Find Transaction Fraud Using Face Detection and Hidden Keyboard

Kalyani Wankhede[1], Madhav Tengetol[2],Rutuja Tak[3] Prof. Nilesh Wani

[1,2,3]Student, Department of Computer Engineering, DY Patil School of Engineering Academy, Ambi, Pune, Maharashtra, India

---***---

Abstract - The proliferation of credit and debit card and online transaction, the growing popularity of internet and mobile banking, and the increasing use of mobile phone as a payment device. However, the security of e-banking has received attention due to the fraudulent behaviour of fraudsters. Throughout this paper, The different techniques and models used for e-banking security were ranked in this study based on an expert opinion. we've an inclination to propose logical graph of BP (LGBP) that will be a complete order-based model. Here we tend to area unit able to realize Face by pattern viola jones and LBP acknowledge formula for face detection as we tend to use invisible keyword sequence for authentication of OTP.

Key Words: Behaviour profile, e-commerce security, face detection on line dealing, face structure, Face Detection, Invisible Keyboard Sequence

1.INTRODUCTION

E-banking gives customers a lot of satisfaction in terms of getting a better service quality. it also gives banks a competitive advantage over the other players in the sector. Fraud is a serious problem for banks too, and there are rules they must follow when it comes to handling unauthorized transactions.the absence of adequate e-banking security has kept many people away from the service till today.

In this paper, we've an inclination to propose logical graph of BP (LGBP) that will be a complete order-based model to represent the relation of attributes of dealings records. supported LGBP and users dealings records we tend to area unit able to cipher a path-based transition likelihood from associate degree attribute to a distinct one. Here we tend to area unit able to realize Face by pattern viola jones and LBP acknowledge formula for face detection as we tend to use invisible keyword sequence for authentication of OTP. The keyword sequence modification once. At constant time, we've an inclination to stipulate associate degree knowledge entropy-based diversity constant thus on characterizes the variability of dealings behaviors of a user.

2.METHODOLOGY

This paper proposes a method for credit card transaction system which will make use of face recognition and face detection technology, using **Viola–Jones** and **Local Binary Pattern** (LBP) algorithm. The main problem faced by credit card users is attack to lot of privacy issues such as credit card. we are proposing a system that will reduce the risk of credit card frauds. The system we are proposing will match the image of user's face with dataset of respective user. A database will be maintained for authentication purpose. If the image matches, that means user is genuine and he will be allowed to proceed otherwise, the user will be denied to do the transaction.[2]

It is easy for fraudsters to hack your internet banking password by capturing your keystrokes on your keyboard. Virtual keyboard is actually not necessary in the internet banking.. It protects you from pressing any key on that computer or laptop.In our project User can enter correct keys when the user will have the sequence of the shuffled keyword. Here the sequence of the keyword will be sent to the users registered email id and OTP will be sent to mobile number.[4]

3. RELATED WORK

In this project, we propose a method to extract users BPs based on their transaction records.It is used to detect transaction fraud in the online shopping scenario by using the face detection. In addition, also we have used Viola-Jones Algorithm and LBP Algorithm for face detection. we tend to use invisible keyword sequence for authentication of OTP.
In existing system many banking sectors victimization the Signature based transactions there is likelihood of duplicate signature by someone. entirely OTP verification is accessible on mobile, but someone's making an attempt to induce your phone and sees OTP and transfer money from one account to the another account. Even by the upper than two mentioned methodology the fraud dealings is up to the mark. we've an inclination to in addition track fraud user with location by mackintosh address of the user laptop computer transportable or computer that have last dealings successfully.

4. LITERATURE SURVEY

There are many techniques and methods carried out online Transactions Fraud. This research results demonstration and usefulness of queing model on providing guidance on identification identifying Frauds during online transactions. Most of the people store their password and personal information very confidentially but sometimes it may be stolen by someone unexpectedly

Project Title:
Transaction Fraud Detection Based on Total Order Relation and Behaviour Diversity (2018)[1]
Technique:
An important way of detecting fraud is to extract Behaviour Profiles (BP) of users based on historical transaction record and then verify incoming transaction is fraud or valid. Markov chain models are popular to represent BP's of users,, which is effective for those users whose transactional behaviour are stable.

Project Title:

Detection of Fraud in online credit card Transactions (2016) [3]

Technique:

In this paper the algorithm calculates the threshold value based on previous transactions and classifies them into three categories(Low,High,Medium).

The Current Transactions is compared with threshold value and on the basis of the calculated probability it is classified as fraud or not.

Speed of the software is slow and can be enhanced by implementation of algorithms of less complexity.

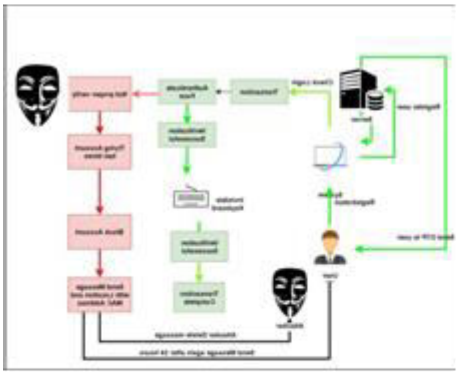
5. SOFTWARE REQUIREMENT

- Software requirement consist of database, web application program and server.
- Database Requirement : MySql , Xamp Server
- Professional Environment: Eclipse, Anaconda
- Language used : Java, Python
- Operating system: Windows OS

6. HARDWARE REQUIREMENT

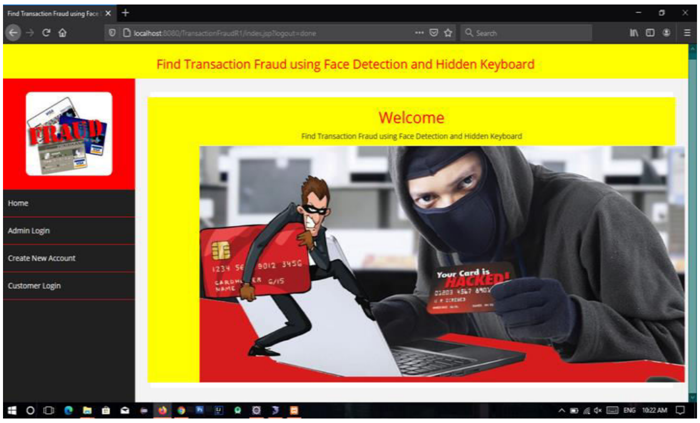
- The basic requirement is a personal computer on the server side, which will store the database, RAM , Keyboard.
- System Type: 64-bit or 32-bi
- Processor: Intel core i5, 2 GHz
- Random Access Memory (RAM): 8 GB
- Storage Capacity: 1 TB
- IO device: mouse and keyboard
- Device Name: Laptop or Computer

7 . SYSTEM ARCHITECTURE



8. RESULTS AND DISCUSSION

Our project of Find Transaction Fraud Using Face Detection and Hidden Keyboard was successfully tested on local machine. This is our Welcome Page.



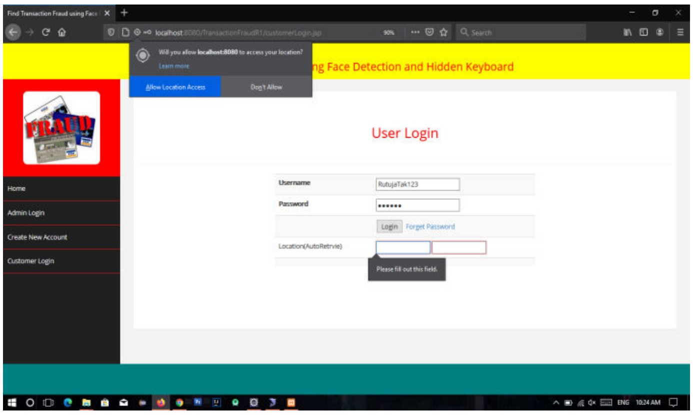
Find Transaction Fraud using Face
localhost:8080/TransactionFraudR1/index.jsp?logout=done
Search
Find Transaction Fraud using Face Detection and Hidden Keyboard
FRAUD
Home
Admin Login
Create New Account
Customer Login
Welcome
Find Transaction Fraud using Face Detection and Hidden Keyboard
Your Card is HACKED!
ENG
10:22 AM

Fig a. Welcome Page

first step is to register successfully on the login page. we've an inclination track fraud user with location by mackintosh address of the user laptop.

User Functionality:-

- User register and login to the system.
- Transfer amount to users new or existing.
- Select amount and pass face detection
- Enter correct OTP
- Get Massage about transactio

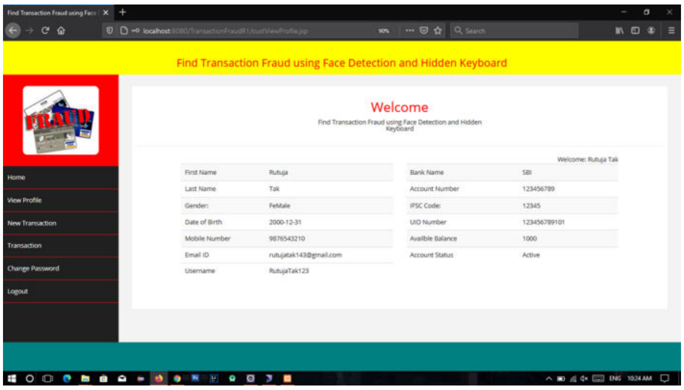


Find Transaction Fraud using Face
localhost:8080/TransactionFraudR1/customerLogin.jsp
90%
Search
Will you allow localhost:8080 to access your location?
Learn more
Allow Location Access
Don't Allow
ng Face Detection and Hidden Keyboard
FRAUD
Home
Admin Login
Create New Account
Customer Login
User Login
Login
Forget Password
Please fill out this field.
ENG
10:24 AM

Username RutujaTak123
Password ••••••
Location(AutoRetrvie)

Fig b. User Login Page

This is User Database.



Find Transaction Fraud using Face
localhost:8080/TransactionFraudR1/custViewProfile.jsp
90%
Search
Find Transaction Fraud using Face Detection and Hidden Keyboard
FRAUD
Home
View Profile
New Transaction
Transaction
Change Password
Logout
Welcome
Find Transaction Fraud using Face Detection and Hidden Keyboard
ENG
10:24 AM

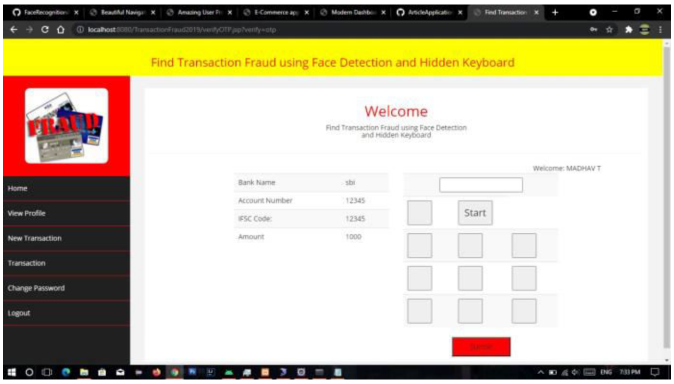
Welcome: Rutuja Tak

First Name	Rutuja	Bank Name	SBI
Last Name	Tak	Account Number	123456789
Gender:	FeMale	IFSC Code:	12345
Date of Birth	2000-12-31	UID Number	123456789101
Mobile Number	9876543210	Availble Balance	1000
Email ID	rutujatak143@gmail.com	Account Status	Active
Username	RutujaTak123		

Fig c. User Data

User can enter correct keys when the user will have the sequence of the shuffled keyword. Here the sequence of the keyword will be sent to the users registered email id and OTP will be sent to mobile number.

The numbers on keyboards is invisible.



Find Transaction Fraud using Face Detection and Hidden Keyboard

Welcome

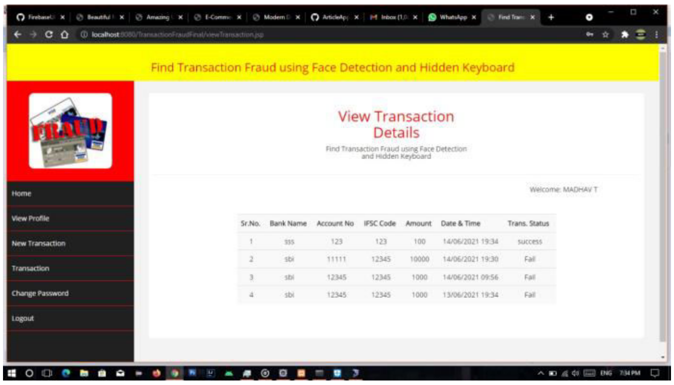
Find Transaction Fraud using Face Detection and Hidden Keyboard

Welcome: MADHAV T

Bank Name	sbi
Account Number	12345
IFSC Code:	12345
Amount	1000

Fig d. Invisible Keyword

This is the transaction details of users: -



Find Transaction Fraud using Face Detection and Hidden Keyboard

View Transaction Details

Find Transaction Fraud using Face Detection and Hidden Keyboard

Welcome: MADHAV T

Sr.No.	Bank Name	Account No	IFSC Code	Amount	Date & Time	Trans. Status
1	sss	123	123	100	14/06/2021 19:34	success
2	sbi	11111	12345	10000	14/06/2021 19:30	Fail
3	sbi	12345	12345	1000	14/06/2021 09:56	Fail
4	sbi	12345	12345	1000	13/06/2021 19:34	Fail

Fig e.Transaction Details

9. CONCLUSIONS

Our proposed project has been designed for the purpose of reducing the credit card frauds that may occur during online payment transaction. There is no need of specialized hardware for installing this system. It just need a computer and a camera for face reorganization.
The system is reliable and efficient mode of transaction process. The virtual keyboard plays a crucial role in the working of our project, therefore the we avoid unnecessary frauds related to password hack.

10. REFERENCES

[1] Lutao Zheng, G Liu, C Yang, Transaction Fraud Detection Based on Total Order Relation and Behaviour Diversity, 2329-924X, IEEE, 2018

[2] T Dhikhi"2018 Credit card fraudulent Transaction Detection IEEE International Conference"

[3] Deepak Pawar,Swapnil Rabse, Naina Kaushik, Detection of Fraud in online Credit Card Transactions, IJTRA, ISSM:2320-8163, Mar-Apr-2016

[4] Shweta Jamkavale, Ashwini Kute, RupaliPawar, Komal Jamkavale4,PrashantJawalkar,Secure Transaction By Using Wireless Password with Shuffling Keypad, IJRASETVolume 4 Issue X, October 2016.

[5] P.VIOLA and M.j.Jones, Robust real time face detection ,international journal of computer vision,57 (2004),

[6] Global Online Payment Methods: Full Year 2016, GmbH & Co. KG,Berlin, Germany, Mar. 2016

[7] Random forest for credit card fraud detection, Zheng Lutao and Wang Shuo 2018 *IEEE 15th International conference*

[8[Method for secure credit card transaction, Nader Nassar, Grant Miller, International Conference, 2013.

[9] Credit card fraud detection using machine learning, John williams, 7th IEEE International Conference, 2017.

[10] N. Abdelhamid, A. Ayesh, and F. Thabtah, Phishing detection based associative classification data mining, Expert Syst. Appl., vol. 41, no. 13, pp. 59485959, 2014.

AUTHORS PROFILE

Mr. Tengetol Madhav Ramrao pursuing Bacholar of Computer Engineering from Dr D Y Patil School of Engineering Ambi Pune, Maharashtra,India

Ms. Wankhede Kalyani C. pursuing Bacholar of Computer Engineering from Dr D Y Patil School of Engineering Ambi Pune, Maharashtra,India

.

Ms. Tak Rutuja B. pursuing Bacholar of Computer Engineering from Dr D Y Patil School of Engineering Ambi Pune, Maharashtra,India