

Face identification with Multiparty Access in Net Banking Environments

Palani Kumar.R¹, Bharathi.S² and Sowmiya.K³

¹ Kongunadu College of Engineering and Technology/IT, Trichy, Tamilnadu
Email: ashokpalani26@gmail.com

²⁻³ NKongunadu College of Engineering and Technology, Trichy, Tamilnadu
Email: {bharathivijayalakshmi, sowmiyap83}@gmail.com

Abstract—The internet banking services are secured with different security techniques and methods. The credentials like username and password are the important security measure to provide protection for banking systems. There is a change to steal the username and password, possibility to access the banking application like net banking from the unauthorized users. To protect unauthorized access towards security and privacy, a new emerging technique called biometric based authentication and identification techniques are followed in the banking sector. The Face Recognition is the technique to analyze the characteristics of human involved in authentication process. Fingerprints, face, hand geometry, voice and iris are the basic behaviour or characteristics of a person. The project deals with totally functional face recognition for verifying characteristics of a human face. With that, it also provides multiparty access systems; the account holder provides privileges to the minimum number of users with valid credentials. ICP algorithm gives high level security in online banking systems than the traditional authentication systems.

Index Terms— Bio-metrics, Iterative Closest Point algorithm, KNN-Classification algorithm, biometric cryptosystems.

I. INTRODUCTION

The basic cloud systems and superior data structures are providing complex information access towards banking application and online transaction systems. It produced a very low quality of content. The use of fog computing in cloud computing and big data applications uses different variety of content. The fog computing uses number of metrics to improve the accuracy from traditional file content with very minimum of quality content. Control Plane and Data plane are important in Fog networking. For example, the computing services are present in the network on the data plane in fog computing different from servers used in data centers. The fog computing provides better quality of service with the following metrics like user requirements, transparent location circulation and limited resource group, decrease in latency and bandwidth of the network and edge analytics/stream mining, provides good graphical user interface (GUI) and provides better fault tolerance when a single system failure, other system in network will provide specific assistance to the system. Internet of Things(IoT) are supported to Fog networking concept, in which regularly used home held devices are connected to the networking systems. Mobile phones, wearable health assistance systems, virtual reality devices are connected with cloud application and cloud centers. The fog computing provide the extension services of

cloud computing and services to the edge of the network, gives the better results than cloud data created in the particular user end. Fog computing offers improved efficiency, less of amount of data for processing cloud data, examine the purpose of the data and identify the location to store specific data in the cloud. Origin of the fog computing frameworks manages the effective data processing with respect to the organization.

A. System Analysis

Existing system

A Challenge is remain in online security to provide protected transaction on the internet. User authentication techniques like username and password are always providing better security access to online transaction services. However, advancement in technical aspects the additional security measures are added with existing services and involves more cost investments. All the banking application service providers fight against fraud access in banking system. One Time Passwords (OTP) is one of the fraud prevention techniques used with banking applications. The time variant codes are generated and send to the users and it is valid for few minutes and within that user wants to enter their OTP. Debit cards and credit cards are with pin number as security measures for identifying valid users with valid credentials like pin number. The problem is that all existing security measures present one challenge or the other. Transaction monitoring systems checks for validation of valid users with specified credentials of username and pass- word. This systems leads to fraud identification in credit card and debit card. In this technique, use the existing components and perform background process with existing one.

Proposed System

Online banking application system provides fast access of transactions with very minimum timestamp. All the handheld devices like mobile phone comes applications and perform quick transaction and perform all the operations are performed at anywhere and anytime. Using latest technologies the unauthorized users can hack the details of account holder like username, password, credit /debit card pin number and security questions. To provide better access of internet banking in secure way from unauthorized users with the technique Face Biometric Authentication. The banking sectors provide Internet banking now uses Static User ids and passwords along with OTP-One time Passwords to mobile number. Although this is the best security feature available to date, this security method is still vulnerable and it is very important to enhance the existing security. The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological behaviors. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. Biometrics is not into Internet banking applications yet. It is because of the practical difficulties and it is very expensive to implement and execute this technology. But, now with technology advancement and cost of Biometric devices coming down, we have probabilities to integrate Biometric Technology to Online Banking. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features. And also extend the process to implement the system with multiparty access. The user of the account is considered as primary user. The primary user provides the permission to access account to other persons considered as secondary users. The primary user set the limit for secondary access. At the time of login verification, face can be recognized as whether it is primary or secondary. The OTP based password can be send at the time transactions. Finally SMS alert send to primary user with detail description of user name, time of access, amount details. Session time analysis can be used prevent from infrequent access.

II. SYSTEM IMPLEMENTATION

A. Modules Description

Bank Interface Creation

Online banking is thus changing the way people shop and how retailers operate. There is a steep decline in traditional payment methods such as cash and cheque and people are choosing the emerging digital payment technologies as they render convenient and flexible methods for conducting cashless financial transactions. Therefore online banking is reshaping the financial services ecosystem and more consumers are using their mobile devices for payment-related transactions as well as for accessing sensitive personal information. However, this technology and digital convergence has also attracted the threat of cyber-attacks and made banks and financial institutions more vulnerable to fraud. It has led to a new breed of fraud perpetrators that use sophisticated technologies to hack into personal devices and corporate networks. Traditional techniques such as password or tokens are no match to their attacks. To overcome, these attacks, we can design the interface for

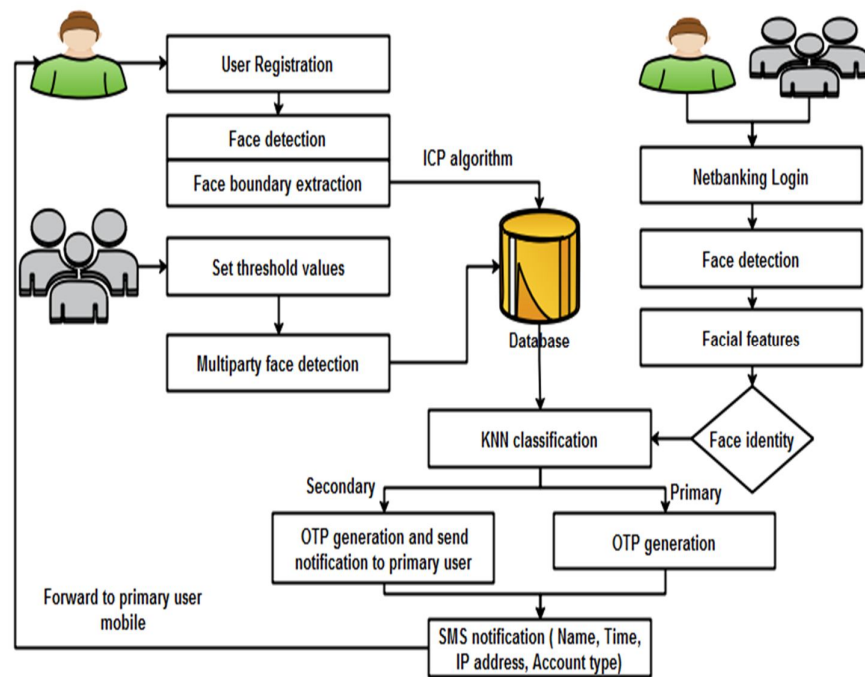


Fig 1. system architecture

online transactions in banking system. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transactions, debit card transactions and on.

Face Detection

The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. These Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based account security systems. Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and difficult. In this module, we can implement features based method to detect the facial parts such as nose, lips, eyes, cheeks using iterative closest point algorithm. In this module we use, for performing ICP, a set of features selected based on the tolerance level of spatial deviation. This allows a rapid convergence of the algorithm which processes only these points and cancels points which presents spatial deviation value superior to the tolerance value. In contrast, correspondence concerns all intersecting points.

Access Permissions

Multi-party authorization (MPA) is a process to protect online transactions from undesirable acts by a malicious insider or inexperienced technician acting alone. MPA requires that a second authorized user approve an action before it is allowed to take place. This pro-actively protects data or systems from an undesirable act. In this module, user of account specified as primary user. In this module, primary user provides access permission to secondary users with predefined threshold values. Admin can store details of secondary users with relationship information.

Face Verification

In this module, perform the verification of multiple users using classification algorithm named as K-Nearest Neighbor Classification. The k-nearest neighbor algorithm (k-NN) is a method for classifying objects based on closest training examples in the feature space. K-NN is a type of instance-based learning, or lazy learning where the function is only approximated locally and all computation is deferred until classification. The k-nearest neighbor algorithm is amongst the simplest of all machine learning algorithms: an object is classified by a

majority vote of its neighbors, with the object being assigned to the class most common amongst its k nearest neighbors. Based on classification results, user enters into the system.

Otp Generation

One time password can be generated using SHA-3 algorithm. Hash algorithms are fundament to many cryptographic applications. A secure hash algorithm, often known simply as an “SHA,” is a hashing algorithm that is considered cryptographically secure. In general, hashing functions are used to sort and organize digital data into smaller, more categorized packets for password. And transfer the OTP to Server. Server can be compare OTP and Allow access to the system. In the secondary access, OTP can be transfer to main user and also secondary users. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device.

B. Algorithm

Iterative Closest Point Algorithm

In the Iterative Closest Point or, in some sources, the Iterative Corresponding Point, one point cloud (vertex cloud), the reference, or target, is kept fixed, while the other one, the source, is transformed to best match the reference. The algorithm iteratively revises the transformation (combination of translation and rotation) needed to minimize an error metric, usually the distance from the source to the reference point cloud. ICP is one of the widely used algorithms in aligning three dimensional models given an initial guess of the rigid body transformation required. Given 2 points r_1 and r_2 , the Euclidean distance is:

Given a point r_1 and set of points A , the Euclidean distance is:

$$d(r_1, A) = \min_{i \in 1..n} d(r_1, a_i)$$

The scene shape S is aligned to be in the best alignment with the model shape M .

The distance of each point s of the scene from the model is:

$$d(s, M) = \min_{m \in M} \|m - s\|$$

Algorithm steps as follows

```
function ICP(Scene,Model)
begin
  E` ← + ∞;
  (Rot,Trans) ← In Initialize-Alignment(Scene,Model);
  repeat
    E ← E`;
    Aligned-Scene ← Apply-Alignment(Scene,Rot,Trans);
    Pairs ← Return-Closest-Pairs(Aligned-Scene,Model);
    (Rot,Trans,E`)
  Update Alignment(Scene,Model,Pairs,Rot,Trans);
  Until |E` - E| < Threshold
  return (Rot,Trans);
end
```

k-nn classification algorithm

In face recognition, the KNN algorithm is a method for classifying objects based on closest training examples in the feature space. KNN is a type of instance-based learning, or lazy learning where the function is only approximated locally and all computation is deferred until classification. The KNN is the fundamental and simplest classification technique when there is little or no prior knowledge about the distribution of the data. This rule simply retains the entire training set during learning and assigns to each query a class represented by the majority label of its k-nearest neighbors in the training set. The Nearest Neighbor rule (NN) is the simplest form of KNN when $K = 1$. In this method each sample should be classified similarly to its surrounding samples. Therefore, if the classification of a sample is unknown, then it could be predicted by considering the classification of its nearest neighbor samples. Given an unknown sample and a training set, all the distances between the unknown sample and all the samples in the training set can be computed. The distance with the smallest value corresponds to the sample in the training set closest to the unknown sample. Therefore, the

unknown sample may be classified based on the classification of this nearest neighbor. The algorithm steps as follows:

```

for all the unknown samples UnSample(i)
for all the known samples Sample(j)
compute the distance between
Unsamples(i) and Sample(j)
end for
find the k smallest distances
locate the corresponding samples
Sample(j1),...,Sample(jK)
assign UnSample(i) to the class which appears more frequently end fo

```

The performance of a KNN classifier is primarily determined by the choice of K as well as the distance metric applied. The estimate is affected by the sensitivity of the selection of the neighborhood size K, because the radius of the local region is determined by the distance of the Kth nearest neighbor to the query and different K yields different conditional class probabilities.

III. CONCLUSIONS

Biometric technology offers enhanced security while being convenient to use. It guarantees that information is accessed only by authorized persons. The security system offers a reliable method for authenticating users. It reduces frauds and minimizes password administrator costs. When biometric technology goes mainstream, banks can use biometrics in every transaction requiring the authentication of identity. In this paper, we can implement face recognition system to online net-banking application in IOT environments. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. The Face Recognition identification overcomes all the above. And also provide multi-person access control to provide access privileges to users with improved security. Real time alert system about unauthorized access and multi person access.

In future, we can extend the framework to implement an ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additionally, the system also contains the original verifying methods which were inputting owner's password which is sent by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

REFERENCES

- [1] Belás, Jaroslav, et al. "Electronic banking security and customer satisfaction in commercial banks." *Journal of security and sustainability issues* (2016).
- [2] Nishanthini, S., and R. Nallusamy. "A new level security in multi biometric system using fine quantization structures." *identity* (2017).
- [3] Council, Federal Financial Institutions Examination. "Authentication in an internet banking environment." *Financial Institution Letter*, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC). Retrieved March 18 (2005): 2005.
- [4] Gupta, Garima, and Sumit Dhariwal. "A Bird Eye View on Secure Banking by using Different Image Based Hiding Technique Encryption and Decryption." *International Journal of Engineering and Management Research (IJEMR)* 7.2 (2017): 593-598.
- [5] Lin, Yong, et al. "An efficient parallel approach for sclera vein recognition." *IEEE Transactions on Information Forensics and Security* 9.2 (2014): 147-157.
- [6] J. Yuan and S. Yu, "Efficient privacy-preserving biometric identification in cloud computing," in 2013 Proceedings IEEE INFOCOM, 2013, pp. 2652-2660.
- [7] K. Ren, "A Privacy- Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2594-2608, 2016.
- [8] U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported Internet of Things environment," in 2015 6th International Conference on the Network of the Future (NOF), 2015, pp. 1-3.