Comprehensive Design and Analysis Project

Design Document

IT16158764 – Basnayake M.C.S.B

Fraud Detection Based on Facial Patterns

Bachelor of Science (Honors) in Information Technology

Department of Software Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

May 2019

DECLARATION, COPYRIGHT STATEMENT AND THE STATEMENT OF THE SUPERVISOR

We declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student Id	Signature
B.M.C.S. Basnayake	IT16158764	

The supervisor/s should certify the proposal report with the following declaration.

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

…….. ……..

Signature Date

CONTENTS

FIGURE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

The purpose of the **Design Document** (DD) is to present a detailed description of the **Fraud Detection System**'s detect using **Facial Behavioral Patterns**. This document is including followings,

- Functional Requirements
- Non-Functional Requirements
- Interfaces (User, Hardware, Software)
- Architectural Design
- Constraints & etc.

The Design Document is the basic document to refer when developing the system and help to understand how developers are going to develop the proposed system.

1.2 Scope

This document is tending to cover a sub-module of **Fraud Detection System**'s **Facial Behavioral Patterns** that include,

- High level information
- What this sub module supposed to do
- How will this sub-module contribute to system?
- Data communication methods
- Machine learning aspects of this sub-module

1.3 Definitions, Acronyms, and Abbreviations

ML	Machine Learning
LAN	Local Area Network
WAN	Wide Area Network
UX	User Experience

PC	Personal Computer
WPF	Windows Presentation Foundation

1.4 Overview

Fraud Detection System based on main four main components. Fraud detection using,

- Facial Patterns and emotions Recognition
- Voice Patterns
- Behavioral Patterns
- Transaction Patterns

In here we focused on **Fraud detection using Facial and emotions**.

When a customer comes to a cashier point, system will can run face recognition and detect,

- Emotions
- Expressions
- Eye movement

Using these data, we can predict whether person is suspicious or not.

2 OVERALL DESCRIPTIONS

As stated in 1.4 there are four main components and focus is **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. 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.

Finally, those ratings though our ML model and it gave a final score and confidence rate as the response.

2.1 Product perspective

There are some projects still in research level but no clear product for Fraud detection using Facial and emotions. Here are some examples.

Lie Detection based on Human facial gestures

This system identifies lies using facial gestures. Mostly it uses expression of the human face. [1]

Face Reading Technology for Lie Detection

This system also identifies lies using facial gestures. But this system uses thermal camera as well. [2]

These systems only detect lies and it only identifies using face. But our system has four components and result will be a combination of those.

2.1.1 System interfaces

- Windows
- Android

2.1.2 User interfaces

Following figures are some of the main interface sketches.

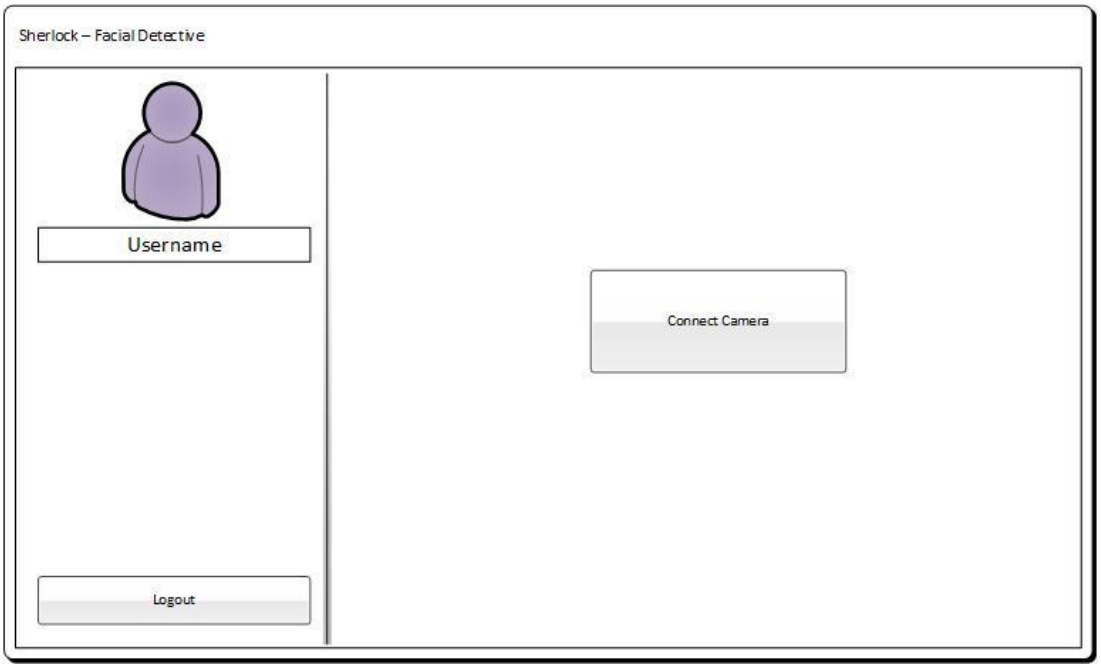

Figure 1: UI for connect camera

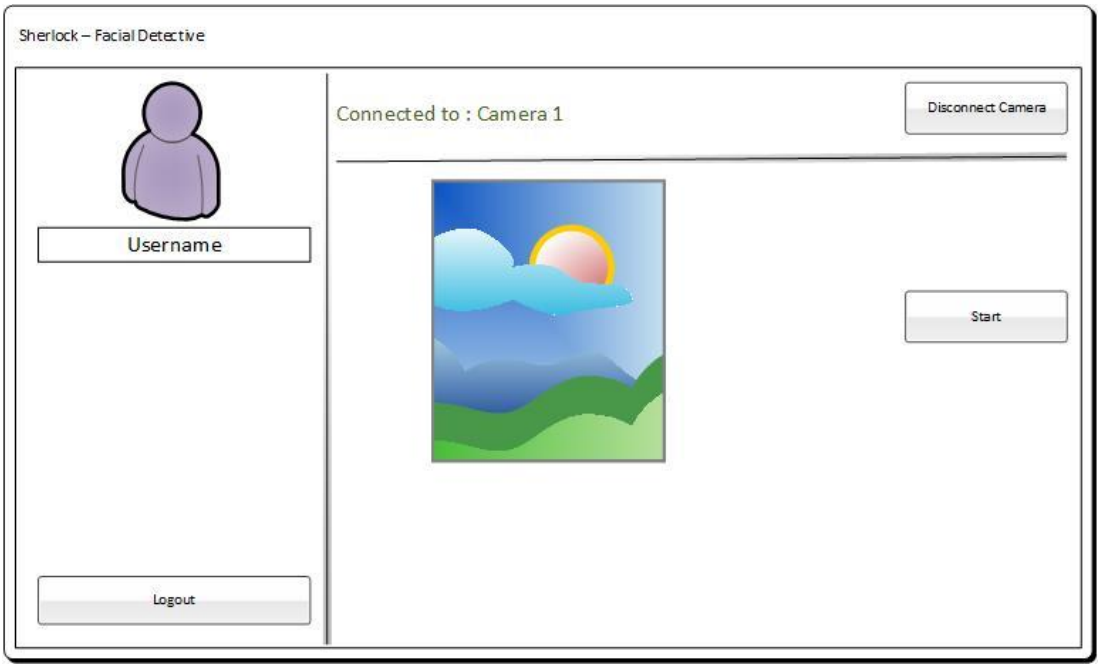

Figure 2: UI for Start detection

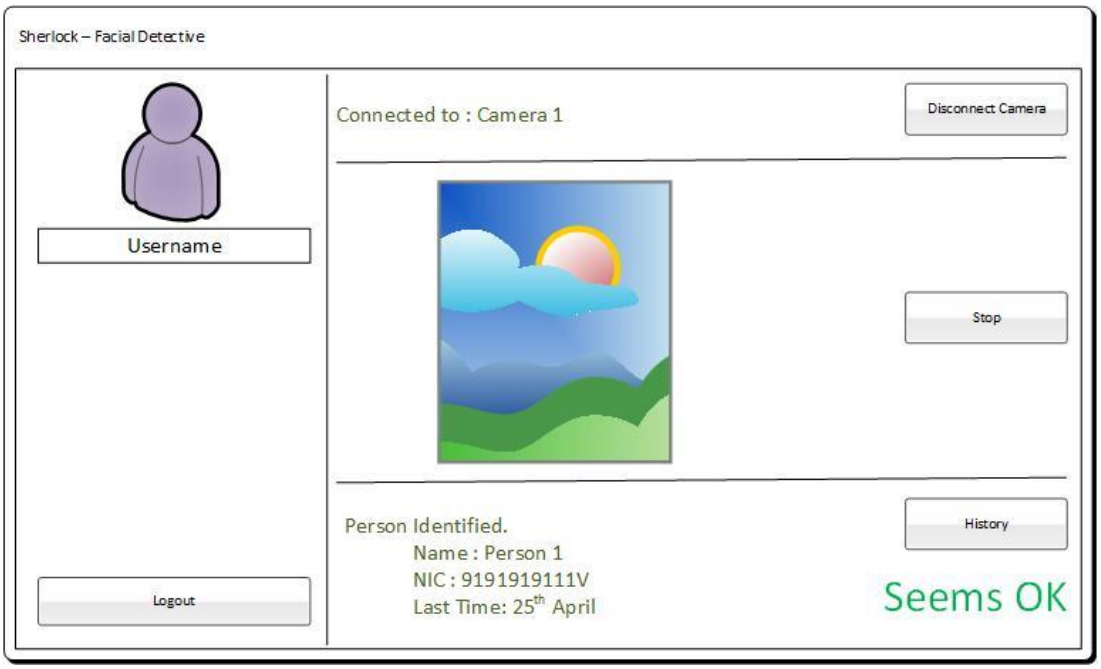

Figure 3: UI for when user identified and seems ok state

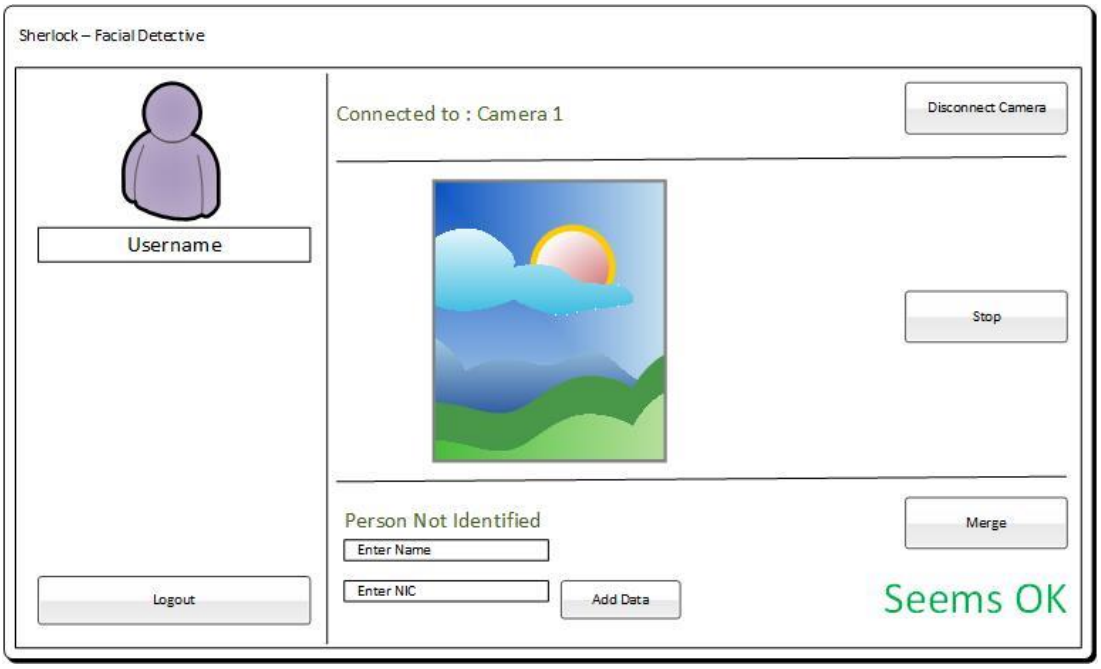

Figure 4: UI for User not identified and Option for add or Merge

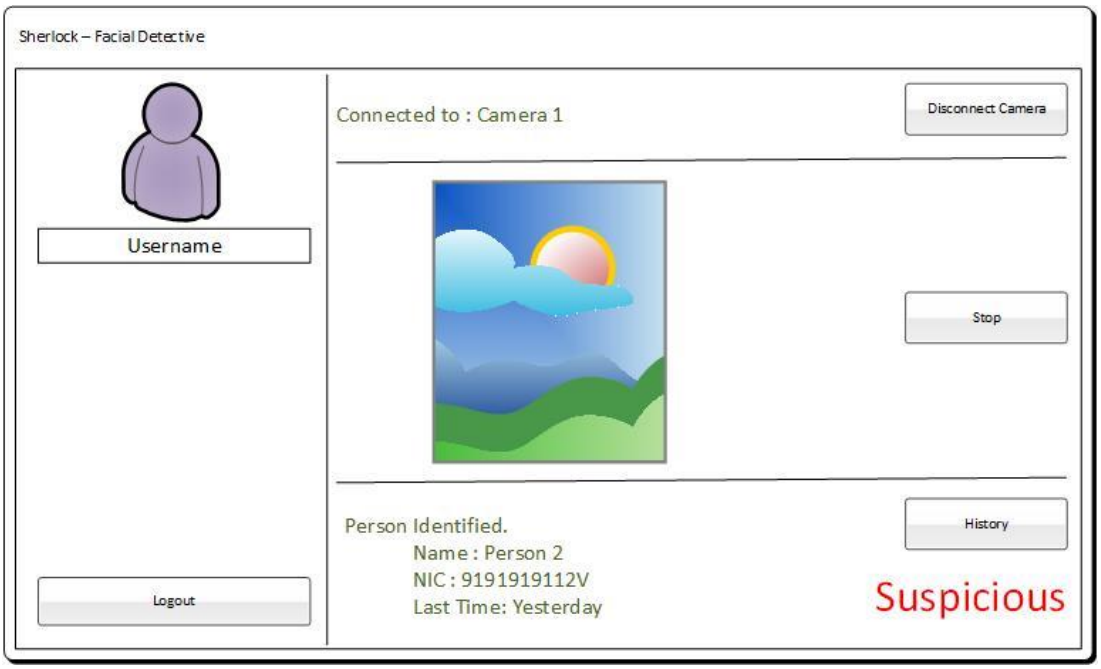

Figure 5: When person is suspicious

2.1.3 Hardware interfaces

- Camera to get facial data.
- Windows PC

2.1.4 Software interfaces

- There will be WPF/ Windows Forms application to capture user data from camera and monitor.
- Using a web application user can monitor the system.

2.1.5 Communication interfaces

- LAN or WAN.
- Cable for connect with Camera and cashier counter Computer.

2.1.6 Memory constraints

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

2.1.7 Operations

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

2.1.8 Site adaptation requirements

- 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.

2.2 Product functions

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

- Cashier counter PC application - Cashiers who has training and experience in computer usage.
- Web Application/ Dashboard – Management who have experience in computer usage, but we need good UX.

2.4 Constraints

- 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

- Assume that one server can handle all the customers in a peak hour.
- Assume that fraudsters are not highly trained to hide their expressions and emotions.
- WPF and Windows Form depends on windows OS.
- Future versions will support Linux.

2.6 Apportioning of requirements

The requirements mentioned in the 1st and 2nd section of the document are primary 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 component are,

- Identify face of a person.

- Identify person by face
- Cashier counter application
- Mark facial landmarks
- Get emotional data from facial landmarks

Desirable requirements of this component are,

- Classification of persons according to the level of suspiciousness.
- Learning from previous findings.
- Get micro-expressions to the calculations
- Getting a heat signature map of the person’s face.

There are no optional requirements for this component at the time this DD was created.

3 SPECIFIC REQUIREMENTS

3.1 External interface requirements

3.1.1 User interfaces

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.

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.

3.1.3 Software interfaces

WPF/ Windows Forms application to capture user data from camera

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

Using a web application user can monitor the system

Web application for more functionality.

3.1.4 Communication interfaces

LAN or WAN

- In order to connect with the server.
    - Cashier counter application need to connect to the server. For that we need LAN or WAN.

Internet

- To get Cognitive services data.
    - Server is always communicating with the cognitive services. So, for that it need internet to communicate.

Cable for connect with Camera and cashier counter Computer.

- In order to get data that comes from camera.

3.2 Architectural Design

3.2.1 High level Architectural Design

Basically, this is the process that happening in client side.

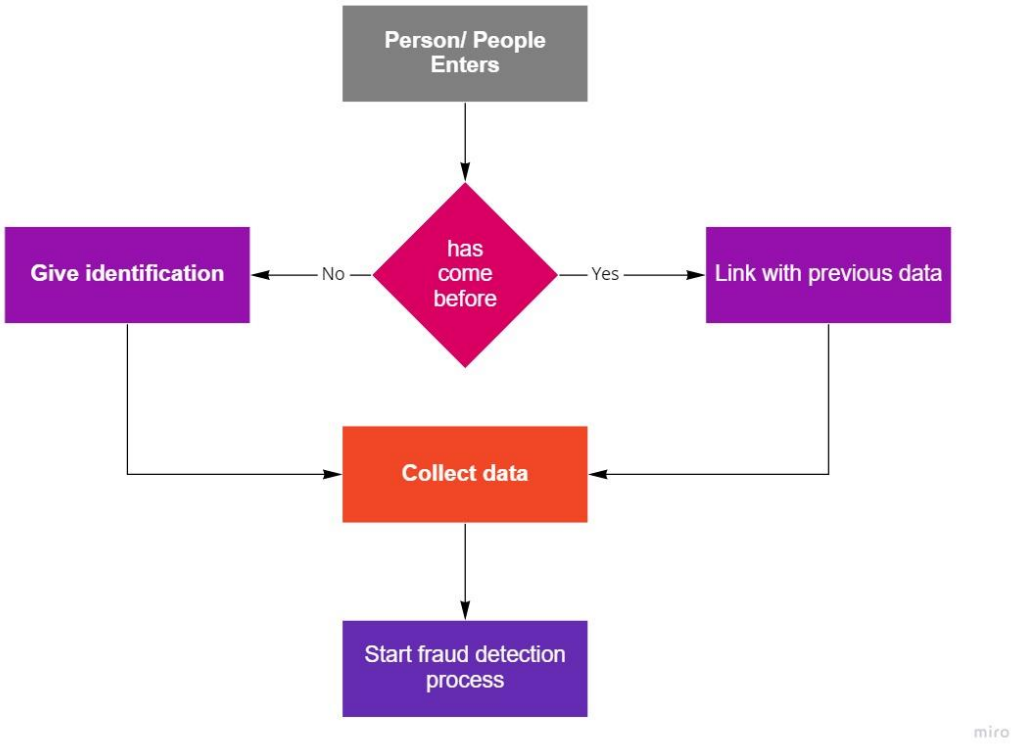

Figure 6: Cashier counter application process

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

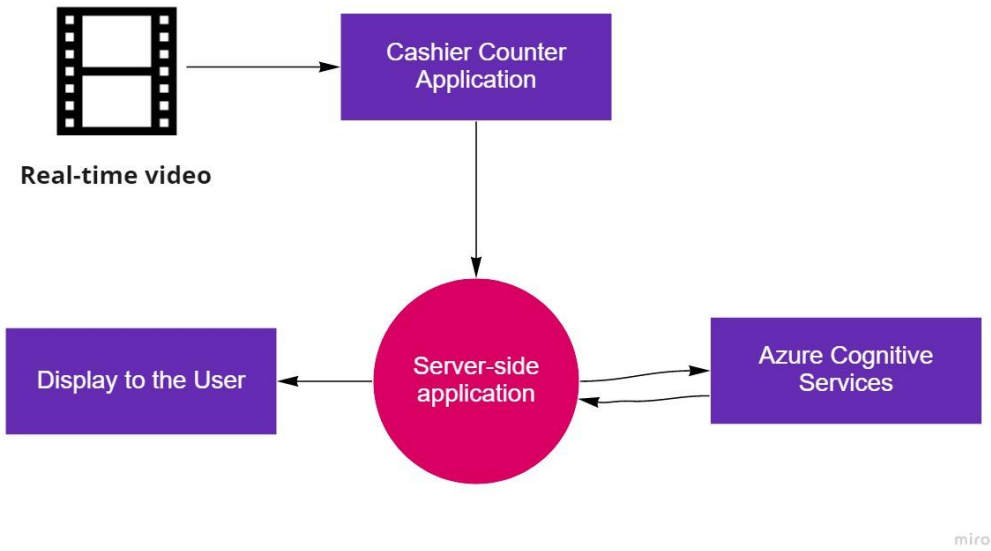

Figure 7: Server communication design

3.2.2 Hardware and software requirements with justification

Hardware Requirements

- Cashier Counter Cameras
    - One of the main hardware requirements for this component is Cashier counter cameras since without the data we cannot make use of this component, only with the data that has been provided through the cameras we can run the algorithm that will identify fraudsters.
- Cashier counter PC
    - These requirements due to image processing and other processes ground in the background to detection. And PC need at least,
        - Quad Core 6th Gen Processor
        - 8GB RAM

        - 4GB space
        - Good connection with server
    - Other wise the process will be laggy and not a good experience to the end user.

Software Requirements

- WPF application for initial processing.
- Cognitive services for facial identification process.

3.2.3 Risk Mitigation Plan with alternative solution identification

We 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 profiles for those who came to cahier counter and can update their risk factor in those profiles of the person.

3.2.4 Cost Benefit Analysis for the proposed solution

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

- Can connect between multiple sites if there is a WAN connection between sites so we can communicate between them to identify large scale frauds.
- Since system is predicting before frauds happen. It benefits to the company that this system is using.

3.3 Performance requirements

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.

Checking the application on all possible devices should be done.

3.5 Software system attributes

3.5.1 Reliability

This module should be predicting the fraud possibilities in higher rates.

With updates and learning processes we can make more reliable.

3.5.2 Availability

This system's availability mostly relies on the LAN and internet performance of the bank premises. If the connection is available, all the information streams are open, and the system will function as usual.

Only when updating the system, service will unavailable. But most of the time its available. Updating system at nighttime will minimize this issue.

3.5.3 Security

Most of the sensitive data we save in server-side application. So, security will be good with that. And mostly network security depend on how good the banking environment's network security is.

3.5.4 Maintainability

With updates we can maintain cahier counter PC application's performance and security.

3.6 Other requirements

- Use of server-side application. So, servers and internet connection will be required.
- Azure Cognitive Services [3], for that we need Azure subscription.
    - In order to identify and get an idea about emotions and other facial points. This system uses cognitive services. These are already built and matured services no need for rebuild.

4 REFERENCES

[1] P. T. Upadhyay and D. Roy, "csjournals," [Online]. Available: http://csjournals.com/IJCSC/PDF7-1/23.%20Tejpal.pdf.

[2] H. Ugail, M. H. Yap and B. Rajoub, "Face Reading Technology for Lie," [Online]. Available: https://www.cl.cam.ac.uk/research/security/seminars/archive/slides/2011-10-25.pdf.

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