ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

# Confidential Data Protection Using Fingerprint Minutiae

[I]Namita Chandra, [II]Ashwini Taksal, [III]Dhanshri Shinde, [IV]Prof. Archana Lomte
[I, II, III]Dept. of Computer, BSIOTR (W), Pune University, Maharashtra, India
[IV]Assistant Professor, Dept. of Computer, BSIOTR (W), Pune University, Maharashtra, India
E-mail : [I]namitachandra1992@gmail.com, [II]ashwinitaksal29@gmail.com,
[III]dhanshrishinde3@gmail.com, [IV]archanalomte@gmail.com

**Abstract**
*Online banking is one of the most sensitive tasks performed by general internet user. In today's era of virtualization it is adopted as a parallel medium of communication, transaction and social networking. It is the fast gaining momentum across the globe for its convenience and ease of conducting transactions at a speed and service levels never dreamt of, a decade ago. But along with its various advantages, there is a need to step back and re-think on the perception it carries. With the increase in the internet usage, the need of security has increased because of the increase in the hacking and phishing procedures. Moreover, every user has some sensitive and confidential data, which needs more security. In this paper, we provide the security to the confidential data of the user using the OTP and the Biometric Fingerprint scanner. The enrolled fingerprint in the database is authenticated to validate the user and to give him access to his own data.*

**Keywords**
*Authentication, Biometrics, Digital Persona, Internet/Online Banking, OTP, QR Code, Security*

## I. Introduction

Introduction to The Online Banking has revolutionized the way in which the people and the business used to do banking [1, 9, 14]. Internet and the mobile equipments have made it possible for the customers to do transactions and other banking related operations, anytime, anywhere. In this digital age, online banking has become an easier and comfortable method to carry out transactions as compared to the traditional banking practices. Nevertheless, its usage in this age is also a question in the context of the user's security and services. On one side, the introduction of mobile banking has made possible for the customers to do transactions and other banking related operations, with the help of the mobile equipments, round the clock [2, 5,16]. However, the medium chosen for online banking is the internet and hence, of course all the vulnerabilities of the internet apply for the online banking application systems and all the internet hacking and phishing. With the coming up of new technologies, comes the need of immediate security. Moreover, these questions of security apply both to the user and to the bank itself. The rate of frauds to the users has increased to an extent drastically. Not only has it caused the harassment to the user, with his sensitive data loss, but also to the banking business. European Internet Security Survey conducted by Entrust (2005) reports that 83% of individuals in the UK, 72% in Germany and 80% of North Americans are concerned with identity theft attacks on their online banking accounts. Recent banks are becoming increasingly reluctant to reimburse users who fall prey to online scams such as phishing or pharming. The first hacking incident in Korea in 2005 spurred the FSS (The Korean Financial Supervisory Service) to announce a comprehensive countermeasure. So to protect these kinds of attacks on the sensitive and confidential data of the user, in this paper, we are going to propose a system which will use the OTP (One Time Password) [1, 6, 9,14] and the Biometrics Fingerprint Scanner named, Digital Persona to make the user safe [9].
This will enable the user to access his data only if he is authenticated for the system and proves himself the legitimate user by scanning of his fingerprint.

## II. System Architecture

The system includes the usage of Biometrics system and the Central Controller to provide the 3-level authentication to the user which can be described as follows:-

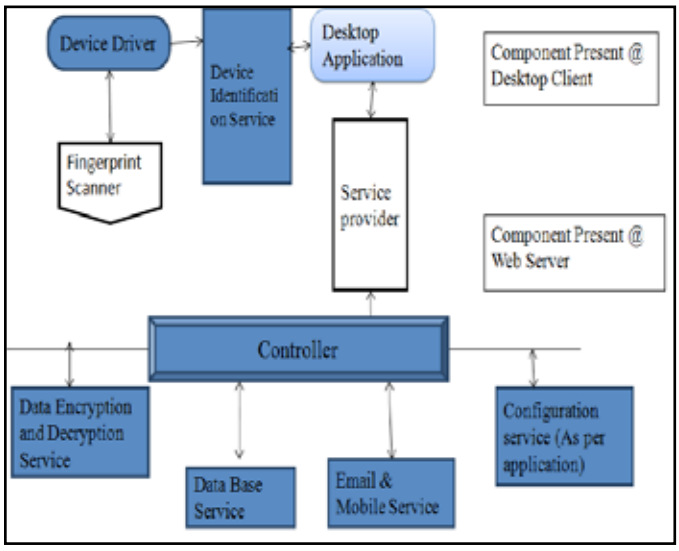


Fig. 1: System Architecture

The desktop application at the Desktop Client is the user using the banking application. He is provided the security initially with the authentication via login, then confirmation of the OTP and finally the Biometrics Device – DigitalPersona Fingerprint Scanner.
The controller is responsible for overlooking all the functions of the services.

1. The Data Encryption and Decryption Service provides the user with encrypted password which cannot be visualized even by the person who is responsible for carrying out the registration of the user.
2. Database Service stores the information of the user, including the password of the user in an encrypted form and also the confidential data in encrypted form.
3. After the user has registered, an acknowledgement email is sent to the user's registered email id and also the OTP is sent to the registered Mobile number. This function is carried out by the email and the mobile service.
4. The configuration services are responsible to configure the

other services of the system to perform their function as per the application is concerned.

An overview of the diagram can be seen as follows:-

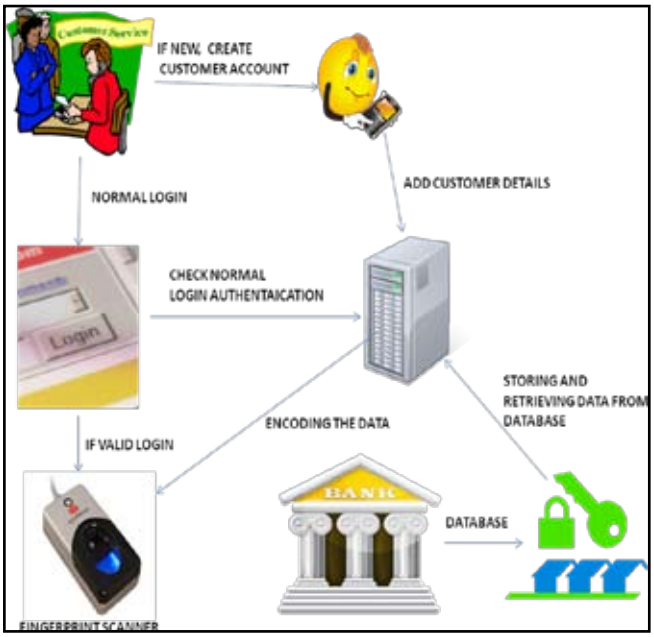


Fig. 2: Overview of System Architecture

## III. Implementation

### A. OTP (One Time Password) Generation Algorithm

We can call it a hashing algorithm rather than calling it an encryption-decryption or authentication algorithm [1, 6, 9, 14]. The basic approach is to transform an array of bytes into another.

- The key must be at least 20 bytes.
- 20 bytes random secret key + 8 bytes counter (say example, Phone no.) = OTP generated.
- OTP will be valid for a couple of minutes.
- This OTP is sent to the user's registered mobile number.

### B. AES (Advanced Encryption Standard) Algorithm

It is a Symmetric key algorithm, which means that only one key is required for both the encryption and the decryption of the data [9]. The basic principle to this is to design a substitution-permutation network and the approach is as follows:-

- Assume the secret key is of 128 bytes.
- This key is arranged in the form of matrix of size of 4 × 4 bytes.
- The first word from the key fills the first column of the matrix, and so on.
- Hence, the four column of the key matrix are expanded into a schedule of 44 words as each round consumes four words from the key schedule.

### C. Fingerprint Recognition Algorithm

The DigitalPersona fingerprint recognition system uses the processes of fingerprint enrollment and fingerprint verification.

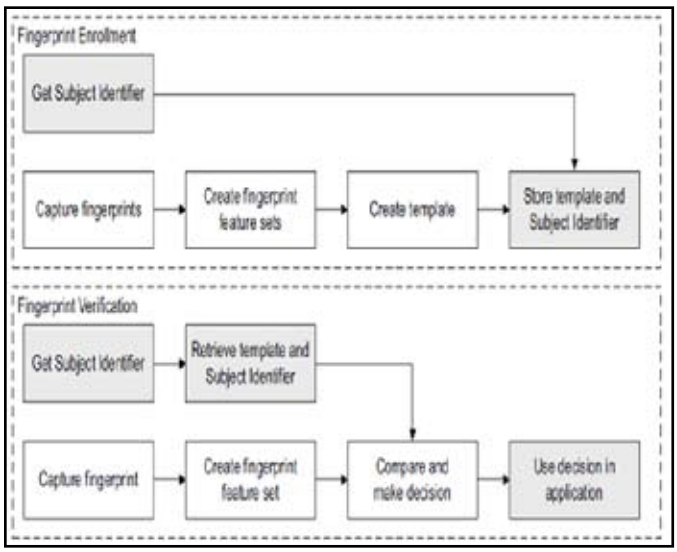


Fig. 3: DigitalPersona Fingerprint recognition system

### 1. Fingerprint Enrollment

This fingerprint enrollment is the initial step of storing the sample of the user to be authenticated in the database which will be used for validating the authenticated user at the time of fingerprint verification [4, 7, 8]. The following procedure describes typical fingerprint enrollment. (Steps preceded by an asterisk are not performed by the One Touch for Windows SDK: C/C++ Edition.)

1. *Obtain the enrollee's identifier (Subject Identifier).
2. Capture the enrollee's fingerprint using the fingerprint reader.
3. Extract the fingerprint feature set for the purpose of enrollment from the fingerprint sample.
4. Repeat steps 2 and 3 until you have enough fingerprint feature sets to create a fingerprint template.
5. Create a fingerprint template.
6. *Associate the fingerprint template with the enrollee through a Subject Identifier, such as a user name, email address, or employee number.
7. *Store the fingerprint template, along with the Subject Identifier, for later comparison.

Fingerprint templates can be stored in any type of repository that you choose, such as a fingerprint capture device, a smart card, or a local or central database.

### 2. Fingerprint Verification

Fingerprint verification is the process of comparing the fingerprint data to the fingerprint template produced at enrollment and deciding if the two, the one stored in the repository and the same taken from the customer/user that is to be authenticated, match[10][11][12]. The following procedure describes typical fingerprint verification. (Steps preceded by an asterisk are not performed by the One Touch for Windows SDK: C/C++ Edition.)

1. *Obtain the Subject Identifier of the person to be verified.
2. Capture a fingerprint sample using the fingerprint reader.
3. Extract a fingerprint feature set for the purpose of verification from the fingerprint sample.
4. *Retrieve the fingerprint sample stored in the repository for the verification of matching among the two.
5. Perform a one-to-one comparison between the fingerprint feature set and the fingerprint template, and make a decision of match or non-match.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

6. *Act on the decision accordingly, for example, unlock the door to a building for a match, or deny access to the building for a non-match

## 3. False Positives and False Negatives

Fingerprint recognition systems provide many security and convenience advantages over traditional methods of recognition. However, they are essentially pattern recognition systems that inherently occasionally make certain errors because no two impressions of the same finger are identical. During verification, [10,11,12]sometimes a person who is legitimately enrolled is rejected by the system (a false negative decision), and sometimes a person who is not enrolled is accepted by the system (a false positive decision).

The proportion of false positive decisions is known as the false accept rate (FAR), and the proportion of false negative decisions is known as the false reject rate (FRR). In fingerprint recognition systems, the FAR and the FRR are traded off against each other, that is, the lower the FAR, the higher the FRR, and the higher the FAR, the lower the FRR.

A One Touch for Windows: C/C++ Edition API function enables you to set the value of the FAR, also referred to as the security level, to accommodate the needs of your application. In some applications, such as an access control system to a highly confidential site or database, a lower FAR is required. In other applications, such control system to a highly confidential site or database, a lower FAR is required. In other applications, such as an entry system to an entertainment theme park, security (which reduces ticket fraud committed by a small fraction of patrons by sharing their entry tickets) may not be as significant as accessibility for all of the patrons, and it may be preferable to decrease the FRR at the expense of an increased FAR.

It is important to remember that the accuracy of the fingerprint recognition system is largely related to the quality of the fingerprint. Testing with sizable groups of people over an extended period has shown that a majority of people have feature-rich, high-quality fingerprints. These fingerprints will almost surely be recognized accurately by the DigitalPersona Fingerprint Recognition Engine and practically never be falsely accepted or falsely rejected. The DigitalPersona fingerprint recognition system is optimized to recognize fingerprints of poor quality. However, a very small number of people may have to try a second or even a third time to obtain an accurate reading [4,7,8,10,11,12].Their fingerprints may be difficult to verify because they are either worn from manual labor or have unreadable ridges. Instruction in the proper use of the fingerprint reader will help these people achieve the desired results.

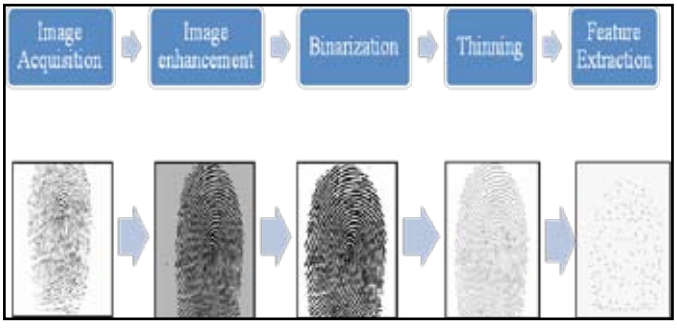


Fig. 2: Process of Fingerprint Enrolment

The process of this enrollment initially takes place on the accordance of five steps:-

1. Image Acquisition: - This is initial step of taking the fingerprint input via The DigitalPersona Fingerprint Scanner.
2. Image Enhancement: - The input taken may be in the form of an image. Because of the input device or may be because of the noises present, the image may be blurred enough to be stored in the database. Hence the contrast of the image is adjusted according to the visibility.
3. Binarization: - The enhanced image of the input fingerprint is contrasted in such a way that it has only two components, one is black and the other is white. The black represents the ridges of the finger and the white represents the valleys.
4. Thinning: - To extract the features of the finger, the bifurcations and the ridges are made 1 pixel wide structures. It shows the bifurcations too.
5. Feature Extraction: -The actual minutiae are extracted from the 1 pixel wide structure. These are actually the points of bifurcations, the ridges and the valleys in the finger.

These minutiae are stored in the fingerprint database at the time of enrollment and at the time of the verification, these stored minutiae are compared to that of the user to be authenticated.

## IV. Conclusions

In this paper, we provide a 3-level authentication to the user of the system. The Bank generates the OTP using permutations and combinations and random password generation and then user reads the OTP using their mobile phone, which is validated against the registered mobile number. Also the password and the username are validated. In the last stage of verification, the finger scanning is also done and the user is finally authenticated.

## V. AcknowledgEment

The authors are sincerely grateful to Prof. A.C.Lomte, our Project guide and mentor for her valuable guidance and encouragement. Also the authors are thankful to the Computer Engineering Department of JSPM's Bhivarabai Sawant Institute of Technology & Research (For Women) for their support in providing a good environment and facilities like books, internet and the other resources to complete this research.

## References

*[1] Young Sil Lee, Nack Hyun Kim,Hyotek Lim, HeungKuk Jo, Hoon Jae Lee, "Online Banking Authentication Syst em using Mobile-OTP with QR-code", Page(s):644-648,Nov. 30 2010-Dec.2 2010, E-ISBN :978-89-88678-30-5.*

*[2] M.Peyravian and C. Jefferies, "Secure remote user access over insecure networks",Computer Communications,Vol.29,Issue 1,pp.660-667,2006.*

*[3] P.reid, "Biometric for network Security", 1st Indian Reprint, Pearson Education, New Delhi, 2004.*

*[4] E.Spinella, "Biometrics Scanning technologies:Finger, Facial and Retinal Scanning", SANS technology Institute, San Francisco, dec.,2002.*

*[5] L.Lamport, "Password authentication with insecure communication", Communications of ACM, Vol.24,No.11,pp. 770-772,1981.*

*[6] DeFigueiredo, Dimitri: "the case for mobile Two-Factor Authentication". Security & Privacy, IEEE, Sept.-Oct. 2011.*

*[7] Jinwei gu, jie Zhou and Chunyu Yang," Fingerprint*

*Recognition by Combining Global Structure and Local Cues", IEEE TRANSACTIONS ON IMAGE PROCESSING, pp.1952, Vol.15,No. 7, July 2006.*

*[8] Pankaj Bhowmik, Kishore Bhowmik, Mohammad Nurul Azam, Mohammed Wahiduzzaman Rony, "Fingerprint Image Enhancement And It"s Feature Extraction For Recognition", IJSTR, VOLUME 1, ISSUE 5, JUNE 2012 ISSN 2277-8616 117.*

*[9] Namita Chandra, Ashwini Taksal, Dhanshri Shinde, Prof. Archana Lomte," Sensitive Data Protection Using Bio-Metrics", IJARCSSE Volume 4, Issue 1, January 2014.*

*[10] Neeraj Singla, Sugandha Sharma,"Biometric Fingerprint Indentification Using Artificial Neural Network", IJARCST, Vol. 2 Issue 1 Jan-March 2014.*

*[11] Uday Rajanna, Ali Erol, George Bebis,"A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion", Springer-Verlag London Limited 2009, Pattern Anal Applic.*

*[12] Mahmoud H. Farhan Loay E. George Azmi T. Hussein,"Fingerprint Identification Using Fractal Geometry", IJARCSSE, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.*

*[13] Yesha Pruthi, Harsha Singh, Aditi Verma,"A Comparative Study on Biometric Technology", IJARCSSE, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.*

*[14 Jaideep Murkute, Hemant Nagpure, Harshal Kute, Neha Mohadikar, Chaitali Devade," Online Banking Authentication System Using QR code and Mobile OTP",International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com,Vol. 3, Issue 2, March-April 2013.*

*[15] Dr.D.S.Rao, Gurleen Kour, Divya Jyoti,"One Time password Security through Cryptography For Mobile Banking", Vol 2(5), 1563-1567, ISSN:2229-6093.*

*[16] Sagar Acharya,"Internet Banking Two Factor Authentication Using Smartphone",International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013 1ISSN 2229-5518.*

## Author's profile

*Namita Chandra is currently pursuing her B.E. in Computer Engineering from JSPM's Bhivarabai Sawant Institute of Technology & Research (For Women), Pune University.*

*Ashwini Taksal is currently pursuing her B.E. in Computer Engineering from JSPM's Bhivarabai Sawant Institute Of technology & Research(For Women), Pune University.*

*Dhanshri Shinde is currently pursuing her B.E. in Computer Engineering from JSPM's Bhivarabai Sawant Institute Of technology & Research(For Women), Pune University.*

*Prof. Archana Lomte is a lecturer in JSPM's Bhivarabai Sawant Institute Of Technology & Research(For Women). She completed her B.E. and M.E. from Pune University.*