FRAUD DETECTION BASED ON HUMAN BEHAVIORAL PATTERNS

19-020

Project Proposal Report

B.M.C.S. Basnayake

U.P.A.S.D. Amarasinghe

N.P. Seneviratne

Y.C. Tittagalla

B.Sc. (Hons) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

March 2019

FRAUD DETECTION BASED ON HUMAN BEHAVIORAL PATTERNS

19-020

Project Proposal Report

B.Sc. (Hons) Degree in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

March 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	
U.P.A.S.D. Amarasinghe	IT16160330	
N.P. Seneviratne	IT16120280	
Y.C. Tittagalla	IT16129740	

Table 1: Team members and details

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

ABSTRACT

Fraud detection is a must in the modern world. With the exponential growth of the economy, frauds have become a major problem, especially in the banking industry.

Most of the time, these frauds are detected by bank officers. They should be always vigilant about their customers and transactions. That is the way a traditional bank would do to identify a fraud. But how reliable is this system? What is more reliable, a machine or a set of humans?

Obviously, a machine is fast, accurate and efficient. Specially with the evolution of Machine Learning algorithms, machines have become more and more intelligent. So, in this research, we would introduce a system, that would detect the behaviors of humans and transactions, analyses them, and tell whether the transaction is a fraud or not. This system will greatly improve the security and the reliability of a banking system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABA	– American Bankers Association
GDP	– Gross Domestic Product
CNN	– Convolutional Neural Network.
FOV	– Field of View
CCTV	– Closed-Circuit Television
SLIIT	– Sri Lanka Institute of Information Technology
ML	– Machine Learning
VSA	– Voice Stress Analyze

1 INTRODUCTION

1.1 What is a Fraud?

According to the world-renowned Oxford dictionary, ‘Fraud’ is described as below.

> *“Wrongful or criminal deception intended to result in financial or personal gain [1]”*

Cambridge dictionary describes it like this.

> *“The crime of getting money by deceiving people [2]”*

All these definitions suggest us that fraud is a crime, a wrong thing, which is done to gain financial gains. Criminal activities are a normal thing in the society. But when it is done, usually, the criminal gets a set of feelings due to the nature of humans. Fear, guilt, anxiety is a few of them. These emotions are exhibited through that person’s body language. Looking at this guy’s facial expressions, body movements, voice patterns even we can say that this person is not normal and there is something wrong here.

Body language expert Traci Brown says that lying takes a lot of energy. That is why we can rely on body language to detect a liar. A liar must think about what they are going to say next. And while doing this, they judge how the other person examines them. What normal people do on autopilot cannot be done by a fraudster. He needs to think a lot [3].

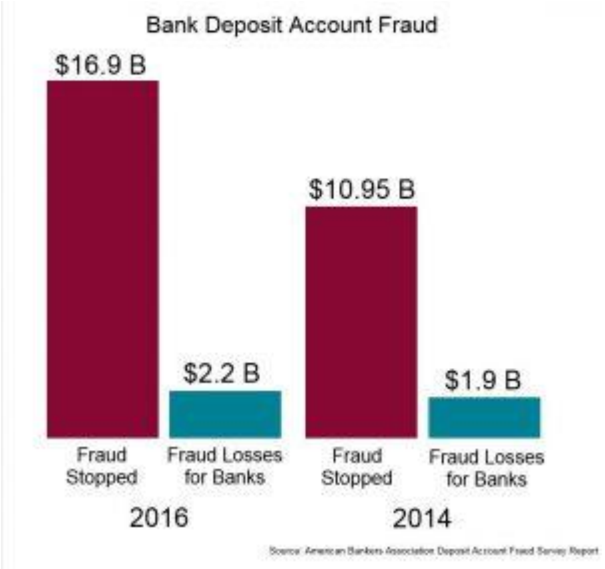
1.2 Our Solution

An artificial intelligent system which can analyze any given scenario and predict frauds before they happen. It uses four modules to decide whether the given scenario is a fraud or not. This includes facial, behavioral, vocal and transaction patterns.

Each module will give a score for the scenario based on its intelligence. Finally, the whole system will use all four modules' scores to give a probability value of the given scenario being a fraud.

Even though this system is mainly targeted on banking systems, the same logic and intelligence can be expanded into any other domain with minimal changes.

Losses due to fraud in the banking industry rose to $2.2 billion in 2016 according to the latest American Bankers Association (ABA) Deposit Account Fraud Survey Report. 35% of these frauds are from cheque based.



Source: American Bankers Association Deposit Account Fraud Survey Report

Figure 1: Bank Deposit Account Frauds

Below is a quotation from **James Chessen**, executive vice president of ABA's Center for Payments and Cybersecurity.

> *"Fraud prevention never stops, banks are constantly monitoring for patterns and trends and quickly evolving their techniques to stay a step ahead of fraudsters. Fraud moves like water trying to find cracks in the system"*

This statement clearly suggests that fraud prevention still must go a long way and it needs more than the intelligence of humans. So artificial intelligent approach is a must for the fraud prevention domain.

The estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars. Disguising the illegal origins of money is becoming a common thing in the society as illegal arms sales, drug trafficking, smuggling rates are going higher.

1.2.1 The rule-based approach

Fraudulent activities in finance can be detected by looking at on-surface and evident signals. Unusually, large transactions or the ones that happen in atypical locations obviously deserve additional verification. Purely rule-based systems entail using algorithms that perform several fraud detection scenarios, manually written by fraud analysts. Today, legacy systems apply about 300 different rules on average to approve a transaction. That's why rule-based systems remain too straightforward. They require adding/adjusting scenarios manually and can hardly detect implicit correlations. On top of that, rule-based systems often use software that can hardly process the real-time data streams that are critical for the digital space. [4]

1.2.2 ML-based fraud detection

However, there are also subtle and hidden events in user behavior that may not be evident, but still signal possible fraud. Machine learning allows for creating algorithms that process large datasets with many variables and help find these hidden correlations between user behavior and the likelihood of fraudulent actions. Another strength of machine learning system compared to rule-based ones is faster data processing and less manual work. For example, smart algorithms fit well with behavior analytics for helping reduce the number of verification steps.

1.3 Background & Literature survey

1.3.1 Facial behavior and patterns

In facial behavior and pattern, we are trying to gather data like,

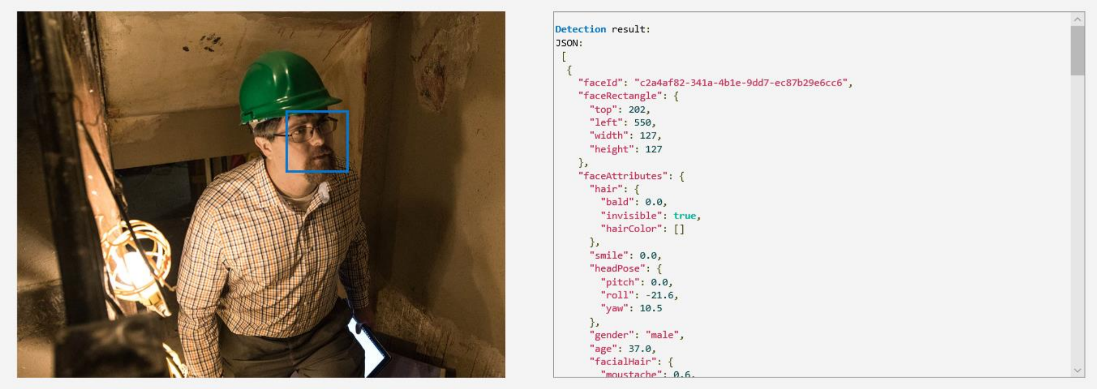
- Emotions.
- Expressions and Micro-Expressions. (Facial Land marks)
- Eye movement.

1.3.1.1 Microsoft Cognitive Services: Vision API, Face

The Azure Face API is a cognitive service that provides algorithms for detecting, recognizing, and analyzing human faces in images. The ability to process human face information is important in many different software scenarios, such as security, natural user interface, image content analysis and management, mobile apps, and robotics [5].

The Face API provides several different functions,

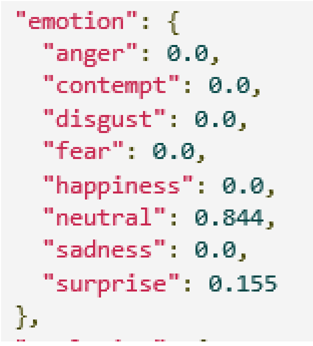
- Detect and compare human faces
- Organize images into groups based on similarities
- Detect emotions.
- Detect facial land marks.



```
Detection result:
JSON:
 [
  {
    "faceId": "c2a4af82-341a-4b1e-9dd7-ec87b29e6cc6",
    "faceRectangle": {
      "top": 202,
      "left": 550,
      "width": 127,
      "height": 127
    },
    "faceAttributes": {
      "hair": {
        "bald": 0.0,
        "invisible": true,
        "hairColor": []
      },
      "smile": 0.0,
      "headPose": {
        "pitch": 0.0,
        "roll": -21.6,
        "yaw": 10.5
      },
      "gender": "male",
      "age": 37.0,
      "facialHair": {
        "moustache": 0.6,
```

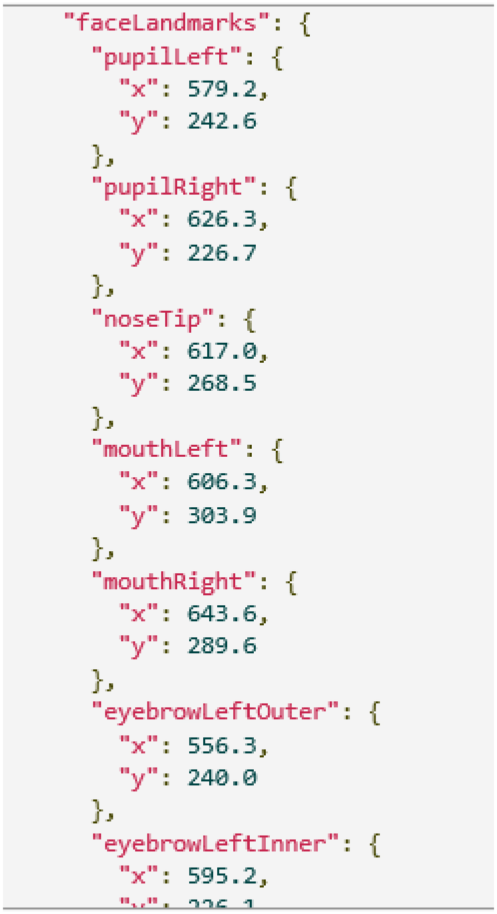
Figure 2: Face detection in Microsoft cognitive services

Inside the Detection result json,



```
"emotion": {
  "anger": 0.0,
  "contempt": 0.0,
  "disgust": 0.0,
  "fear": 0.0,
  "happiness": 0.0,
  "neutral": 0.844,
  "sadness": 0.0,
  "surprise": 0.155
},
```

Figure 3: Cognitive services Vision API, Emotion information

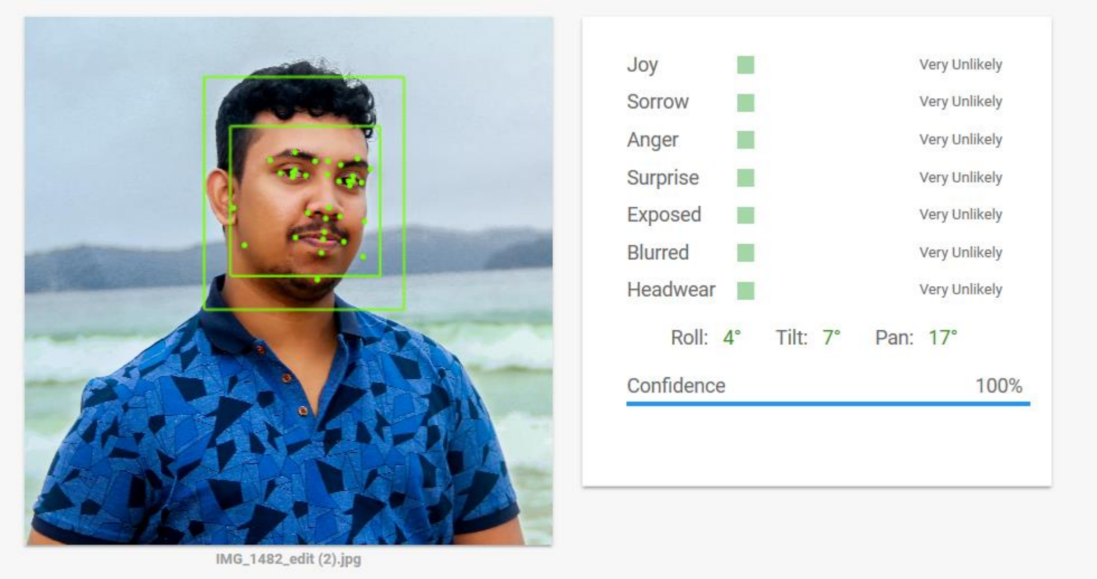


```
"faceLandmarks": {
  "pupilLeft": {
    "x": 579.2,
    "y": 242.6
  },
  "pupilRight": {
    "x": 626.3,
    "y": 226.7
  },
  "noseTip": {
    "x": 617.0,
    "y": 268.5
  },
  "mouthLeft": {
    "x": 606.3,
    "y": 303.9
  },
  "mouthRight": {
    "x": 643.6,
    "y": 289.6
  },
  "eyebrowLeftOuter": {
    "x": 556.3,
    "y": 240.0
  },
  "eyebrowLeftInner": {
    "x": 595.2,
    "y": 226.1
```

Figure 4: Cognitive Services Vision API, Facial Landmarks

1.3.1.2 Google Cloud Vision

Cloud Vision offers both pretrained models via an API and the ability to build custom models using AutoML Vision to provide flexibility depending on your use case [6].



Joy	🟩	Very Unlikely
Sorrow	🟩	Very Unlikely
Anger	🟩	Very Unlikely
Surprise	🟩	Very Unlikely
Exposed	🟩	Very Unlikely
Blurred	🟩	Very Unlikely
Headwear	🟩	Very Unlikely

Roll: 4° Tilt: 7° Pan: 17°

Confidence 100%

Figure 5: Google cloud vision [6]

1.3.2 Mapping CCTV footage (2D) human behavior into 3D model

One of the most daunting tasks in capturing human behavior patterns is to convert the 2D image into a 3D model so that we can identify the movements that are happening. There are many ways to capture these data by using special equipment but since this solution is a general-purpose solution, we will have to go with CCTV camera footage which is available in every shop or work place. This is done mainly by using a technique using DensePose

Ways to identify voice, facial expressions, behavior patterns and transaction are coming from the same source (Same person)

1.3.3 Looking to Listen: Audio-Visual Speech Separation

Google AI researcher has implemented a deep learning-based system called Looking to Listen which can isolate the voice of a video by analyzing the visual data. [7]

Peoples can separate different voices from different people on crowded environment with their brain. They are manually muting the other people’s sound and focusing a individual speaker’s voice. This is called Cock Tail Party Effect. [8]. They did able to implement a system which can separate two different people voice from a video by analyzing video and lips movements. This application able to suppress one person's voice and enhance the other person's sound. They have made a sample videos to demonstrate their system. [9]

1.3.4 Unvoiced Singing Voice Separation

Sound demos is another sound and voice related project developed by Chao-Ling and Prof. Jyh-Shing Roger Jang this system can separate unvoiced Singing voice and accompaniment separation. [10]

They have used to 2 voice separation algorithms. Robust Principal Component Analysis (RPCA) and Repeating pattern extraction technique (REPET) This research is used the MIR-1K Dataset which contains 1000 song clips accompaniment and the voice recorded separately with right and left channels. [11]

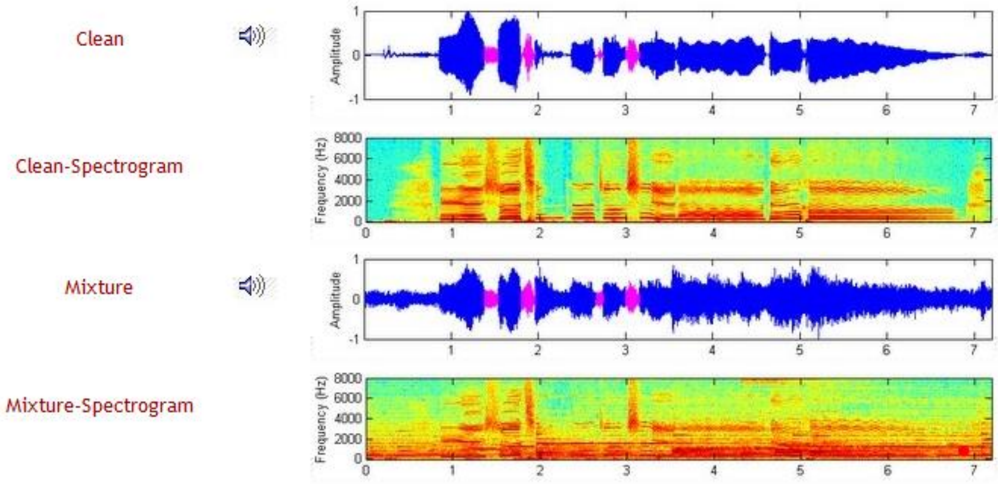


Figure 6: Singing voice and the accompaniment separation spectrogram

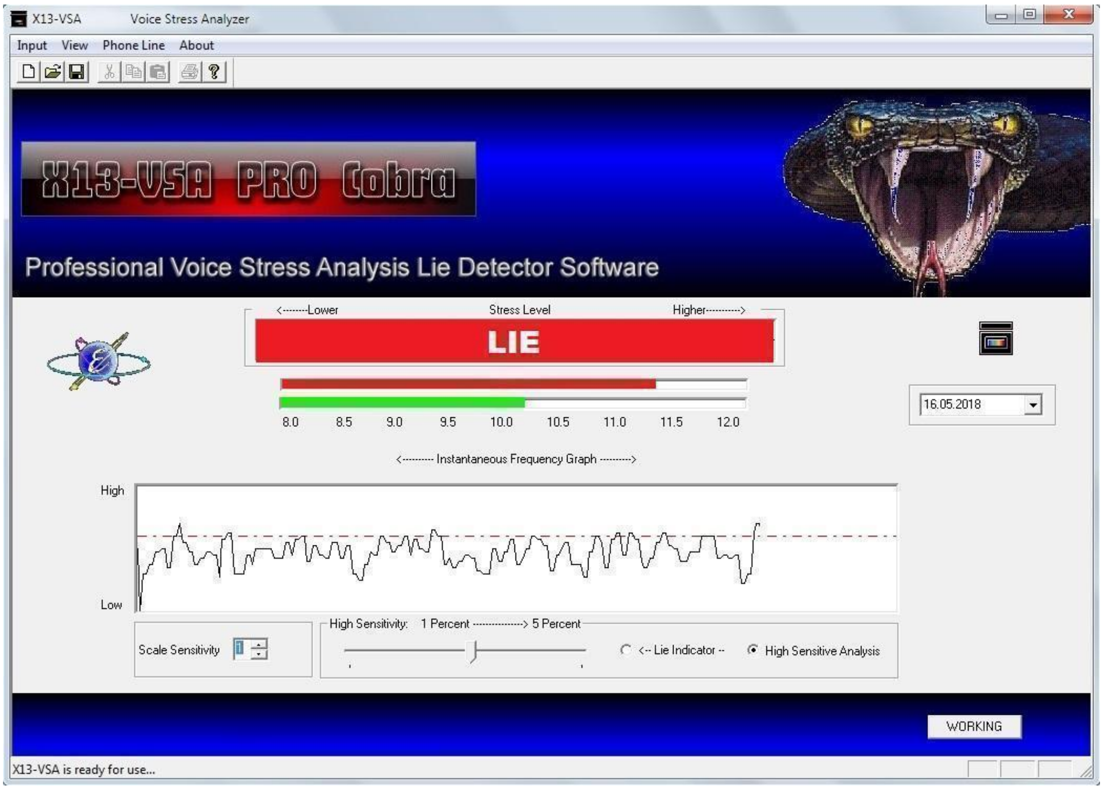
1.3.5 Markov modelling for randomly changing systems

Fraudsters do not use same techniques over and over. They are updated about fraud detection mechanisms. When their old hacks fail, they will use new methods. This cannot be predicted using simple machine learning models which are based on trained data. This is where Markov modelling comes in. This model assumes that future states depend only on the present state and not on the sequence of event that preceded it. Hence, the model will use real time data to be updated and to learn about new mechanisms of frauds. [12]

1.3.6 X13-VSA Voice Lie Detector

X13-VSA is a voice lie detector application. Most likely voice based portable polygraph application which is already quite popular commercial lie detector tool. This is developed by X13 Team. This application analyzes the peoples voice and the stress level and verify the truth. It is called VSA (Voice Stress Analyze) based lie detector, this method become popular since 1970 and widely use on secret government organization, insurance companies & police department. Since this application is a software application 98% cost effective according their official website. [13]

This product is commercially available regular price between $299 and $1480, They have released three different product versions which are same application with additional features.



16.05.2018

Scale Sensitivity 1

High Sensitivity: 1 Percent ----------> 5 Percent

○ <-- Lie Indicator --

● High Sensitive Analysis

X13-VSA is ready for use...

Figure 7: X13-VSA Voice Lie Detector

1.3.7 Enterprise Fraud Detection Solution – WSO2 analytics platform

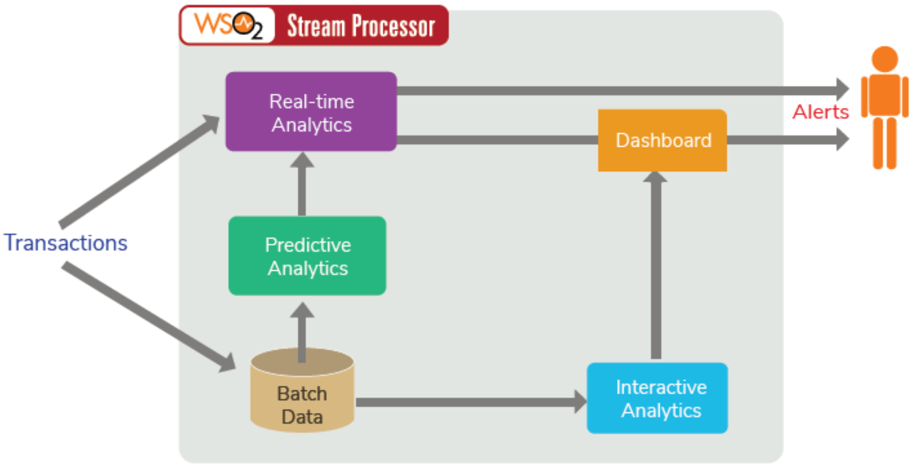


Figure 8. Enterprise Fraud Detection Solution High Level Architecture

The fraud detection solution uses the above stated Markov modelling, generic rules, fraud scoring and data clustering mechanisms. WSO2 stream processor is an open source stream processing platform. It has batch, real-time, predictive analytics capabilities. This can ingest data from Kafka, HTTP requests and message brokers. The solution covers big data and internet of things projects since it treats millions of events per second. [14]

1.3.8 Identify lies by analyzing human voice key points based on psychology.

There are few key points in the human voice clip to identify fraudulent activities. This information is collected from two articles. One Detecting Deception: Speech and Voice as a Lie Detector published on Forensic strategic solutions website [15] . And the other article has found How to Detect Lies article published on Medium corporation website. [16]

- Sound based
    - Changes of Breathing.
    - Voice frequency changing patterns.
    - Stammering & Stuttering
    - Speech patterns. (Frequently pausing, Repeating,)
    - The volume and the tone of the voice.
    - Along with emotions. (Angry, Afraid, Aggressive, Convincing)
- Language based
    - Human vocal patterns. (Avoid pronouns, avoid contractions, Generalize and exaggerate)
    - Language changes in the same conversation. (Try to control the language)
    - Words patterns (Optional - because we have to identify words as well)
    - Avoiding the questions (Optional), Answering pattern (Short answers/Long Answers, Elaborate answers)

There are many key features that we can identify fraudster with but most of them are unique to each person so in this scenario we will identify the whole person as a fraudster without limiting to a set of key features.

Research Gap

1.3.9 A complete solution comprising four modules

Even though there are systems for fraud detection and prevention, most of them only consider about one or two aspects. But this research will cover every aspect of fraud detection including micro facial expressions, voice patterns, transaction patterns and body movements. These features qualify the research product for a complete fraud detection solution. The importance of the 'complete solution' is that even if one module fails at some point, other three modules will be able to keep the accuracy of the prediction.

1.3.10 Research Gap for Voice-based Fraud Detection.

There are many voices-based recognition and analysis natural networks available on earth. But so far no one had tried to develop a lie detector by analyzing voice with a neural network. X13-VSA is the closest product found on internet. This system only analyzing the voices stress level to detect the lies. although this system is analyzing voice with algorithms.

According to other psychological papers there are many things can be considered to recognize lie by analyzing human voice patterns. So far no one has tried to develop a voice-based lie detector based on other psychological fact. Also, there are no particular reasons why anyone did not tried to develop a voice based lie detecting system based on other psychological facts.

In Table 2. Summarized table of existing resources related to voices-based fraud detection we have mentioned summarized analysis of everything we have found on internet and all through the literature review.

There is many hardware equipment which can remove background noises without any software solution and as a lie detector classis polygraph machine also an complete hardware equipment. Many software solutions and research exist for background noise reduction.

However, there are no hardware only equipment for isolating human voice and to identify speaker. Third party application can isolate speaker sound but yet no third-party application publicly available to identify a speaker. But many technological researched are available to isolate vocals and identify speakers. Many publicly accessible git hub projects are available for this.

Video vocal mapping is a way to identify speaker with video and voice analysis at the same time, Google has done this kind of project we have mention is in literature review on above named Looking to Listen [9].

Only few voice-based lies detector available outside the polygraph machines. X13-VSA is one of those. And also, there are not many solutions to analyze and identity key points of voices. Stress and emotion analyzing researches are exists but stammer, stutter, frequently pausing cannot recognize currently available project.

	Hardware Equipment	Third Party Software	Datasets (public)	Services, Libraries or Models	Technology Researches
Background Noise Reduction	**YES**	**YES**	**YES**	**YES**	**YES**
Isolating Vocals	**NO**	**YES**	**YES** **mir-1k** [11]	**YES**	**YES**
Identify the Speaker	**NO**	**NO**	**YES** **TIMIT** [18]	**YES** [19]	**YES**
Video Vocal Mapping	**NO**	**NO**	**NO**	**NO**	**YES** **Google** [9]
Voice Based Lie Detectors	**YES** **Polygraph** [15]	**YES** **X13-VSA** [13]	**NO**	**NO**	**YES**
Identify Key Points of Voice	**NO**	**SOME** **emotions**	**NO**	**NO**	**SOME** **Stress, emotions**

Table 2. Summarized table of existing resources related to voices-based fraud detection

1.3.11 Research Gap for Fraud Detection Using Transaction

A transaction fraud detection system for Automatic Teller Machines states that it’s steps to identify a fraud as below.

- Predict the type of transaction to be requested by the user.

- Compare the predicted transaction with the transaction actually requested by the user.

https://patents.google.com/patent/US5386104A/en

Above system basically compares the user’s current transaction with his/her expected transaction. So it is a user profile based system. But to get better results, we might need to predict transactions based on a community level because there might be trends for seasonal changes and for other reasons. Otherwise, getting limited to user profile based predictions will lead to incorrect predictions.

1.3.12 How a trained AI can identify anomalies faster and more efficiently than a human

First thing that comes to mind when mentioning machine, is efficiency or fastness. It does not take breaks like humans. Decision making only happens logically. But humans tend to bias to their opinions when taking decisions. After going through a series of decision making, machine’s accuracy will be much higher. So it is evident that AI will greatly improve the fraud detection mechanisms than the traditional human approach.

	Hardware Equipment	Third Party Software	Datasets	Services, Libraries or Models	Technology Researches
Person Identification	**YES**	**YES**	**YES (Coco dataset)**	**YES**	**YES**
Person Tracking	**YES**	**YES**	**YES**	**YES**	**YES**
Behavior Mapping	**NO**	**NO**	**NO**	**NO**	**NO**
Identify Key Points for Frauds	**NO**	**NO**	**NO**	**NO**	**NO)**

Table 3; Summarized table of existing resources related to behavior pattern fraud detection

1.4 Research Problem

Today, the world has a problem of different kinds of fraudulent activities. If we can identify these activities beforehand, we can prevent lot of loss. There is no clear existing system to validate these behaviors so it’s prone to many human errors. These kinds of frauds happen in many places around the world, as in cloth shops, banks, grocery stores and even hospitals.

As mentioned above, this can be used in various places for different uses. With this system, we can prevent unexpected fraudulent activities while preventing big losses to the society.

Our outcome is a machine learning based solution that will be comprised of 4 modules. Each module will give “**this is suspicious**” mark. Average of these marks will determine whether this is a possible fraud or not.

Assembling multiple different models is a common approach in data science. While you can make a single model, it will always have its strengths and weaknesses. It will recognize some patterns, but miss the others. To make predictions more accurate we will combine all four components. Thus, all models from the ensemble analyze the same transaction and then “vote” to make a final decision. It allows for leveraging the strengths of multiple different methods and make decision as precise as possible.

1.5 Potential For Entrepreneurship / Commercialization

Since this solution uses attributes that are common to most of the places, we can use this system in any place with minor modifications.

One of the major problems in the banks or financial institutes is fraud activities. With this all round solution, these companies will be able to easily reduce lots of fraud activities.

OBJECTIVES

1.6 Main Objectives

Main objective of this proposed system is to implement a system which can identify differences between regular customers and deceiving persons by analyzing fraudulent activities in a crowded environment. This system states a prediction of each individual customers whether they are suspicious or not based on their transactions patterns and human behavioral patterns such as facial expressions, body language, changes of voice.

1.7 Specific Objectives

1.7.1 Fraud detection based on facial behavior and patterns

Implement a sub system which can identify fraudulent activities of customers by analyzing facial behaviors and facials expression patterns. This system can calculate how suspicious the customer or the person via machine learning model.

- Gather data from Kinect sensor. Which are RGB Camera data and depth data.
- Turn those video data to frame by frame photos.
- Gather/ Extract nearest person’s facial data.
- Try to compare frame by frame and extract
    - Emotions.
    - Micro-expressions.
    - Eye movement & etc.

- Using those data train, a CNN.
- Using that trained CNN predict customer is suspicious or not.
- With giving a feed back after words we can improve accuracy of the CNN.

1.7.2 Fraud detection based on changes of voice & speaking patterns.

Implement a sub system which can identify customers' fraudulent activities of the by analyzing their voice data and speaking patterns. This sub system will be able to states a prediction for a customer whether he is suspicious or not by analyzing his voice changes and speaking pattern.

- Making a three microphones setup which can be connect to single personal computer via portable sound card.
- Implement simple recording application which is able to record from all microphone at once into individual sound clips.
- Gather all voice data from all parallel microphones.
- Analyze the voices clips, then modify and trim the voice clips for individual customers.
- Isolate the voice of the customer by removing background noises and other people's voices.
- Identify vocal changes and key points of speaking patterns.
- Label the data with facts or under supervision of knowledgeable person.
- Implement a suitable neural network to train the machine learning model.
- Train the final machine learning model with the implemented neural network.
- Integrate trained machine learning model with final system and display the results on user interfaces of the system.

1.7.3 Fraud detection based on transaction patterns.

Implement a sub system which can identify fraudulent activities based on transactions details. By analyzing previous transaction data, transaction system will be able to state the likelihood of a transaction being frau.

- Gather previous transactions data from an organization or reliable publicly open data source.
- Analyze all transaction data and label the data using commonly identified rules from previous researches.
- Construct neural network to train a machine learning model.
- Train the neural network with labeled data set and integrate the model with final system results will be display in user interfaces.

1.7.4 Fraud detection based on human behavioral and body language.

Implement a sub system which can identify fraudulent activities of customers by analyzing human body-language and abnormal movements from CCTV camera footages and systematically categorize and profiling each customer according to risk level and suspiciousness.

- Configure other already implemented neural networks on a high-end personal computer. Such as DensePose.
- Download and train the machine learning model with required dataset for above mentioned neural networks.
- Collect CCTV footage from research site or organization which is suitable for our project.
- Organize the CCTV footages and identify abnormal behaviors manually under supervision of knowledgeable person or Implement simple algorithm to identify abnormal behaviors and label the dataset using DensePose outputs.
- Implement a deep learning neural network and train a machine learning model with the above dataset.
- Categorizing persons according to risk level and result will be show on main systems’ user interfaces.

2 METHODOLOGY

In this part we will describe how we will tackle the aforementioned problems which is identifying fraud (anomalies) in the surrounding area. In the following scenario we will consider a Bank as the environment and user as the person who is with suspicious behavior.

When the customer first enters to the site, he/she will be tracked by the CCTV cameras in the premise even if the customer changed between floors or multiple CCTV cameras he will be identified as a single person, this tracking is even done throughout the components that means the program will know that it’s same person who had abnormal behaviors, voice, facial expressions and the transaction details. By tracking the person like this we increase rate of getting positive result.

2.1 Requirements Gathering

Requirement gathering is the main part of an any project. For this project we have divided requirement gathering into two main categories. Literature reviews and identifying existing system. Literature review also had two main categories Psychological articles and technological papers.

2.1.1 Literature Reviews

2.1.1.1 Psychological Articles

Since this project mostly based on human behavioral patterns. Psychology has major part of this project. Reading through past research papers, psychology article and psychology eBooks we have gathered many information related to this project. Basically, human can identify fraudulent activities by looking at another person's body language, movements patterns, facial expressions. And, human can identify if someone lying or not. Also, there are highly paying professions are available to identify human body-language and predict humans' future behaviors. We have found few psychological evidences to identify fraudulent activities by analyzing human behavior pattern.

2.1.1.2 Technical Articles

Final solution is a software solution. Cause of that technology literature reviews also has a major part of this project. To implement this system, we have to read through past research papers, technology articles and technology eBooks and gather information related to our project. Mostly machine learning, deep learning and neural network knowledge will be very useful to implement this solution. Other than data science we have collect information about image processing algorithms, sound waves manipulation, high tech devices which can identify body parts easily such as Kinect sensor, leap motion and various range of motion sensing devices.

2.1.2 Existing Systems & Relative Systems

There aren’t any systems that are known to detect fraud before it happens most of systems in place right now will only give us result after the fraud has happened. This is not that much useful at all of course we can track down the person who did the fraud afterwards, but it always says that prevention is better than the cure. [15]

There are also polygraph system which not that practical to use when we need to analyze huge crowd at once and do it discreetly so that it would not induce paranoia with other people.

2.2 Feasibility Study

2.2.1 Schedule Feasibility

This proposed system should be able to finalize before the due date. Both software solution and the documentation should be able to present before each milestones' due dates. With other academic works and career work we should determine does this system scope is feasible to complete within give time duration. With current estimation we will be able to deliver the system within given time duration.

2.2.2 Economic Feasibility

This proposed system should be a generic product which can be purchased by other organizations. These systems mostly require for financial organization. But some part of this system is allowed to work with other organization as well. Most financial organization looking for these kinds of product with much reliability. Because of that, this system will be economically feasible. Also, our prototyping project economically feasible as well, because we are planning to use easily achievable common devices.

2.2.3 Operational Feasibility

This proposed system should be fully operational and user friendly, User only get analysis data prediction on their display. It won't be effect to organization daily routine. Since this system evolving with the new record. Result will become much more accurate with the time. This system can be easily adapting with the organization, because of that, this product also operational feasible.

2.2.4 Technical Feasibility

Technical feasibility is most important from above all otherwise we cannot implement a proposed system. With the current machine learning technologies this system is technically feasible as well. We have divided the gathered technical data into some categories to describe.

2.2.4.1 Machine Learning & Deep Learning

Machine learning is data scientific study of algorithms and statistical model. This is subset of Artificial Intelligences instead of creating a explicit algorithms machine learning can create mathematical model of sample data. [16]

For fraud detection based on voice part need few extra supports before main functionality, Frist customer voice should be separate from background noise and voice should be isolated with other human voices. Otherwise result will not be much accurate. For these tasks there are many background noises reducing, voice isolating neural networks and machine learning models exist today. Also using multiple microphone sound background noise reduction and voice isolation possible without any neural networks. For an example

- Google researchers implemented Audio-Visual Speech Separation tool.
- Both RNN & CNN voice isolating open source project on GitHub
- Mobile phones are voice isolating and removing background noises by using multiple microphones.

Beside this only requirement is to recognize key points of voices and train machine learning model to make prediction with those data or using deep neural network without considering key points directly train a machine learning model to identify fraudulent activities. This is also feasible because there are some papers identify emotions and stress level of a personal by analyzing human voice.

2.2.4.2 Kinect Sensor

Two major lie or fraud detection areas of this research are,

- Facial behavior,
    - Expressions and Emotions.
    - Eye tracking.
- Body language behavior
    - Touching nose.
    - Covering face/ mouth.

Using normal camera these sensitive data can hard to retrieve. Even somehow, we've able to retrieve those data it can be inaccurate. So, we decided to use Kinect Sensor [17] to capture above mentioned data.

Kinect sensor is a line motion sensing input device which is developed by Microsoft [17]. Kinect consisted with 3 major inputs.

- RGB Camera.
- 3D depth sensor.
- Multi-array microphones.

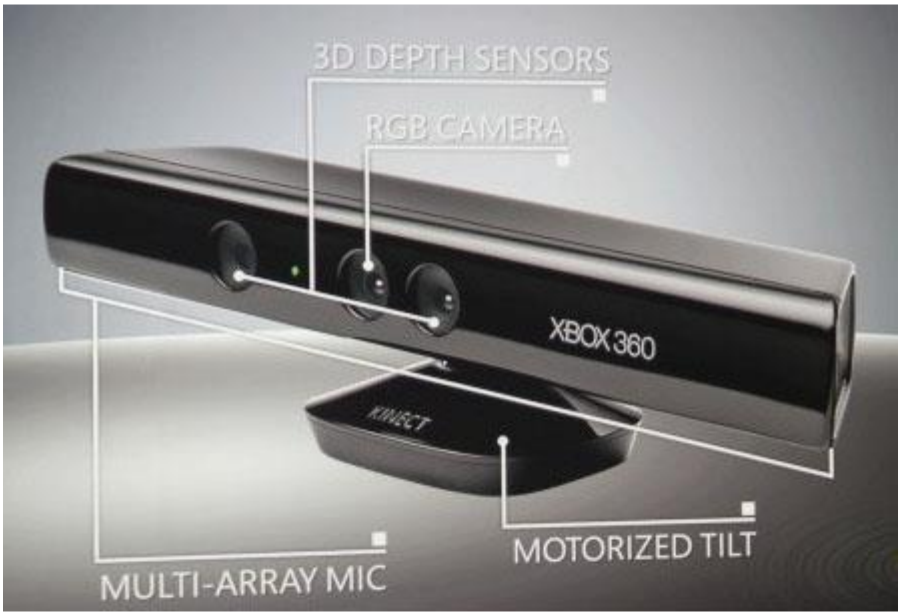


Figure 9: Kinect for Xbox 360, Inputs

RGB camera and Depth sensor are used to recognize all above facts during the test. And Kinect SDK can use for our development purposes.

2.2.4.3 CCTV

Since we are using CCTV cameras to track people in site and the luxury of calibrated cameras or environment models are not available in most situations, we are going to build a model of the relationship between the field of view (FOV) lines of various cameras so that we track where the person is at in all times. https://ieeexplore.ieee.org/document/937537

2.3 Requirements Analysis

Requirement analysis is also a major part of any software-based project after the literature review, we have to analysis all data and information we have gathered on all through the process of literature review. In research gap we have mentioned some analysis part of this project. What currently available and what we have to create for this project.

2.4 System Analysis & Designing

Our solution is mainly focused for Financial Institutes. The aim of this system is to analyze the human facial expressions, behavioral patterns, voice patterns, background environment and human interaction with the environment and identify the possible anomalies.

- Facial patterns using camera or Kinect like sense detection camera.
- Human behavioral patterns using CCTVs stream.
- Voice and Speaking patterns using Microphone.
- Suspicious transactions using Transaction data/ history and environment/ social factors.

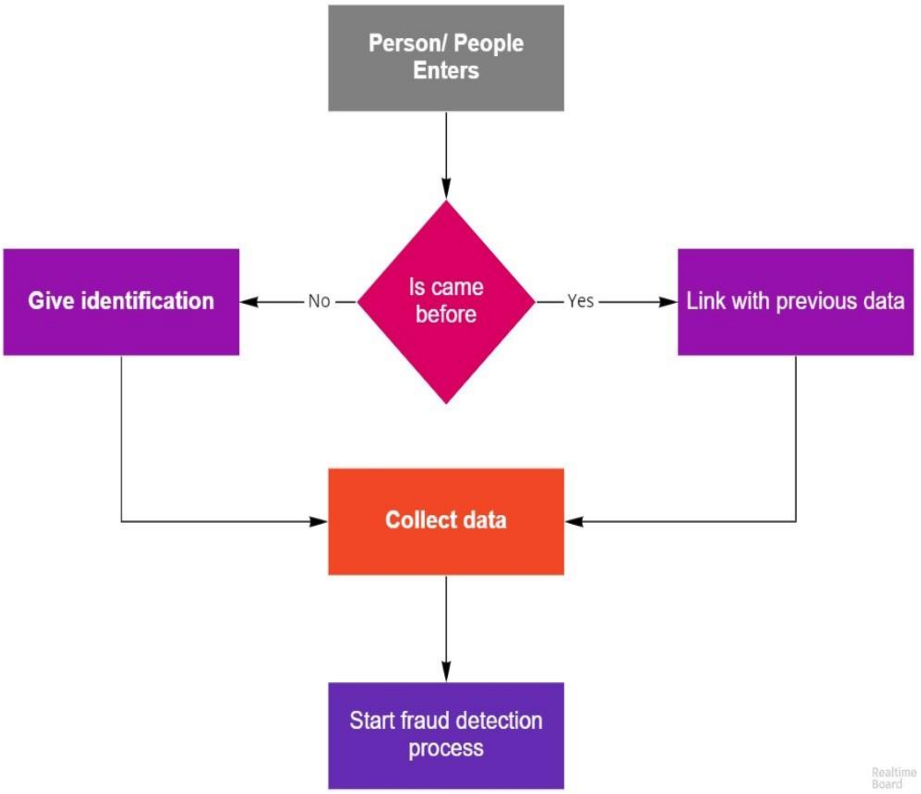


Figure 10: High level diagram of the system 12

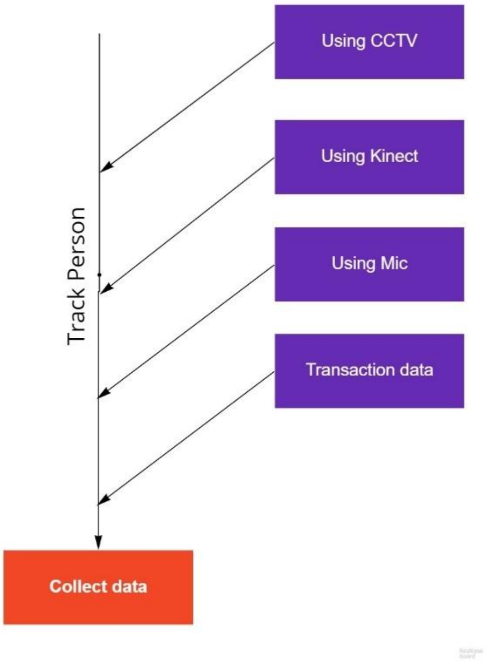


Figure 11: Data collecting process

2.4.1 Main Functionalities

2.4.1.1 Identify frauds based on facial behavior and patterns

Humans can identify or inspect, whether a user is trying to do a fraudulent activity or trying to lie by looking at the person. On average people don’t do much better than a coin flip.

But by using machine learning techniques and algorithms we can automate and increase the accuracy of the detection of fraudulent activities and identify patterns that people normally use for doing fraudulent activities.

To get the facial data we can use a Kinect camera/ sensor that aim towards to the customer’s (user’s) face.

Using the camera, we can detect

- Expressions and Micro-Expressions.
- Emotions.
- Eye movements.
- Nose touching and mouth covering.
- Sweating.

These are some psychological effects when someone trying to hide their true intentions from others or simply when someone trying do a fraudulent activity.

By using these data, we can predict or assume whether this user is suspicious or not, with some confidence level. With information that cashier or officer who doing the transaction can give more attention to the user(customer) and probably reduce or prevent fraudulent activities from happening.

2.4.1.2 Identify Fraudulent Activities by Human Speaking Patterns.

Human can identify frauds, lies, deceits or scams by another person's voice or speaking pattern. Mainly there are two types of methods to identify frauds using the voice. Those types are, **Language Based** & Sounds Based. Since language-based type depend on specific language it cannot be implemented for Sri Lanka, because identifying meaning of Sinhala speeches are quite bigger domain. So, the target is to identifies deceits with sounds based.

Sound based frauds detecting can be done by two type of methods.

1. Key points and rules based (Based on psychological studies)
2. Deep learning based. (With labeled dataset of deceiving or not)

Key points of sound-based frauds detecting are changes of breathing, changes voice frequencies, stammer, stutter, frequently pausing, repeating, volume and the tone of voice, vocal expression of emotions (screaming, yelling, whining and crying) etc.

Since this solution will be working on crowded environment most challenging part is cancelling the background noises and identify isolated customer voice with fine details of the sound. Then the dataset will be manually label for key points (Method 1), and suspiciousness (Method 2).

Then by training a neural network, this part of the solution can state a prediction for suspiciousness of certain customer by their voice. Overall flow shown in Figure 12: Voice Capture

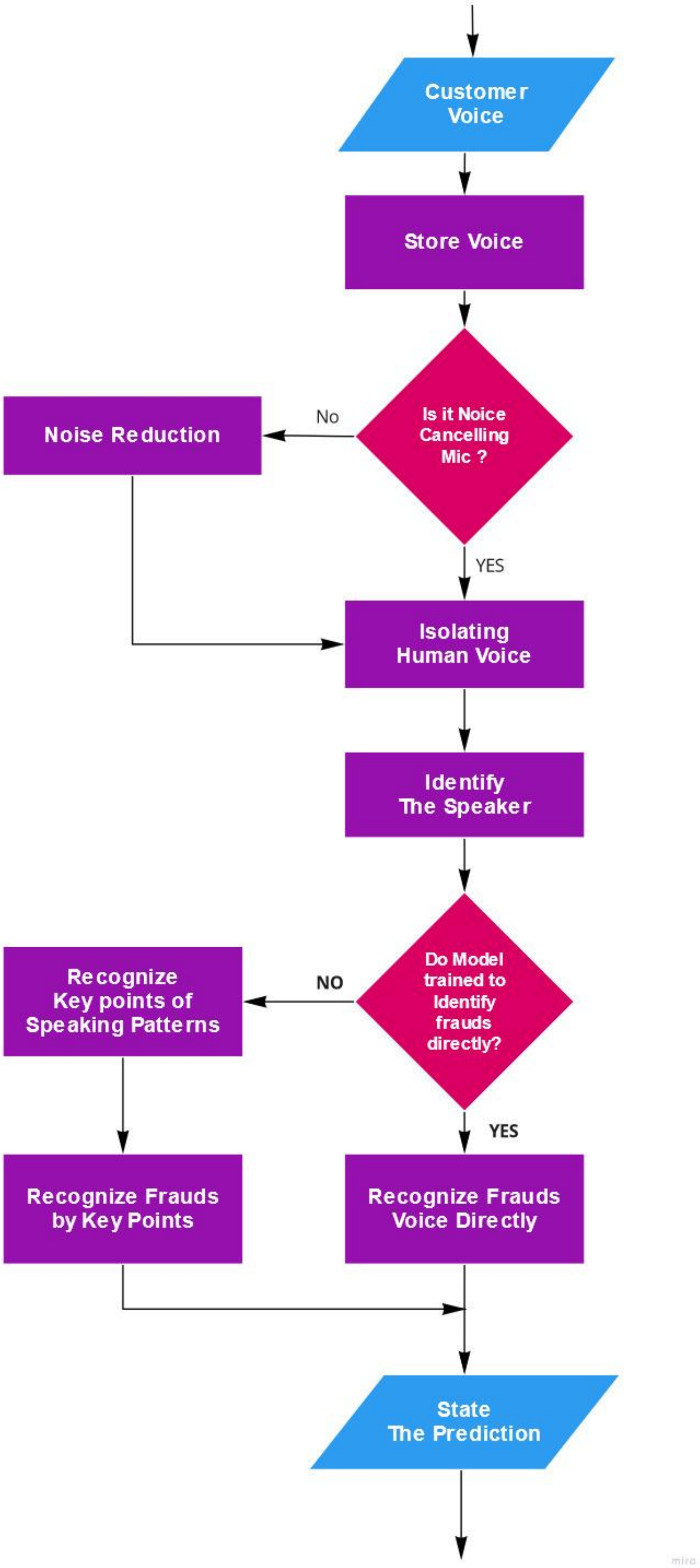

Customer Voice
Store Voice
Is it Noice Cancelling Mic ?
No
Noise Reduction
YES
Isolating Human Voice
Identify The Speaker
Do Model trained to Identify frauds directly?
NO
Recognize Key points of Speaking Patterns
YES
Recognize Frauds by Key Points
Recognize Frauds Voice Directly
State The Prediction
miro

Figure 12: Voice Capture

2.4.1.3 Fraud detection based on transaction patterns.

In this component, customer’s transaction history is checked for unusual patterns. we need to identify a wide array of fraud scenarios to predict a fraud activity using transaction details.

There are some known fraud patterns in transaction details. We can identify these by using a rule engine. But new fraud types/patterns can be introduced by different fraudsters. This system identifies those unknown frauds, by learning new patterns using Machine Learning algorithms.

A transaction can be flagged as a fraud by using different rules. Examples:

- Transaction velocity – how many transactions per minute.
- Abnormal transaction quantities.
- Number of consecutive transactions made.
- Current trends, seasonal changes.
- etc.

Thresholds of the above rules can be changed according to the organization requirements. All these rules will output a single score, which will determine how likely this transaction is a fraud.

2.4.1.4 Fraud detection based on human behavioral and body language

Since the past humans have been able to identify fraudulent activities by looking at another person's body-language and gestures, there are highly paid individuals whose job is to find out those abnormal behavioral patterns. So, in this research part we are trying to automate this process by developing a software solution to identify frauds with human body-languages and abnormal movements using CCTV camera footages. In this research we have decided use deep learning approach since there might be some social cues we might miss if go with labeling each behavior.

There are three main parts to this sub component

1. Identifying anomalies.
2. Creating a risk profile.
3. Tracking between multiple cameras.

By using this method, we will mainly categorize the persons in the vicinity according to a risk level and those who are with a higher risk level will be analyzed thoroughly by the other components of this research. By doing this we are saving the computational power wastage of analyzing every single person in detail who enters the vicinity.

2.4.2 Gantt Chart

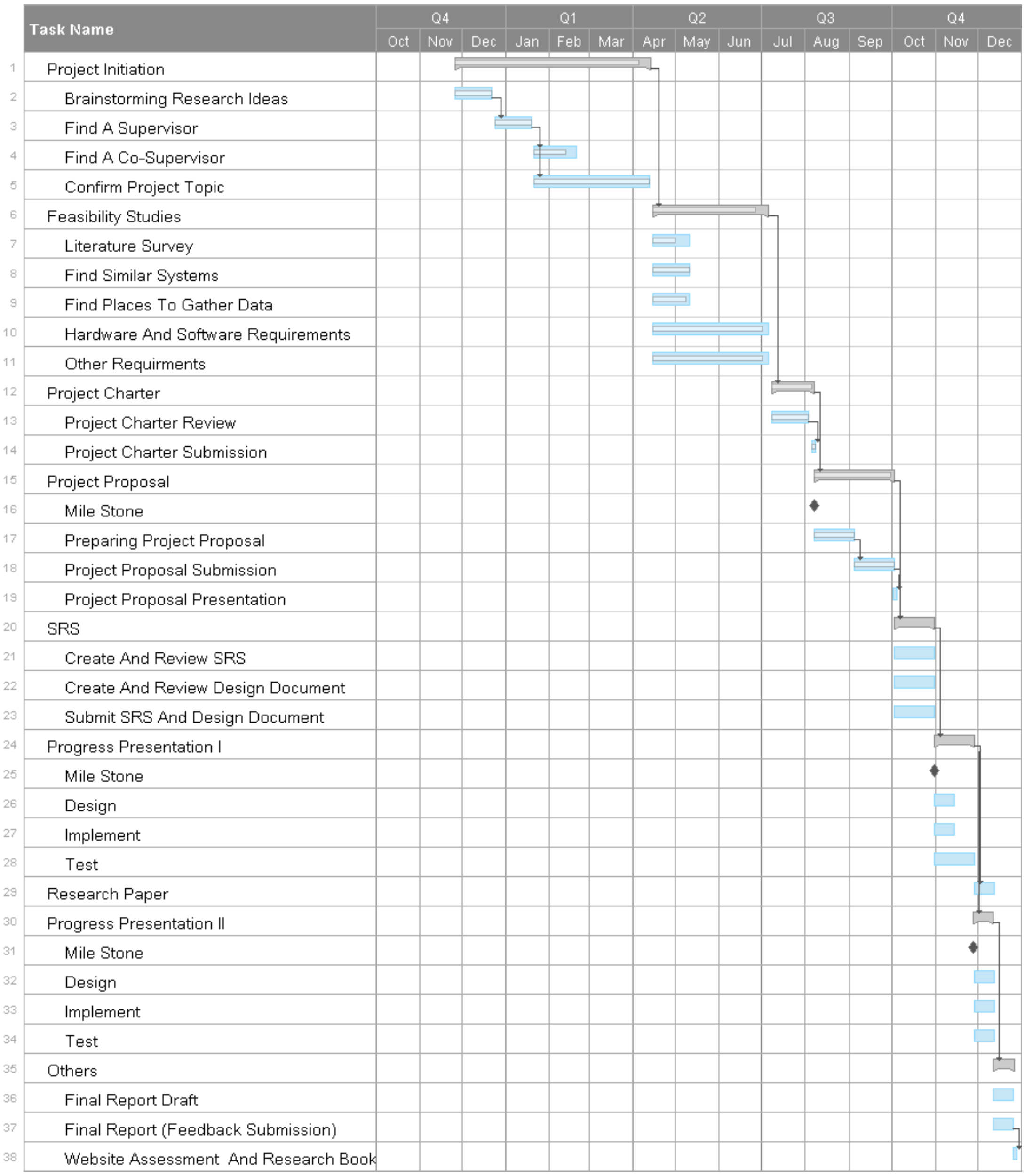


Figure 13: Gantt Chart

2.5 System Implementation

Implementation of overall system start with gathering raw data to train machine learning models. Each team members required different kind of dataset for their projects. Some members required special devices setups to collect data. Such as,

i. Front facing camera footages to identify facial expressions
ii. Voice recording to identity lie with changes of voices.
iii. Financial company transaction data to transaction analysis.
iv. CCTV camera footages to identify body-language.

Once we have gathered the raw dataset, it needs to be labeled carefully before train a neural network. Even though some data will be labeled manually, and some data will be labeled with using simple algorithms to cut off some work load.

2.5.1 Preparing Dataset for the Project

2.5.1.1 Preparing dataset to Identify frauds with Facial behavior patterns.

In order to detect fraud detection using facial behavioral patterns we need to gather raw Kinect [17] camera data. And using those data we can trains a Convolutional Neural Network (CNN) [20].

To gather above-mentioned data, we have 2 main methods.

Gather data on LB Finance

- We can use real world scenario for this as well.
- More accurate data.
- Hard or can’t get permission to get data from bank environment.
- And customer can get confuse when there’s a big bulky setup if front of their faces.
- Once we setup the configuration we can’t access to our setup until end of the day.
- Hard to label data.

Gather data on SLIIT

- We can use SLIIT main building 2nd floor public area for this experiment.
- 2nd floor public area is normally crowded. So, we can simulate kind of real-world scenario.
- Easy to configure and setup.
- Can organize a small event and label data when users face to the camera.

We chose the second method to gather our data. Even though first method is the best option it also hard in many ways.

For the second method we are going to organize a small interview and gather labeled data.

About the interviews

We are going interview our participants with series of questions from different areas. We are trying to do our best to fit those questions to bank environment. They can decide whether they need to lie or tell the truth.

In that interview we are going to gather the data facial data, voice and behavioral data. After the interview we give them to label the data.

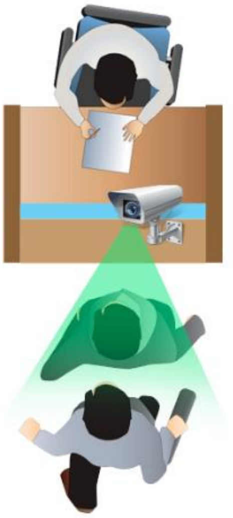


Figure 14: How interviews going to held

More about the environment can find on 2.5.1.2 below

2.5.1.2 Preparing dataset to Identify frauds with changes of human voice patterns.

To Implement a sound-based fraud detection system. First need to gather raw data and label the dataset before train the machine learning model.

To collect the recording data there are two different approaches for this attempt. Our client still does not give us the permission to provide a support to collect data from banking environment. Because of this issue we are creating similar environment on a public area and also create some regular anomalies and fraudulent anomalies to create the raw data which is required for this system.

Creating similar environment

For this attempt we are creating three cash counter environments in a crowded place. As shown, in the figure.

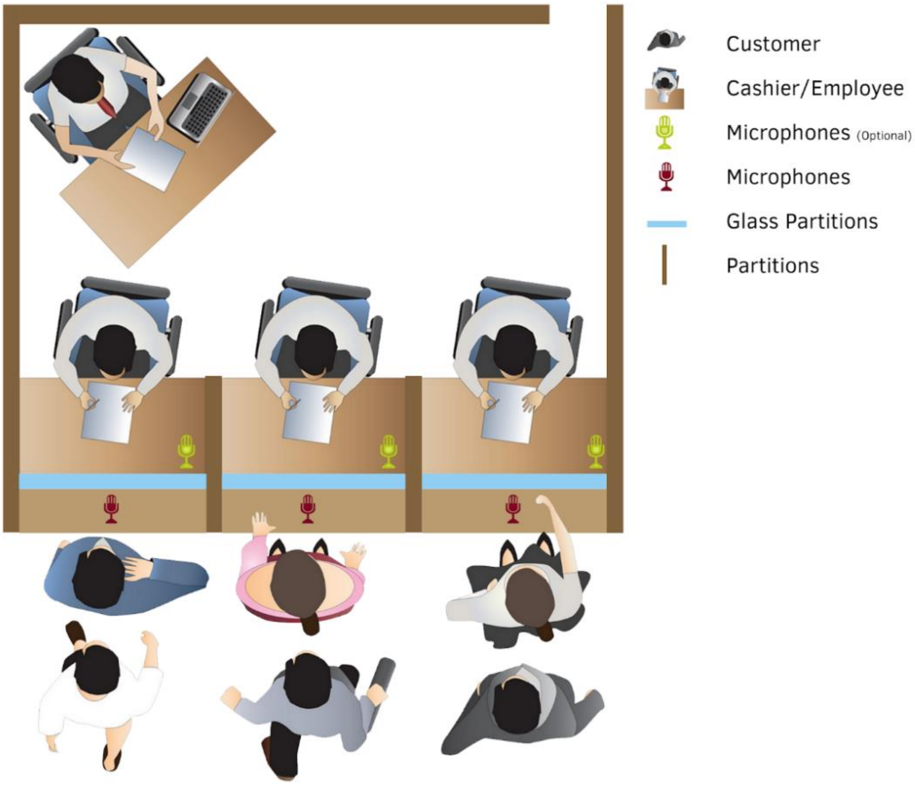


Figure 15: Parallel Cash Counters in a Banking Environment

We have decided to choose SLIIT (Sri Lanka Institute of Information Technology) main building 2nd floor public area for this experiment. Because SLIIT also very crowded with many background noises. In this case we can recreate the more similar background noised environment like bank.

Microphone Setup.

This proposed microphone setup will be creating with three microphones parallelly placed with the counter as in the (Figure 15: Parallel Cash Counters in a Banking Environment**).** All three desktop microphones (Figure 16: Desktop Microphones) connected to USB hub (Figure 18: Multi USB Hub **)** And the USB hub connected to PC. As in

Figure 16: Desktop Microphones

Figure 17: Lavalier Microphones

Figure 18: Multi USB Hub

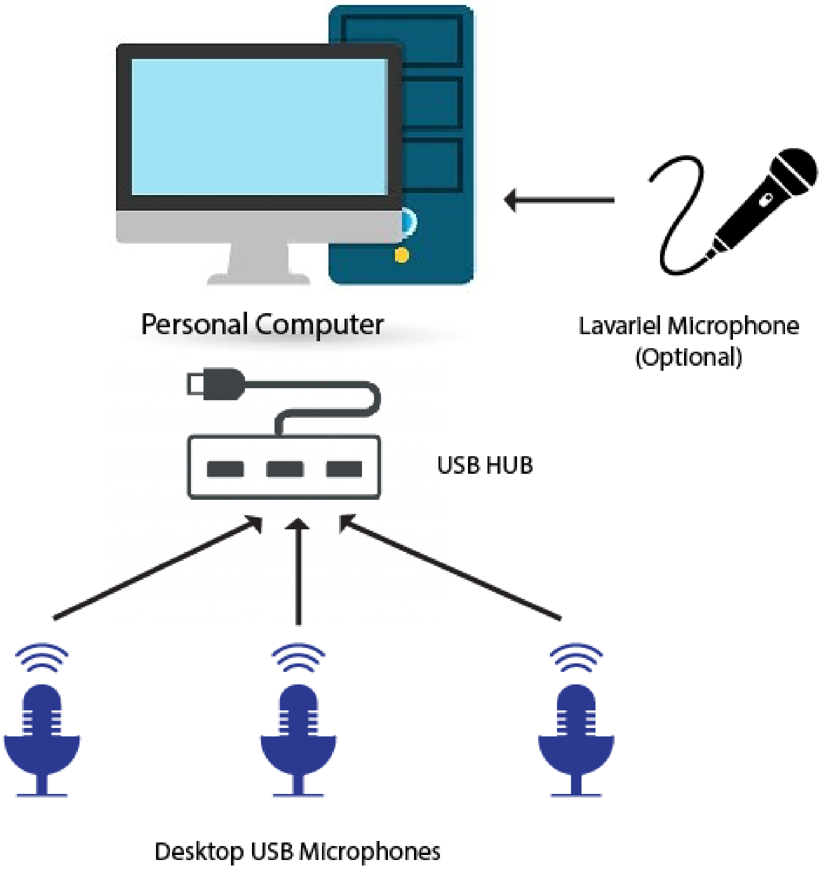


Figure 19. Microphone setup high-level diagram

Creating anomalies/events.

As for the anomalies we are creating some simple events. First of all, we must choose sample population for this experiment. For that we will choose few random students from SLIIT. To create similar event, we are creating simple questionnaire and interview those selected students. The sample questionnaire will be attached in the appendixes.

This questionnaire interview will perform twice for the same sample population and first time they should responds to the questionnaire with truth and second time they should answer the questionnaire with fake answers. Both data collections will be stored along with the labels.

In second experiment, we are giving three envelopes the sample population and one of these envelopes contains money other two contains useless papers. Person from the sample population should convince the cashier to take both papers contained envelopes instead money contained envelope. If the person successfully achieves to give cashier paper contained envelopes. We will allow to take the money inside the envelope. This way we can create similar event like fraud.

With these 2 experiments we will be able to create equally valued dataset to train our machine learning model. Executing these experiments, we will able to collect as much as data to require to train the machine learning model.

Recording software implementation.

And there is simple software implementation to record all three microphones parallelly into a different sound clip. These kinds of open source software do not exist on internet. In that case easiest way to implement simple software to record from three different microphone separately.

This setup will work for real bank environment and the temporary created environment as well.

Collect Data and Analyze

Then all sound clips carefully trimmed and encoded into common file format and stores the all data very organized way. hen manually labeled those data with the known information and facts. Also, key points will be labeled as well such as.

- Stress Level of the voice.
- Stammering & Stuttering
- Speech patterns. (Frequently pausing, Repeating,)
- The volume and the tone of the voice.
- Emotions. (Angry, Afraid, Aggressive, Convincing)

2.5.1.3 Preparing dataset to identify frauds with transaction data.

Transaction data is needed to train the specified machine learning model. These can be collected from a financial institute. To label the transactions as legit or not, police data records could be beneficial. The disadvantage of these data sets is that they are extremely imbalanced. Legit transactions are much higher than fraud ones. “Boosting” is a technique that can be used to work with this kind of data set.

If for any reason, the dataset is not available, a public data set can be used to train the model.

After data collection phase, the data should be pre-processed. Even though there will be lots of columns to this data set, model only needs a specific number of features. Customer names, ids, addresses and other sensitive data are not needed. To decide whether the given transaction is legit or not, crucial features might be transaction time, place, amount and merchant. Further data analyzing can be done using transaction quantities and transaction velocity (how many transactions per given time) for a specific customer.

These data are now in a raw state. It cannot be sent through a model directly. Data set should be checked for missing values and should standardize. After this process, model training can be started.

2.5.1.4 Preparing dataset to Identify frauds with body-language.

To gather data to analyze behavior pattern we are going to use CCTV camera footage which will be provided by the LB Finance and a Pharmacy in the area. The CCTV footages that are collected from the LB Finance are in analog format so we’ll need to additional conversions before we feed it into our system.

2.5.2 Individual research parts implementation.

After finalizing dataset for the project, we need to require neural networks or experiments to train the machine learning model. Some system required support of already implemented projects. For an example,

- To identify human body landmarks from cctv footages most reliable way is to use Facebook DensePose project.
- OpenCV and cognitive services will be very useful to cut down some unnecessary workload of implementation
- There are many existing neural networks which can identify speakers individually, or voice isolate without any background noise.
- Etc.

2.5.2.1 Implementation of Identify frauds with Facial behavior patterns.

To implement we need pre-process video footages we gathered using Kinect camera. Normally Kinect camera's output video is around 25-30 fps.

First, we need to take frame by frame as series of images. And try to detect the face of the person who we interviewed. We know interviewed person is the one who nearest to the camera so we can extract him/ her by using Kinect camera's depth sensor. After that we can crop the face from the image.

If this process unable to find a face or hand that covering the face, then we can simply remove that frame from further processing.

Then we can start train our CNN using,

- Facial data.
  - Facial land marks.
  - Expressions and Micro-expressions.
  - Emotions.

- Eye tracking.
    - Eye direction.
    - Eye blinking.
- Behaviors
    - Touching nose.
    - Covering mouth.

Once we trained our CNN, then we can use that CNN to predict how suspicious our user/ customer is.

2.5.2.2 Implementation of Identify frauds with changes of human voice patterns.

Prepared dataset needs to be pre-process before the final approach current dataset is labeled it does contain background noises and peoples sound. regular polygraph machines are operating in covered environment which doesn't has any background noises and other people sounds Figure 20. But it our situation we are having major problem causing by background noises. Banking or financial institute environments are crowded places Figure 21,

Because of this issue we need to preprocess the dataset. By,

- Background Noise Reducing
- Isolating speakers voice & Identifying the speaker

Commonly noise cancelation will be done by recording the noise with another microphone and inverting the noise wave and adding to the original sound clip. Figure 22. For this project we are going to use existing sound isolating neural network and as for the input we will use all three-microphone data.

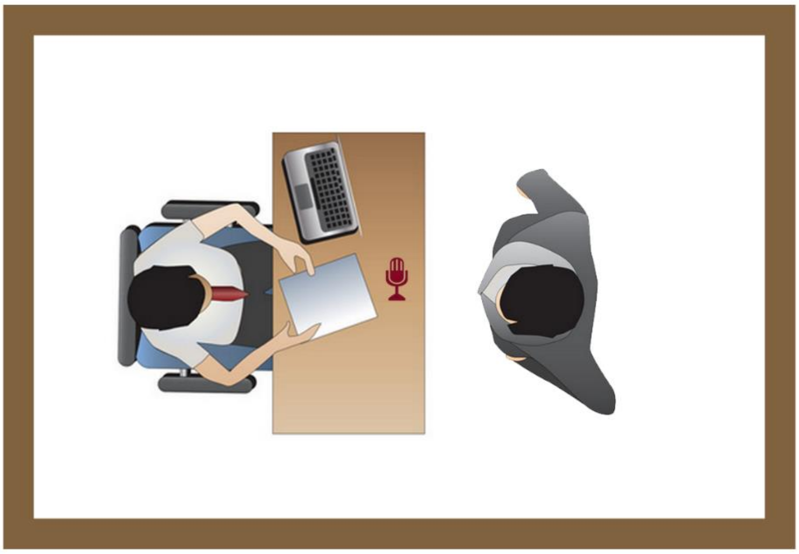


Figure 20. Analyze voice in regular lie detector.

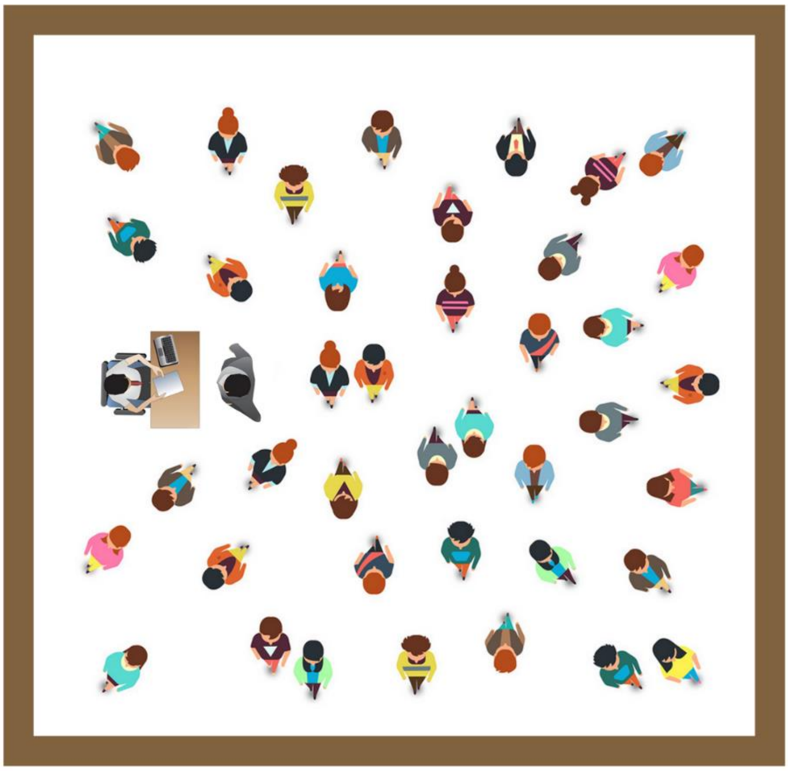


Figure 21. Analyzing voice in crowded environment

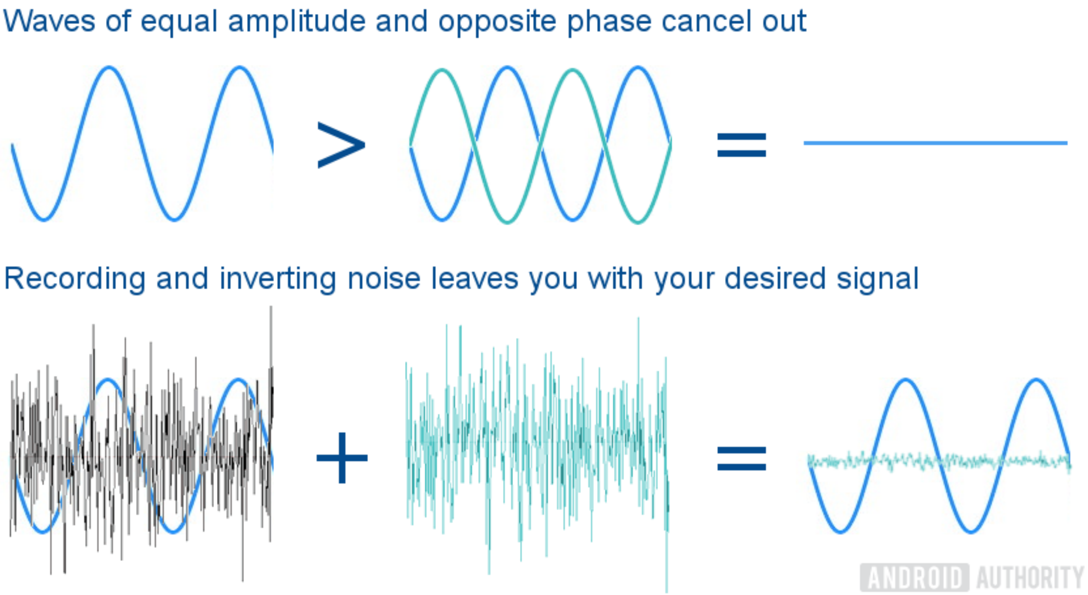

Waves of equal amplitude and opposite phase cancel out
>
=
Recording and inverting noise leaves you with your desired signal
+
=
ANDROID AUTHORITY

Figure 22. Noise cancelling with inverting soundwaves.

After isolating speakers voice next Implementation of this sub system is has two possible approaches to identify deceiving persons by voice.

1. Key points and rules based

    By identifying the key points of the voice and then we are state the prediction of the person is deceiving or not with comparing to the psychological fact which we are founded in psychological literature review.

2. Direct deep learning model based.

    Instead of identifying the key points of voice and comparing it with psychological facts we will only goes with final label of the dataset. Which is the person being Suspicious of not. And train the final machine learning model with those data.

At the moment we will not decide which is the preferred approach because we will decide the final approach later in-between the prototype implementation. Because this decision depends with the accuracy of the result.

2.5.2.3 Implementation of fraud identification with transaction data.

First, a model should be defined. Since this is a classification problem, there are many algorithms that can be used for the model. Logistic regression, naïve bayes classifier, support vector machines, k-nearest neighbor, random forests are some of them. Most suitable algorithm should be chosen based on their characteristics.

After the algorithm is setup, capturing data patterns can be started. This is the heart of modelling. Given features of the data set will be used to understand patterns. Then the prediction phase can begin. To test the reliability of the model, evaluation tests should be done using a different data set.

2.5.2.4 Implementation of Identify frauds with body-language.

After gathering the data there are two main ways to approach this solution one is to use a deep neural network to identify the anomalies by using this technique we may get more accurate results since there are some social cues that humans do miss but in this case we'll need professional who's good at recognizing human behavior patterns and classifying them accordingly there might be thousands and thousands of footage that we might have to review so this is drawback when we go with this approach.

2.5.3 Final System Integration and Implementation.

2.6 System Testing

All system needs to be test before any releases. Testing of this system is another main part of this research. We have categorized the testing into few categories.

- Software Application Test. – Since the final application is a software-based system. So, we need to test application with common software application testing phases.
    - Unit Testing
    - Integrate Testing

- Functionality Testing – All major functionalities must be tested before present the final software application. So, we have two 3 alternative approaches for that,
    - Separate 30% of data from training dataset and train the model with other 70% of data. Finally use this 30% of data to test the functionalities.
    - Deploy the finalize system on LB finance and get some amount of results within specific time duration.
    - Recreate the similar environment at Sri Lanka Institute of Information Technology and recreate some anomalies regular and deceiving persona behaving anomalies then test the functionalities with those data.

  From these 3 approaches we will decide preferring approach later with situation. And update those data with final documentation.

3 DESCRIPTION OF PERSONAL AND FACILITIES

3.1 B.M.C.S. Basnayake - IT16158764

- Project manager, Developer - Managing and leading the research team.
- Project plan creator and maintainer.
- Project progress monitoring.
- Getting data for micro facial expressions.
- Categorize data using knowledge of micro facial expressions when doing a fraud activity.
- Modelling machine learning module.
- Evaluate the predictions using new data sets.

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

- Program manager, Developer
- Meetings coordinator.
- Systems integration coordinator.
- Choosing a suitable environment for the data gathering phase.
- Initializing microphones for voice detection.
- Noice cancellation for isolating the customer voice.
- Labelling data.
- Identifying patterns of voices using suitable algorithms.
- Neural network implementation.
- Prediction evaluation using other data sets which were not used to train the model.
- Integration with other module interfaces.

3.3 N.P. Seneviratne - IT16120280

- Developer
- Communication with the supervisor.
- Provide status reports to the supervisor.

- Collecting data from financial institutes like banks and crime investigation centers.
- Data pre-processing – identify unbalanced data and improper data.
- Cleaning data – getting data which can be given to the model.
- Identifying most influential feature for transaction-based fraud detection.
- Choosing a suitable algorithm for pattern identification.
- Monitor the accuracy of the model using evaluation data.
- Interface implementation.

3.4 Y.C. Tittagalla - IT16129740

- Developer
- Project deliverables maintainer.
- Project scope keeper.
- Interface designer.
- CCTV data collection.
- Identify abnormal body movements in the supervision of a knowledgeable person.
- Label the scenarios as legit or fraud.
- Profile management.
- Categorizing people according to the risk levels.

4 BUDGET

Description	Unit Price	Quantity	Amount
Devices			
Desktop Microphone USB	1,200 LKR	3	3,600
Lavalier Microphone USB/3.5mm	900 LKR	1	900
USB Hub Mini 4 Port USB 2.0	800 LKR	1	800
Kinect Camera 360	7500 LKR	1	7,500
Devices depreciation cost			
Storage Devices	3,000 LKR/Year	1	3,000
High-End PC for Training	24,000 LKR/Year	1 Month	2,000
Services			
Stationary Cost			500
Publication Cost			2,000
Electricity Cost	20 LKR/ KWh	200h	4,000
Cloud Subscription Cost/Host			800
Internet Usage Cost			2,500
TOTAL			**27,600**

Table 4: Budget of the project.

5 WORKS CITED

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

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

[3] 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].

[4] 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].

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

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

[7] 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.

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

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

[10] 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].

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

[12] 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.

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

[14] 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].

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

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

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

[18] 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].

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

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

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

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

[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.