A Novel Method for Securing Online Banking Transactions

ASHIMA ARYA[1], PAYAL CHHABRA[2], NEHA BHATIA[3], BHAWNA KUKREJA[4]
[1, 2, 3, 4] *Assistant Professor, Panipat Institute of Engineering & Technology, Samalkha, Panipat*

Abstract— One of the primary responsibilities of a financial/banking institution is the keep its clients secured against thefts. Protection against thefts is the primary reason why people choose to keep their money with banks instead of keeping it home, in their safe. Considering security as our primary target we have created this banking application which uses two-phase security mechanism for secure transaction. Firstly, via verifying OTP(One Time Password), secondly via recognizing the face and iris of the customer. Another reason why people choose banks in a secure environment is to easily trade money with online portfolios, debit cards, credit cards, smart cards, etc. The third option provided here is a track record of finding the location of a transaction that has been made, which may keep customers safe from fraud or at least locate the location of the theft.

Indexed Terms-- Face Recognition, Machine Learning, Geo-location, Secured Mobile Banking, IP address, ISP, Neural Network

I. INTRODUCTION

As paper money grew, the threat of robbery increased and its management became increasingly difficult. So the banking institutions got in line. For decades role of financial institutes for to create, circulate and safeguard money, which still is, but earlier people had to wait in line or long queues for hours to get or loan , deposit money and many more work related to banks. [1].

People used to send money orders to give their loved ones who were far apart money. Today with innovation in technology e-money came into the picture. It is an easier way to transact. You can get rid of big queues and get money. Pay bills without even carrying money in your pockets.

Internet Banking -Internet banking [2] is the most convenient way to transfer your money to someone else account. It is a revolution; you can pay any kind of bill using your money online. It can lead you to be cash-less environment. You don`t even have to change the currency while traveling to another country.

- It makes your life hassle-free.
- You can go out with as limited cash as you want without being concerned about getting robbed.
- No need to remember total count of money or get a risk.

- Online Banking Security Problems [3]

Billions of financial records transactions arise online every day of the year, 24 *7, as human beings grow in consciousness they begin shifting in the direction of cashless or a digital mode of transaction. Now you can not only move with less cash in your pockets, but you are free from theft as well. But is your money completely safe? Are all the transactions you make secure? Is your integrity always protected?

The problems with online transactions are of three sorts:

Sort 1: Programmer`s error- The vulnerabilities because of errors made up by programmers for example buffer overflow, might provide a backdoor to malicious users to find a way to earn profits.
Sort 2: Bank`s flaw- Banks no longer specify or ask the organizer to hold strict security.
Sort 3: Customer`s mistakes- Customers aren`t always aware of their security, they sometimes share their information with misguided phone calls. People create passwords for their applications either too short which is too easy to identify or too long, which they usually forget.

Hacking ways are also increases with security increases for malicious users. It is easy for hackers to hack into the accounts of users or even the bank`s database. It is easy to guess passwords with attacking the vulnerabilities, also there are tool kits in Kali Linux to guess the passwords. A dictionary attack usually helps to find out the passwords.

If you are using face recognition for security purpose then it would be very easy to get into the system with face recognition by displaying a picture, if there is no life in biometric verification it does not help, anyone can show a customer photo and can get authorization.

II. WORK IN PROGRESS

E-banking

Digital banking is also called E-banking, digital banking, online banking, or net banking, in which electronics and telecommunications provide banking services to the customer online. By using net banking, a client can access his / her account to avail of all the bank-related services via online mode. It has three different categories:

- *Level* 0 provides primary or basic service through their websites. Meanwhile many more services are also available on their applications as well.
- *Level 1 There is no fund-based transferring of money allowed. This is through applications. At this level, the customer can avail of the services through applications. Services like balance checking etc.*
- *Level 2- Level 2 allows customers to operate various services like fund transfer, bill payment, redeeming of securities and purchases, etc.*
- More or less, almost all the banks provide their customers to avail the facility of internet banking through the internet or E-delivery channels.
- Modern banks care about E-banks only, they don`t have any physical branch, they operate through applications, anywhere in a country.

- Authentication

Authenticity means determining who a person or thing is or what they call themselves. Authentication is a technology that provides control of access to systems by checking if the user credentials match the data stored on the authorized user website on the data verification server.

Users can usually be identified by the user ID, verification is done when the user provides information, for example, a password, in case it matches the user ID. Most users are familiar with password usage, which is a very important piece of information known only to the legitimate user, known as the information verification feature. Other verification features are used for two-factor authentication or multifactor (MFA), described further.

- Biometrics

It refers to the matrix of various biological features, where bio means dimensions of the human body and features and, matrix refers to a collection. So biometrics is a term that refers to the matrix of body measurements which performed calculus. Official user of the account is verifies and validates by Biometric authentication. Supervised group can identified individual by using various matrix algorithms.

Identifiers of the biometrics are distinctive, characteristics are measurable, they are used to identify and label the individuals. Biometric identifiers are usually categorized as one of the two, physiological and behavioral characteristics.

The physiological type of characteristic of the body is concerned with the shape of that body. Examples of this type include fingerprints, palm veins, DNA, facial recognition, hand printing, hand geometry, iris vision, retina, and scent /odor. Whereas the behavioral type of character is related more to the pattern that the behavior of any person follows, examples include traits like rhythm, pitch, gait, and voice.

- Chatbot

A chatbot (abbreviated as a bot) is software designed to provide an online communication between users, according to Oxford Dictionaries. Using robots and Artificial Intelligence (AI), a chatbot can help customers without the need for a customer service agent on the other hand. Chatbots can range from simple to very smart depending on how they are

organized. A rule-based chatbot can only handle explicit commands, while a chatbot using machine learning will be clever with each interaction. Chatbot in banks are used by large companies such as Bank of America and American Express.

III. E-BANKING FACE AUTHENTICATION SCHEME

Working of biometric authentication Face recognition [4] is a professional way to identify a person's face. The proposed face recognition system uses biometrics to map face features from a photo or video. It compares the information with known face databases to obtain the same. In this methodology, user will use their faces to access their bank accounts to gain instant access and improve security. So, our program starts with getting a photo to put on a webcam. After that this method is used to process the facial features and then features from the detected face are constructed to create a dataset. The detected face is recognized and calculated to find whether the face matched or mismatched.

- Face Detection

Some features like Local Binary Pattern (LBP) and Haar are used by AdaBoostclassifier [5] and the Support Vector Machine (SVM) section is used with Histogram of Oriented Gradients (HOG) features for face testing.

Flexible stand-alone images are processed by Haar which produces an external set of features and then decomposes a crumbling tree of advanced dividers for a strong and quick rectangular distortion by advanced AdaBoost algorithm.

Fig1: Face detection

The original LBP operator labels the pixels of a picture by thresholding the 3-by-3 neighborhood of every pixel with the middle pixel value and considering the result as a binary number. Each face image is often considered as a composition of micro-patterns that may be effectively detected by the LBP operator. To believe facial information, facial images are divided into small N-circular spaces T0, T1, ..., TN. LBP histograms extracted from each sub-region are then grouped into a single histogram, developed with the area defined as:

$$H_{i,j} = \Sigma_{x,y} I(f1(x,y)=i)\ I((x,y)\epsilon Tj) \quad (6)$$

Where i = 0... L-1; j = 0... N-1..The extracted histogram describes the local texture and global shape of facial images.

SVM classifier is been used with HOG features for face detection. HOG outperforms wavelets and degree of smoothing before calculating gradients damages. To perform SVM algorithm training, we'd like to formulate the statement to a different space that captures explicitly the dissimilarity between two facial images. The results summary of the above methods is stated below.

Dataset	Detection		
	Adaboost		SVM
	Haar	LBP	HOG
[1]	99.41%	95.22%	92.67%
[2]	98.34%	98.45%	94.11%

[3]	98.30%	69.80%	87.90%
[4]	96.90%	94.16%	90.58%
[5]	90.66%	88.30%	89.19%
Mean	96.72%	89.18	90.89

Table1: Face detection results summary

Face Recognition

Eigen's faces are considered to be a 2-D facial recognition problem; the face is usually straight and forward. This is why 3-D information about the face is not required which reduces the complexity slightly. It transforms facial images into a gaggle of basic functions which are the main components of facial images that require directions where it works best to represent data. This is commonly helpful in order to reduce the calculation effort. Discrimination line analysis is primarily used here to reduce the number of traits to a controlled number prior to recognition because faces represent a large number of pixel values. The new dimension can be a linear combination of pixel values, forming a template. The combination of lines obtained using discrimination by the Fisher line is called Fisher's face. LBP is an order set for binary pixel intensity comparisons between pixels in the center and eight pixels around it.

$$LBP\ (x_a,y_a) = 7\ \Sigma n=0\ s(i_m - i_a)\ 2n \quad (6)$$

In which i_a corresponds to center pixel (x_a,y_a), i_m to the worth of 8 surrounding pixels, function f(x) is as follows:

$$f_{(x)} = \begin{cases} 1 \text{ if } x>=0 \\ 0 \text{ if } x<0 \end{cases} \quad (7)$$

Dataset

Five data sets were used for the above assessment. In the database, a blue background face collection; no head scale and lightweight variation but with minor changes in head rotation, inclination, inclination, facial expressions, and significant changes in speech. In the database, a complex facial background; great head variation; slight variation of head rotation, tilt, tilt, and rotation; other interpretations in the facial area and significant slight variations due to the time of the object in the undifferentiated light. In the database, a blank back face collection; small head variations; significant fluctuations in head rotation, inclination, inclination, and greater variation in speech; slight translation in the facial area and lightweight variation. In the database, a fixed back face collection with a small head variation and a lightweight variation; great variation in sequence, inclination, inclination, display, and face shape.

Fig2: Dataset [8]

- Chatbot for user's interaction

A Chatbot[9] (also known as a bot for short) is a computer program that can mimic conversation with human users on the internet, it is a code that has the capabilities of conversing online with humans using robotics and Artificial Intelligence (AI), a Chatbot can assist you without the need for any customer service agent on the other end. Chatbot ranges from very basic to highly intelligent depending on the way they are programmed. A rules-based Chatbot is only efficient in handling very specific commands, whereas a Chatbot that uses machine learning algorithms is trained to get smarter with each interaction they make. Chatbots in banking sectors are being used by major brands such as Bank of America and American Express.

- Location tracking of a device using its IP Address

The location of the customer who performed his last transaction can be tracked using his device's IP

Address. The mapping of IP addresses on the Internet from a connected device is known as IP geolocation. The Internet Assigned Number Authority (IANA) is responsible for allocating large blocks of IP addresses to Regional Internet Registries (RIR) operating globally. These RIRs then provide IP address blocks to Internet service providers (ISPs) who then provide IP addresses to businesses, organizations, or individual clients.

A common way to deal with IP Geolocation is to build and maintain a website that contains relevant data. But such non-automated methods are not desirable. Problems that may arise can be IP addresses that are enabled and do not stand and thus the website needs to be updated from time to time. Switching from IPv4 to IPv6 will greatly increase the challenge.

- Methods of IP Geolocation[10]

Delay-Based Pathways: These create a target environment by using relationships between internet delays and local distance.

Topology-based Geolocation Methods: within a targeted geological environment, topology-based geolocation methods also improve topology in addition to the link between internet delays and local distances.

IV. CONCLUSION

In this study, we have introduced an in-depth face-to-face learning program to provide secure and reliable online banking. The introduction of in-depth belief networks that prove facial authenticity on devices has been shown to be effective in increasing security levels when performing banking operations. It is anticipated that the hiring of deep-rooted face-to-face networking networks could increase the level of security of banking applications.

The future work on this paper is about creating new and efficient ways to make e-banking safer, much more efficient, and secure. Thus, making people trust it even more and taking actions against malicious users. First, facial recognition will be extended to count as a noise factor due to the external environment. Verification will also include a recognition module that will lock the banking system if not used by an unauthorized person who is not a real user. Our future work will ultimately investigate the inclusion of our face recognition system in a larger authentication framework. Such a framework may use the levels of trust associated with other schools of trust (eg from touch) to produce a more robust result.

REFERENCES

[1] Xing Fang and Justin Zhan., Online Banking Authentication Using Mobile Phones., Future Information Technology (FutureTech)., 2010

[2] RajpreetKaurJassal and Ravinder Kumar Sehga.l, Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example., IOSR Journal of Computer Engineering (IOSR-JCE)., Aug. 2013

[3] S.T. Bhosale and Dr. B.S.Sawant., SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS., International Journal of Advanced Technology & Engineering Research (IJATER)., February 2012

[4] Fatema A. Albaloosh, Max Smith-Creasey, YousifAlbastaki, and MuttukrishnanRajarajan., Facial Recognition System for Secured Mobile Banking., Sustainability and Resilience Conference: Mitigating Risks and Emergency Planning., 2018

[5] Rahul Bajaj, Ronet Swaminathan, Tanay Srivastava Graceline Jasmine., Face Detection and Recognition & Investigation., April 2018

[6] http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

[7] https://bigdata-madesimple.com/how-do-chatbots-work-an-overview-of-the-architecture-of-a-chatbot/

[8] https://www.researchgate.net/publication/327980768_LBPH_Based_Improved_Face_Recognition_At_Low_Resolution