Fraud Detection based on Human Behavioral Patterns.

B.M.C.S. Basnayake
U.P.A.S.D Amarasinghe
Y.C. Tittagalla
N.P. Seneviratne

Faculty of Computing,
Department of Software Engineering,
SLIIT
Malabe, Sri Lanka.

I. 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. Especially 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.

II. Introduction

A. *What is a Fraud ?*

According to the world-renowned Oxford dictionary, 'Fraud' is defined as below.

"Wrongful or criminal deception intended to result in financial or personal gain [1]"

The Cambridge dictionary definition:

"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].

B. 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.

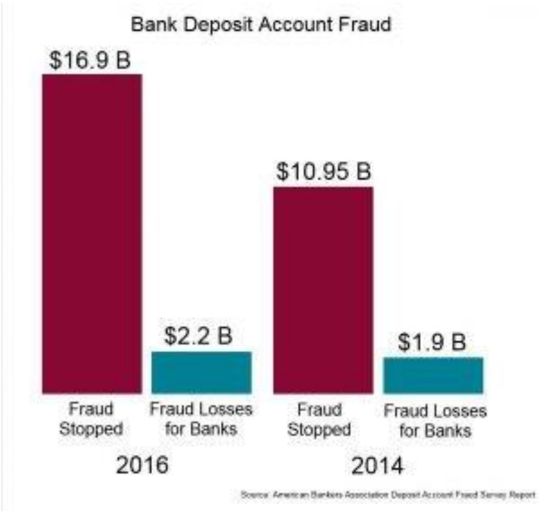


Fig. 1. Bank Deposit Account Frauds

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 society as illegal arms sales, drug trafficking, smuggling rates are going higher.

III. Background Study/Literature Review

C. Markov modelling for randomly changing systems

Fraudsters do not use the 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 events that preceded it. Hence, the model will use real time data to be updated and to learn about new mechanisms of frauds. [4]

D. Enterprise Fraud Detection Solution – WSO2 analytics platform

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. [5]

E. 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 people's voice and the stress level and verify the truth. It is called VSA (Voice Stress Analyzer) 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 to their official website. [6]

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.

F. 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]

People can separate different voices from different people on crowded environment with their brain. They are manually muting the other people’s sound and focusing an individual speaker’s voice. This is called CockTail Party Effect. [8]. They were 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]

IV. Methodology

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.

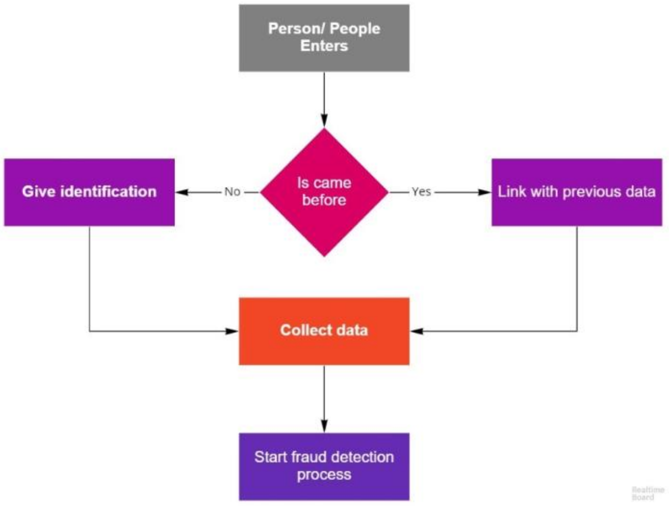


Fig. 2. High level diagram of the system

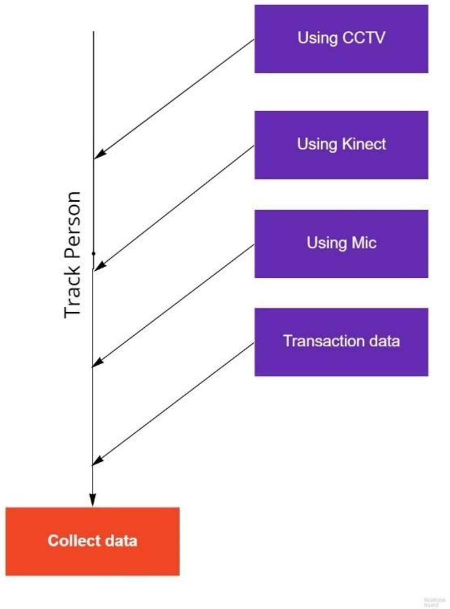


Fig. 3. Data collecting process

G. Facial Component

Humans can identify or inspect, whether a user is trying to do 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 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 tries to hide their true intentions from others or simply when someone tries to 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 is doing the transaction can give more attention to the user(customer) and probably reduce or prevent fraudulent activities from happening.

H. Body Language Component

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 footage. In this research we have decided to 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.

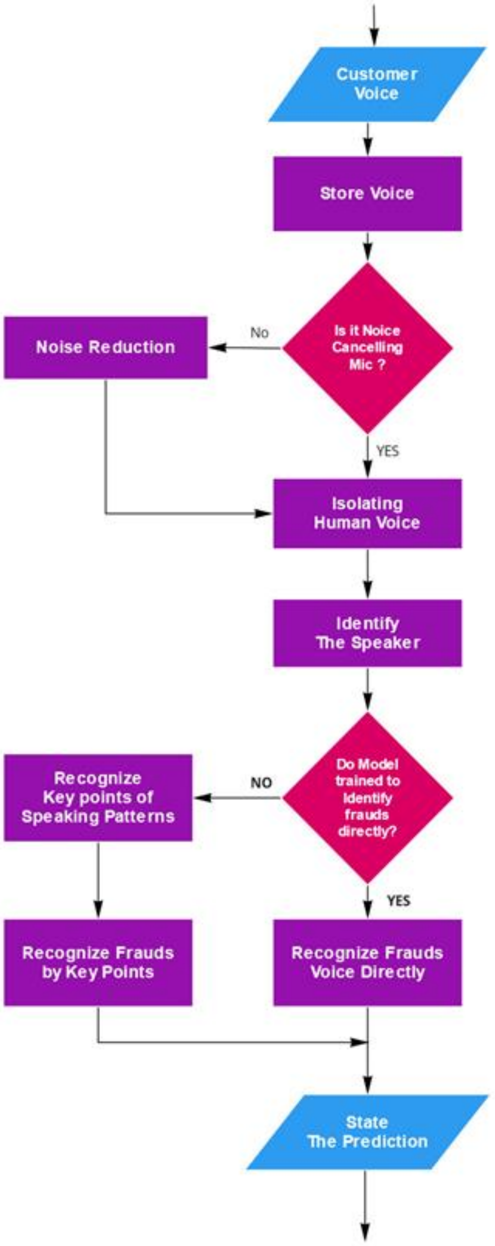

Customer Voice
Store Voice
Is it Noice Cancelling Mic ?
No
Noise Reduction
YES
Isolating Human Voice
Identify The Speaker
Do Model trained to Identify frauds directly?
NO
Recognize Key points of Speaking Patterns
YES
Recognize Frauds by Key Points
Recognize Frauds Voice Directly
State The Prediction

Fig. 4. Voice Capture

I. Voice Component

Like human able identify frauds, lies, deceits or scams by another person's voice or speaking patterns This product is able to identify lies and fraudulent activities. 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 identify deceits with sounds based.

Sound based frauds detecting also focused on key points and rules based (Based on psychological studies) 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 product will be working on crowded environment before analyzing the sound clip we have to preprocess the sound clip by cancelling the background noises and identify isolated customer voice with fine details of the sound. Then trained neural network model able to analyze the sound clip and able to detect lies, this part of the solution can state a prediction for suspicion of certain customer by their voice. Overall flow shown in Figure 4: Voice Capture

J. Transaction Component

To identify the transactions of a fraudster, a trained machine learning model is needed. Training this model is done by using data sets which are labelled. To select a suitable machine learning algorithm, we have to test by trying out different algorithms. After training the model, it is used by the front end angular component to predict the reliability of a transaction.

As the first step, it is necessary to find a suitable dataset to train the transaction model. It is very rare to find actual transaction details online because of the security and confidentiality reasons. One actual dataset available is the credit card fraud detection data set in kaggle. [10] But as the description of the dataset say, it is a set of anonymized transactions. Because of that, there are no column descriptions for the dataset. This does not matter when the machine learning model is trained. But when a real world scenario is applied to this model, we can not determine which data we have to supply to the model to get a prediction. Because of that reason, we have used a synthetic financial dataset to detect fraudulent transactions. [11] It has generated the transaction using a simulator called PaySim. PaySim uses aggregated data from the private dataset to generate a synthetic dataset that resembles the normal operation of transactions and injects malicious behaviour to later evaluate the performance of fraud detection methods.

The main problem in a fraudulent transaction data set is it is extremely unbalanced. When there are 284315 number of genuine transactions in the set, there are only 492 fraudulent transactions. This leads to a bias of the classification model. To overcome and unbalanced dataset, techniques can be used ie: oversampling, undersampling, SMOTE (Synthetic Minority Oversampling Technique). SMOTE randomly creates synthetic records to oversample the dataset hence balancing the fraudulent and genuine transaction record numbers.

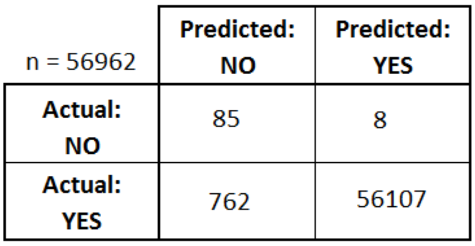
For the training of the machine learning model, logistic regression algorithm was used. Logistic regression is mostly used for classification problems ie: final oupt is a Yes or No. In this case, Fraudulent or Genuine will be the output.

After training the model, there should be a way to persist the model for future use without having to retrain. A package called Joblib is used to do this task. *joblib.dump* persist an arbitrary Python object into one file. After dumping the model, it can be hosted in an api using flask (exposing the endpoint).
access from frontend

V. Results

K. Transaction Component

There are many ways to measure the accuracy and reliability of a machine learning model. Confusion matrix is a regular metric used in classification models.



n = 56962	**Predicted: NO**	**Predicted: YES**
Actual: NO	85	8
Actual: YES	762	56107

Fig. 5. Transaction model confusion matrix

Another type of metric is classification accuracy. It is defined as below.

$$\textbf{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

TP + TN = 56192
TP + TN + FP + FN = 56962
Hence classification accuracy = 56192/56962
= 0.9865

0.9865 can be considered a promising accuracy for a classification model. This model can be used for real world scenarios to predict whether a transaction is fraudulent or genuine.

Beside the transaction based fraud detecting component we have three other human behavioral patterns based fraud identifying components to identify that a transaction is fraudulent. Unlike the transaction module, these three components need more data sets to improve the accuracy of this system. Transaction-based Fraud detection component 90% accuracy but other three human behavior components has less than 50% of accuracy. here is the accuracy of each component of human behavior components.

L. Facial expressions Component

In this component we have successfully able to identify each key point of many facial expressions we have listed above in our research paper.. For example blinking eyes, covering face, covering mouth, touching the fore heads kind of keypoint has 99% of accuracy rate.

Since we have been able to collect many dataset from Internet human expression identification model has high accuracy rate we have tested using test data set it has 98% of accuracy in this system. When it comes to identifying lies with this component those key points are not occurring more often. Since this issue we have less than 50% accuracy rate of identifying lies with facial expressions.

M. Body language Component

In this component we have Used surf algorithm to track the person Identified the actions of that person. Because of this algorithm check in the person is more accurate than before and that action identifications Also has Accuracy rate.

same as the facial expression component this component also identifies body language very accurately. This company has more than 80% of actions identifying Accuracy rate. But when it comes to doing a fraud most of these listed actions Not occurred Very often. So identify frauds with this component also has less than 50% accuracy rate for now.

N. Voice signal Component

In this component we have used multi class classification model to identify each voice best key points for detecting frauds using voice signals. Multi class classification model also has very accuracy rate it can identify most of voice based key points lister above in the research paper. It has 80% accuracy rate of identifying and voice based key points. But like the other two human behavioral pattern identifying components this component also has lower accuracy rate of identifying lies using voice signals. When people lie, they don't do these things. Some of these key points can't be captured by microphone because of the noise in the background. Because of this issue accuracy rate of detecting lies from this module is less than 30%.

Finally we have used an ensemble method to combine each of these components' results to get the final result. Since we have more accuracy rate from transaction-based fraud detection component we are taking 50% of results from that component. Since facial expression based fraud identifying component and body language-based fraud identifying component has equal accuracy rates, we are taking 20% of results from each of these two components. Finally from The voice based fraud identifying component we are taking 10% of results from this component.

Component	Current Accuracy	Combine Rate
Transaction Based Component	95%	50%
Body Language Component	50%	20%
Facial Expression Component	50%	20%
Voice Signal Component	30%	10%

According to this combining rate theoretically accuracy rate of theses 4 components is 70.5%.

Combined Accuracy Rate = 95% x 50% + 50% x 20% + 50% x20% + 30% x 10%

= 70.5%

VI. Conclusions

Since transaction-based frauds identifying component has high accuracy rate we don't have much to implement this component but other three component has very low accuracy rate we have to improve these three components Until it achieve more than 80% of accuracy rate.

Each of these three human behavioral pattern identifying component needs more data to improve the accuracy rate. With more data set it is possible to achieve an 80% accuracy rate in these components. and also voice based fraud identifying component needs to fine-tune voice clearing part to improve the accuracy rate. currently breathing sound cannot be captured by the microphone, because of the background noise. so Voice clearing algorithm needs to fine-tune to achieve the high accuracy rate. Secondly facial expressions based fraud identifying component is not working properly in low lights. we have two options to solve this issue one of those is to upgrade cameras to high end products. Other one is to give more light in counter area of the bank. This problem also occurred in body language based fraud identifying component when there is low light situations identifying action is also difficult.For this one also need to upgrade cameras of the target location or need to light up the whole area.

After improving accuracy rates of all components we can combine these results equally.

VII. References

[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] 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.

[5] 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].

[6] X.-V. Team, "X13-VSA Voice Lie Detector," [Online]. Available: https://lie-detection.com/. [Accessed 8 3 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] Anonymized credit card transactions labeled as fraudulent or genuine. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud

[11] Synthetic datasets generated by the PaySim mobile money simulator. [Online]. Available: https://www.kaggle.com/ntnu-testimon/paysim