Sri Lanka Institute of Information Technology

PROJECT REGISTRATION FORM

The purpose of this form is to allow final year students of the B.Sc. (Hon) degree program to enlist in the final year project group. Enlisting in a project entails specifying the project title and the details of four members in the group, the internal supervisor (compulsory), external supervisor (may be from the industry) and indicating a brief description of the project. The description of the project entered on this form will not be considered as the formal project proposal. It should however indicate the scope of the project and provide the main potential outcome.

PROJECT TITLE	Fraud detection based on human behavioral patterns.
RESEARCH DOMAIN	ARTIFICIAL INTELLIGENCE
PROJECT NUMBER	112

PROJECT GROUP MEMBER DETAILS:

	STUDENT NAME	STUDENT NO.	CONTACT NO.	EMAIL ADDRESS
1	B.M.C.S. Basnayake	IT16158764	0778511690	chathurangabasnayake@outlook.com
2	Y.C. Tittagalla	IT16129740	0719933688	yasirutit1@gmail.com
3	U.P.A.S.D. Amarasinghe	IT16160330	0779955111	samithdilsh@gmail.com
4	N.P. Seneviratne	IT16120280	0713369305	nirmal.seneviratne@gmail.com

SUPERVISOR

Prof. Chandimal Jayawardena		
Name	Signature	Date

CO-SUPERVISOR

Dr. Dharshana Kasthurirathna		
Name	Signature	Date

CO-SUPERVISOR

Name	Signature	Date

EXTERNAL SUPERVISOR

Name	Affiliation	Contact Address	Contact Numbers	Signature/Date

ACCEPTANCE BY CDAP MEMBER

Name	Signature	Date

PROJECT DETAILS

Brief Description of your 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.

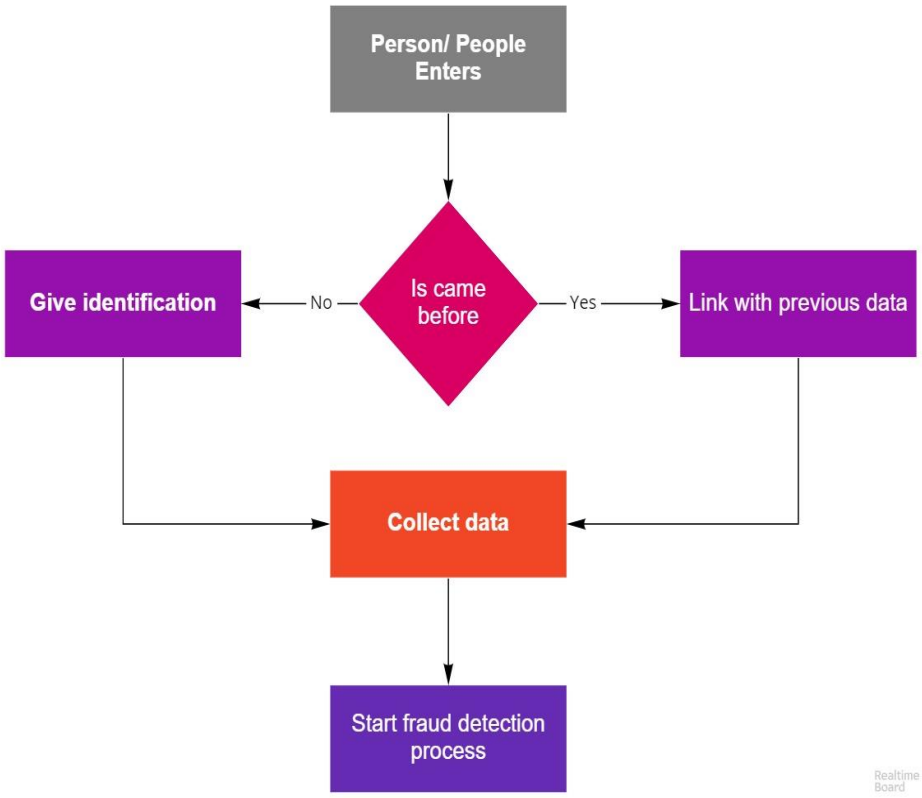
As mentioned above, this can be used in various places for different uses. With this system, we can prevent unexpected fraudulent activities while preventing big losses to the society.

Description of the Solution:

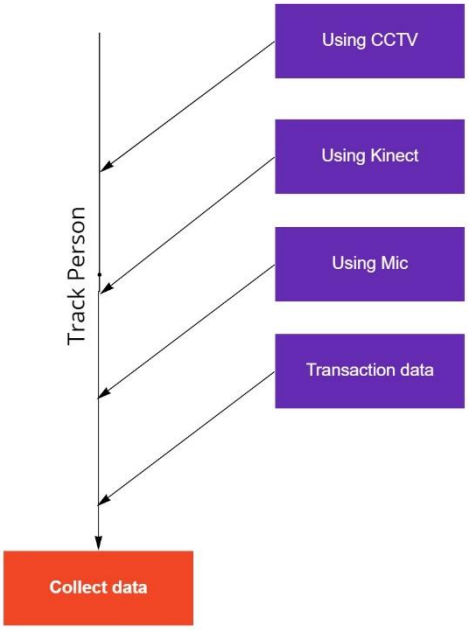
Our solution is mainly focused for Financial Institutes. The aim of this system is to analyze the human facial expressions, behavioral patterns, voice patterns, background environment and human interaction with the environment and identify the possible anomalies.

- 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.

High level diagram of the system



Data collecting process



Main expected outcomes of the project:

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.

WORKLOAD ALLOCATION

MEMBER 1	.....B.M.C.S. Basnayake - Facial Expression Analysis.....

Humans can identify or inspect, whether this user is abnormal or not by looking at person history of facial data and real-time facial data using a Camera aim towards to the user's face or can identify micro expressions using Kinect camera or something like that.

Facial data can be categorized as,

- Expressions and Micro-Expressions.
- Emotions.
- Eye movement.

In this part we are trying to identify or find anomalies of User's facial data. By doing this cashier or officer can give more attention to the user and probably reduce fraudulent activity.

MEMBER 2	..... Y.C. Tittagalla – Body Language Analysis.....

Humans can identify fraudulent activities by looking at another person's body-language and gestures there are highly paid individuals whose job is to find those abnormal behavioral patterns. So, in this research part we are trying to automate this process by develop software solution to identify frauds with human body-languages and fraudulent movements from CCTV camera footages and tracking a person between multiple CCTV camera.

By using this method, we will mainly categorize the persons in the vicinity according to a risk level and those who have 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

MEMBER 3 ……U.P.A.S.D. Amarasinghe – Voice Analysis ……

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)

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.

MEMBER 4 ……N.P. Seneviratne - Transaction Analysis……

In this module, 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 module identifies those unknown frauds too, 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.
- Current trends, seasonal changes

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

EVERY MEMBER	All

Track a person, combine all above parts (real-time and history) and give single percentage or level of confidence about the user. Which he/ she can be "**Suspicious**" or not.

In order to do that we need to find how much each above factors can affect to the final result.

Examples:

- User never came to the cashier or to meet an officer.
  - Facial recognition is not affecting to the final result.
- User directly came to talk with officer or casher.
  - Facial recognition can more effect to final result than the transaction data.

DECLARATION

"We declare that the project would involve material prepared by the Group members and that it would not fully or partially incorporate any material prepared by other persons for a fee or free of charge or that it would include material previously submitted by a candidate for a Degree or Diploma in any other University or Institute of Higher Learning and that, to the best of our knowledge and belief, it would not incorporate any material previously published or written by another person in relation to another project except with prior written approval from the supervisor and/or the coordinator of such project and that such unauthorized reproductions will construe offences punishable under the SLIIT Regulations.

We are aware, that if we are found guilty for the above-mentioned offences or any project related plagiarism, the SLIIT has right to suspend the project at any time and or to suspend us from the examination and or from the Institution for minimum period of one year".

	STUDENT NAME	STUDENT NO.	SIGNATURE
1	B.M.C.S. Basnayake	IT16158764	
2	Y.C. Tittagalla	IT16129740	
3	U.P.A.S.D. Amarasinghe	IT161603300	
4	N.P. Seneviratne	IT16120280	