel credentials are inserted in to the database beforehand. If the user is able to provide the given valid username and password, access will be granted to enter the system.

Cashier counter application

UI for Connect Camera

This UI is allowed user to connect to a camera that already connected to that PC. This is the first step of the application. User need to connect to camera in order to continue.

UI for Start detection

After user connect to a camera. Now user can start detection process or user also can disconnect. When the user starts the detection process. Application will start recording camera out and process that video stream of photos and send them to server to further processing. If there are no person detect in the video application will stop sending data to the server.

Following data will be responses from the server.

UI for when user identified and seems ok state

After user start detection process, now user can stop process or let system stay like that.

When detection is in progress and when a person came in front of the camera. It will predict whether this person is suspicious or not and try to identify the person using previous data. This UI shows when person is identified and seems OK.

UI for User not identified and Option for add or Merge

If person is not identified, then interface will give an option to add this user to system or merge with another user.

When person is suspicious

This will display when person seems suspicious.

Body Language Dashboard

When the customers enter the site they will be scanned for abnormal body language by clicking on the body language tab user(s) of the system can see for what abnormal behaviors they were detected for and the user can decide whether it is disability or an actual fraudster.

In the overview page user(s) can get an idea about the whole situation of the site and take necessary precautions accordingly.

Voice Analyzing Dashboard.

User allows to view more information about voice analyed information by clicking the voice-based fraud detection icon in the dashboard. In this specific interface user able check how the customer's voice based suspicious level changed over the time. Other than viewing analyzed details user cannot perform any other action in this interface.

Transaction Analyzing Dashboard

After logging into the system, user can see some of the statistics of the transaction-based fraud detection system. Most importantly, the currently being analyzed transaction details will be shown in the top of the page. Below that, user can see some statistics of the predicted activities. Frauds detected, non-frauds detected counts will be shown and can be sorted according to user's desire.

Alert Popup

This is the most important part of the module. Alerts of this kind will be shown in the pre-selected personnel devices. The transaction details can be seen via the alert box by clicking more details button. The Contacts button will navigate the user to a screen

which can be used to contact personnel which he desires. All the contact details can be pre-configured by the developers.

3.1.2 Hardware interfaces

Camera to get facial data

We need to digital camera with good quality in order to identify person's face and expressions.

Windows PC

Need a Windows PC to connect the camera and send processed data to servers.

- Quad Core 6th Gen Processor
- 8GB RAM
- 4GB space
- Good connection with server

Body Language Module

The hardware aspects that this component deals with are CCTV cameras and the local servers which the components reside in.

The server will need at least 16GB of RAM and nVIDIA GTX 1080Ti for analyzing videos in real-time. The processor should not bottleneck these other components as for the memory since there is no need of storing the data unless the client asks for it storage space can vary.

Transaction Module

As stated above, this module does not have any specific hardware requirements. But it needs a functioning system unit at least with a core i5 central processor, 4gb ram for the predicting services of the model. Storage devices will not be a major requirement since the trained model is deployed in the client machine. (data sets are only needed at the training phase).

3.1.3 Software interfaces

TensorFlow framework will be used for training the machine learning module. After the training phase it will get the data stream from bank data and predict the probability of frauds.

For the admin personnel of the bank, we will be implementing a web application using Angular which will have a dashboard for the who system. All the modules of the system could be accessed by the Angular based web application.

Since both the frameworks (TensorFlow and Angular) are node package-based java script frameworks, it will be easier to communicate and handle within the software applications.

There will be WPF/ Windows Forms application to capture user data from camera and monitor the Customer's data.

3.1.4 Communication interfaces

Wide Area Network (Internet) will not be a requirement for this system since we will be using the machine learning models for all the basic work. Because of that all the functionalities can be done in the local machines of the Bank premises. After the application is deployed to the local machine, only LAN (Local Area Network) connections will be needed for the system functionality.

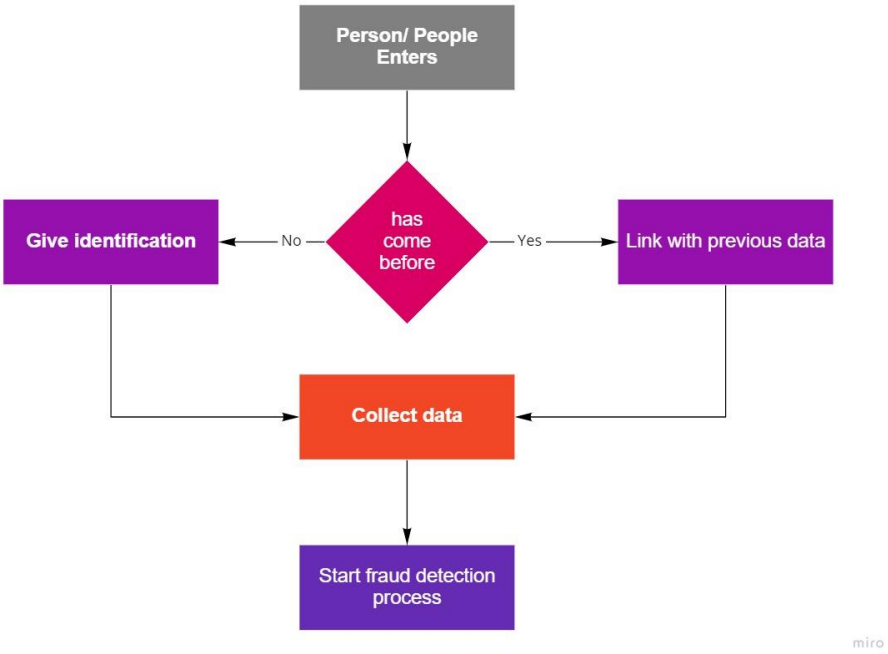
After a possible fraud is detected, the application will need the ability to send alerts to required personnel. This function will need communication mediums. A locally connected network is sufficient for this.

Server is always communicating with the cognitive services. So, for that it need internet to communicate.

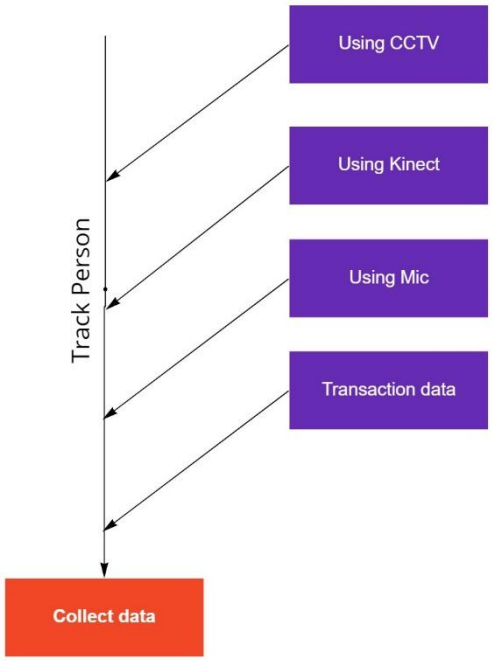
3.2 Architectural Design

3.2.1 High level Architectural Design

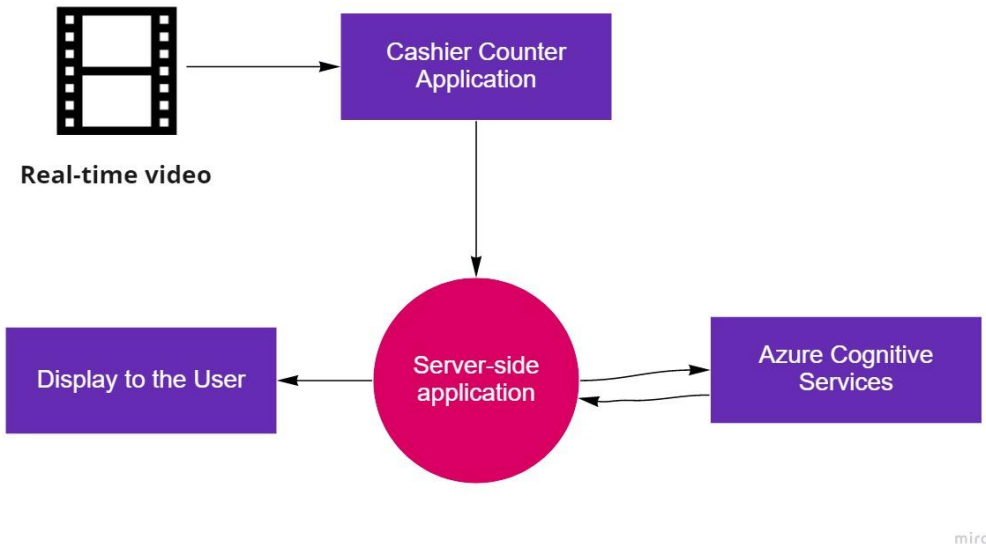
When a person (customer) comes inside the bank premises, our system will start it's functions. Below mentioned decision making will be done to detect whether the customer is previously known or not to the system.



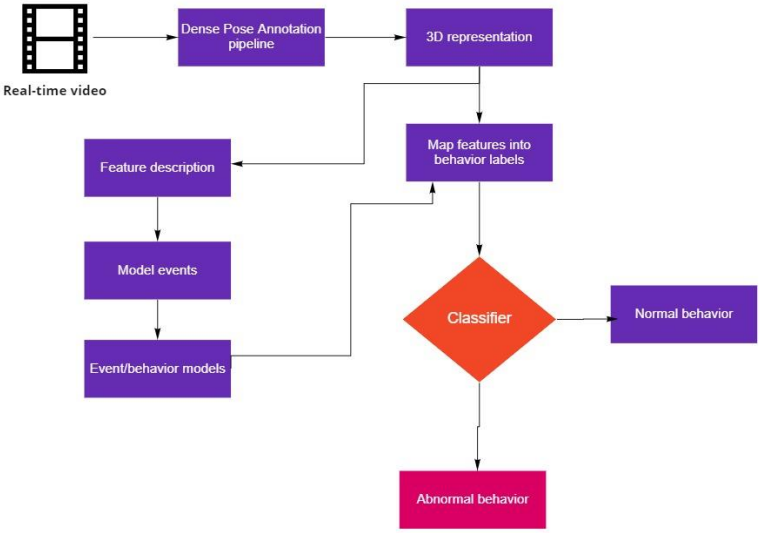
The data collection for the machine learning model will happen in the below communication ways.



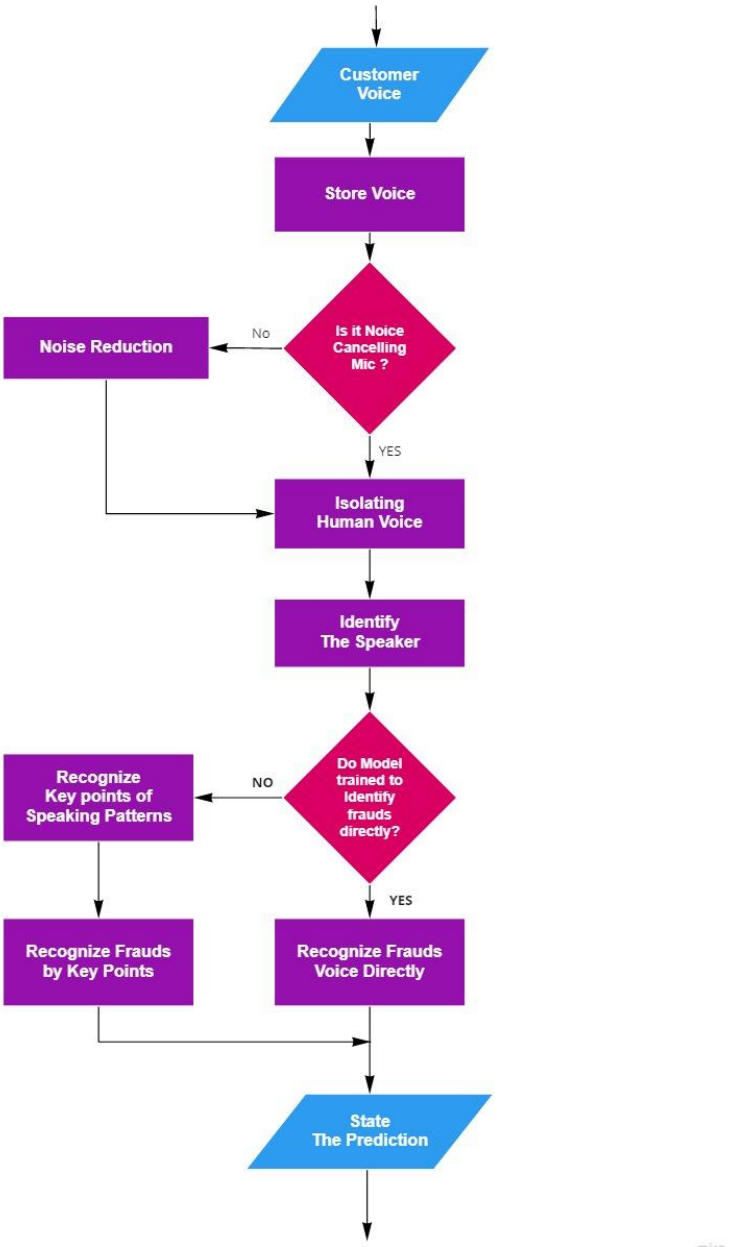
This is how cahier counter application connects to server and server doing this its communications.



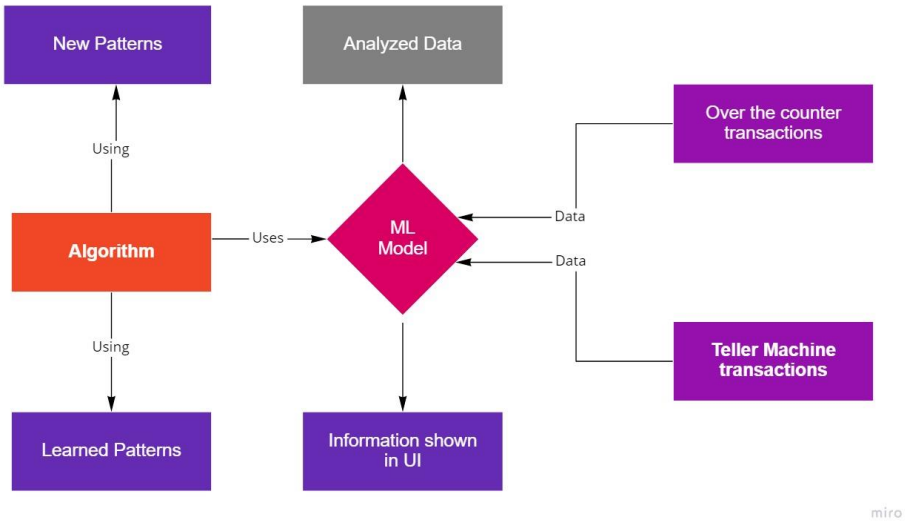
The body movements-based fraud detection module will function according to below high-level diagram.



The voice-based fraud detection module will have the below workflow in its core.



Transaction based fraud detection module will use the below communication model.



3.2.2 Hardware and software requirements with justification

Basic hardware requirement is to have a functional local machine. It will need a medium core i5 processor and a 4GB ram. That is because after training the model, we will not need much processing power to predict the results. But to train the model, we might need powerful machines.

Angular, TensorFlow, MongoDB stack will be used for the software requirement. TensorFlow is a easy to use, popular machine learning framework which can be used in node packages. Since of that, this stack will be easy to use unlike other python based frameworks.

3.2.3 Risk Mitigation Plan with alternative solution identification

In any plan, there might be places where it can all go wrong. Some places we did not think of before. Even though the best type of planning was done, this happens inevitably. There are many other alternatives in case of these scenarios. Other technology stacks like React, Flask, SQL Server will be potential plans. Other UI arrangements could also be discussed to use instead of the dashboard method used in here. Setup of the hardware devices could also be adjusted according to the intention of developers.

We can also reduce the single point of failure risk by not only giving the output based on this component but also combining it with all the other components in the system we can reduce the risk of single of point of failure.

By analyzing past projects and researches we can identify what went wrong and what are the best/optimal algorithms to use for each of the components.

If the tracking of the person turns out be not as optimal for the solution, we proposed we can create a temporary profile for those who enters the site and can update their risk factor in those profiles of the person.

3.2.4 Cost Benefit Analysis for the proposed solution

There will be costs for hardware devices which is needed to identify customers and their various expressions. But this hardware will be crucial for the research because they are a must for this research. So, the cost of them is negligible compared to the benefit we get.

There are lot of cost benefits of using an automated system to detect the frauds,

Since this system will learn from its' past mistakes this after sometime this will very adaptive to the environment that this is deployed in and since this is an automated process it'll run 24/7 regardless of any interference.

The human error will be minimum and not susceptible to bribes there will be somewhat initial cost if the site does not have an already working CCTV camera system but it'll be more cost efficient that hiring agents to watch over the footage.

Can connect between multiple sites if there is a WAN connection between sites so we can communicate between them to identify large scale frauds.

3.3 Performance requirements

Memory Allocation

A small disk space will be sufficient for the application since the machine learning model does not acquire a large space in the hard disk. Most of the data is needed for the training phase only. But if the user do want to save the data they can have addition storage space in the system.Not for the deployment phase. So, after training the model and deploying the application in the localhost of the bank, only a powerful processing unit and a RAM will be needed. Approximately, 1TB of space, 16GB of RAM and a

GPU with high capacity nVIDIA gtx 1080Ti 6GB of VRAM should enough to have the real-time processing done on site.

Response Time

The system should have quick response time since if the fraudster do get away with the fraudulent activities while the system is still processing the last person that was in the counter then it would be of no use.

Workload

The number of counters and the teller machines (all the point of services which have the ability to do transactions) plays the major role here. According to the number of transactions and the system's ability to keep up with them, a peak workload should be defined.

Scalability

The workload scalability might not vary frequently since this is not a publicly open service through internet. This service is only used at a given bank premises. But, when the bank customers get to increase, that should be taken into account. This information can be observed from the bank past data.

Cashier counter PC

In order to work WPF/ Windows Forms application smoothly we recommend,

- Quad Core 6th Gen Processor
- 8GB RAM
- 4GB space
- Good connection with server

Quad Core 6th Gen Processor

When user starts detection. Cashier counter application starts to detect faces. If it not detects any face it will not send data to the server. This face detection process needs some processing power.

And if it detects any face then application starts to video and break that video to photos stream. For that it needs more processing power.

8GB RAM

When application break the video to photos stream it need RAM to convert that video to photos. Until application send those data to server it needs to hold those data. That's why we need 8GB of RAM.

4GB Space

These are purely for caching purposes. Maybe we need to save photos stream to PC first before sending them to server.

Good connection with server

As stated in document this application has two tiers. In order client appl to work correct and smoothly client app need to send and receive the responses quickly. For that it needs good connection with server.

In server-side

Good internet connection also required to connect with cognitive services.

3.4 Design constraints

Using the industry best practices may make the experience more pleasant for the users. Navigation, UI designs is important to be looked at. Because the bank personnel will not be IT professionals, this machine learning model-based solution should be introduced as easy to use through a user-friendly web application. So, this application should be developed as if any person can use it irrelevant of their literacy levels.

3.5 Software system attributes

3.5.1 Reliability

This module should be predicting the fraud possibilities at least at a rate of 80%. If it becomes lower than that, the commitment of this module to the system will be very low. Because from all the four modules, most reliable modules will be giving a higher percentage to the decision of fraud detection. For a competitive product, this should

be in a higher level of reliability. This could be measured by confusion matrices and other techniques, by predicting and later resolving whether the predictions were correct or wrong.

3.5.2 Availability

This system's availability mostly relies on the LAN performance of the bank premises. If the LAN is available, all the information streams are open and the system will function as usual. There are no dependencies outside the premises i.e. internet connection.

Since the local host will have the minimum performance skills required, there will be no delay of analyzing the transactions real time.

3.5.3 Security

Security is a major concern in this context of the application. Banking applications are the most vulnerable for attacks. But since we do not expose our services to the WAN, there is no vulnerabilities available to be penetrated. Only security concerns are the normal physical attacks. Other than that, LAN's cannot be penetrated through outside parties, giving the application whole lot of security.

If an outside person gains access to the local host which our application is deployed, he still should bypass our login system to access the sensitive information. Other than that, there is no way to access bank users' personal sensitive information through our application.

3.5.4 Maintainability

The machine learning model is the only components that changes frequently and automatically. So, there is nothing programmers can do. The model will self-learn patterns while the transaction information is fed through real time day to day transactions.

3.6 Other requirements

There are no other specific requirements to be mentioned.

4 SUPPORTING INFORMATION

4.1 Appendices

4.2 References

5 REFERENCES

[1] Microsoft, "Microsoft Azure Face API," Microsoft, [Online]. Available: https://azure.microsoft.com/en-us/services/cognitive-services/face/. [Accessed 2019].

[2] M. Tenney, "Microsoft Kinect – Hardware," 2012. [Online]. Available: http://gmv.cast.uark.edu/scanning/hardware/microsoft-kinect-resourceshardware/.

[3] O. Kinect, "Open Kinect," 2012. [Online]. Available: https://openkinect.org/.

[4] I. M. a. O. Lan, "Looking to Listen: Audio-Visual Speech Separation," 11 April 2018. [Online]. Available: https://ai.googleblog.com/2018/04/looking-to-listen-audio-visual-speech.html.

[5] En.wikipedia.org, "Cocktail party effect," [Online]. Available: https://en.wikipedia.org/wiki/Cocktail_party_effect. [Accessed 8 March 2019].

[6] Wikipedia, "Convolutional neural network," [Online]. Available: https://en.wikipedia.org/wiki/Convolutional_neural_network.

[7] Wikipedia, "Kinect," [Online]. Available: https://en.wikipedia.org/wiki/Kinect.

[8] M. Rubinstein, "Looking to Listen: Stand-up," 11 April 2018. [Online]. Available: https://www.youtube.com/watch?v=NzZDnRni-8A. [Accessed 8 March 2019].

[9] En.wikipedia.org, "Machine learning," [Online]. Available: https://en.wikipedia.org/wiki/Machine_learning. [Accessed 8 March 2019].

[10] L. F. L. W. M. F. J. G. F. D. S. P. N. L. D. V. Z. John S. Garofolo, "TIMIT Acoustic-Phonetic Continuous Speech Corpus," [Online]. Available: https://catalog.ldc.upenn.edu/LDC93S1. [Accessed 8 March 2018].

[11] M. I. R. lab, "MIR-1K Dataset," [Online]. Available: https://sites.google.com/site/unvoicedsoundseparation/mir-1k.

[12] C.-L. H. a. P. J.-S. R. Jang, "Sound Demos for Unvoiced Singing Voice Separation," [Online]. Available: https://sites.google.com/site/unvoicedsoundseparation/sounddemosforjournal. [Accessed 8 March 2019].

[13] M. J. S. Andrew Briggs, "An Introduction to Markov Modelling for Economic Evaluation," May 1998. [Online]. Available: https://www.researchgate.net/publication/13118783_An_Introduction_to_Markov_Modelling_for_Economic_Evaluation.

[14] GitHub, "Speaker Recoganition," [Online]. Available: https://github.com/topics/speaker-recognition. [Accessed 8 March 2018].

[15] W. Seshika Fernando Senior Technical Lead, "Fraud Detection and Prevention: A Data Analytics Approach," [Online]. Available: https://github.com/topics/speaker-recognition. [Accessed 8 March 2018].

[16] E. Wikipedia, "Polygraph," [Online]. Available: https://en.wikipedia.org/wiki/Polygraph. [Accessed 8 3 2019].

[17] X.-V. Team, "X13-VSA Voice Lie Detector," [Online]. Available: https://lie-detection.com/. [Accessed 8 3 2019].

[18] Altexsoft, "Legacy System Modernization: How to Transform the Enterprise for Digital Future," [Online]. Available:

https://www.altexsoft.com/whitepapers/legacy-system-modernization-how-to-transform-the-enterprise-for-digital-future/. [Accessed 8 3 2019].

[19] Oxford University Press, "Oxford Dictionary," Oxford University Press, 2019. [Online]. Available: https://en.oxforddictionaries.com/definition/fraud.

[20] Cambridge University Press, "Cambridge Dictionary," Cambridge University Press, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/fraud. [Accessed 2019].

[21] Traci Brown Inc, "Body Language Trainer," Traci Brown Inc, [Online]. Available: https://www.bodylanguagetrainer.com/the-truth-about-lies-body-language-and-fraud-detection/. [Accessed 2018].

[22] Google, "Google Cloud Vision," Google, [Online]. Available: https://cloud.google.com/vision/. [Accessed 2019].

[23] R. A. N. N. &. K. I. Guler, "DensePose: Dense Human Pose Estimation in the Wild," IEEE/CVF Conference on Computer Vision and Pattern Recognition, [Online]. Available: https://ieeexplore.ieee.org/document/8578860. [Accessed 2018].

[24] S. Khan, O. Javed, Z. Rasheed and M. Shah, "Human tracking in multiple cameras. Proceedings Eighth IEEE International Conference on Computer Vision," ICCV, 2001. [Online]. Available: https://ieeexplore.ieee.org/document/937537.

[25] S. Kumar, P. S. K., Saroj, P. K., Tripathi and R. C., "Multiple Cameras Using Real Time Object Tracking for Surveillance and Security System," 3rd International Conference on Emerging Trends in Engineering and Technology, 2010. [Online]. Available: https://ieeexplore.ieee.org/document/5698322.

[26] K. J. Tod, "Detecting Deception: Speech and Voice as a Lie Detector," 6 7 2018. [Online]. Available: https://www.forensicstrategic.com/blog/detecting-deception-speech-and-voice-as-a-lie-detector. [Accessed 8 3 2019].

[27] N. Babich, "How to Detect Lies: Speech," 3 2 2016. [Online]. Available: https://medium.com/@101/how-to-detect-lies-speech-346353a8d36c. [Accessed 8 3 2019].

[28] .. H. Q. Y. X. X. W. O., "A Detection System For Human Abnormal Behavior," 2005.

[29] M. I. a. K. W. O. P. Popoola, "Video-Based Abnormal Human Behavior," 2011.

[30] R. A. N. N. Guler, "DensePose: Dense Human Pose Estimation In The Wild," 2018.

[31] G.T.S, "https://medium.com/mlreview/choosing-components-for-personal-deep-learning-machine-56bae813e34a,"," 2017. [Online].

[32] Microsoft, "Microsoft Azure Face API," Microsoft, [Online]. Available: https://azure.microsoft.com/en-us/services/cognitive-services/face/.