Secure Transaction using Dynamic Session Key

T. Mekala, N. Madhu Suganya

Abstract- Cryptography is a concept to protect data during transmission over wireless network. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transmitting (either electrically or physically) and while information is in storage. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. The existing system limits only the total number of users from the unknown remote host to as low as the known remote host. It uses the white list values for tracking legitimate users. But the cookie value expires after certain time period. So the attackers may use different browsers or may try on another machine or may retry after certain time. If any malicious attacks occurred the authenticated user does not know about that. The proposed system uses two algorithms known us Bio-Metric Encryption Algorithm (BEA), Minutiae Extraction Algorithm (MEA). It uses Multi Bio-metric features for authentication purpose. And also this system dynamically generates a new Session Key for each transaction. So the proposed system will protect Data Confidentiality, Data Integrity, Authentication, Availability, Access control of information over the network.

Keywords- Biometric Encryption Algorithm, Finger print, Minutiae Extraction Algorithm, Session key, Biometrics.

I. INTRODUCTION

User authentication and personal privacy is an important aspect of reliable information system. ONLINE guessing attacks [8], [9] on password-based systems are inevitable and commonly observed against web applications and SSH logins. Conventional cryptography uses encryption keys, which are just bit strings long enough, usually 128 bit or more. These keys, either "symmetric" "public," or "private," are an essential part of any cryptosystem, for example, Public Key Infrastructure (PKI). A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker.

On the other hand, biometrics provides a person with unique characteristics which are always there. Biometric is Physiological and behavioral characteristics of person which is absolutely unique to him. Physiological characteristics also called as static biometrics (e.g., fingerprints and iris patterns, as well as facial features, hand geometry and retinal blood vessels). Behavioral biometrics based on data derived from measurement of an action performed by a person, and distinctively incorporating time as a metric, that is, the measured action (e.g., voice, signature verification etc).

Biometrics identifies the person by what the person is rather than what the person carries, unlike the conventional authorization systems like smart cards. Biometric identifiers cannot be misplaced, forgotten, guessed, or easily forged.

Cryptography and biometrics are merged in biometric cryptosystem [6]. Biometric key system can be used broadly in two distinct ways 1.biometric based key generation 2.Biometric matching. To generate cryptographic key [13], [14] we are using biometric finger print. The uses are Easy to use, Cheap, Small size, Low power, and Non-intrusive, Large database already available. Biometric cryptosystems can operate in one of the following three modes, (i) key release, (ii) key binding and (iii) key generation.

Among all biometrics Fingerprint is most likely used. A fingerprint [12] [4] is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).

Cryptography provides high and adjustable security levels, biometrics brings in non- repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. Fingerprint patterns are used here because it is stable throughout person life time. Biometric recognition with cryptography provides a reliable solution for user authentication and identity management.

II. OVERVIEW OF THE PROPOSED SYSTEM

The main objective of the proposed system is to provide secure transaction and to restrict the Online attacks[9] such as Dictionary Attack [7] (a targeted technique of successively trying all the words in an exhaustive list called a dictionary from a pre-arranged list of values), Brute force attacks [9] (systematically checking all possible keys until the correct key is found), Masquerade(uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification), Modification of messages, IP Spoofing(creation of Internet Protocol (IP) packets with a forged source IP address[8], [9], called spoofing,

Manuscript received March, 2013.

T.Mekala, Asst. Professor, CSE dept, M.Kumarasamy college of Engineering. Karur, Tamilnadu, India.

N.Madhu Suganya, PG Scholar, CSE dept, M.Kumarasamy college of Engineering. Karur, Tamilnadu, India.

with the purpose of concealing the identity of the sender or impersonating another computing system) etc using some authentication techniques.

Multimodal biometric authentication has lately evolved as an interesting research area. In addition to these it is more consistent as well highly proficient than knowledge-based (e.g. Password) and token-based (e.g. Key) techniques. The following are very few good advantages of multimodal biometrics 1) improved accuracy 2) in case if sufficient data is not extracted from a given biometric sample, it can serve as a secondary means of enrollment as well as verification or identification and 3) the capability to identify endeavors to spoof biometric systems via non-live data sources particularly fake fingers.

Proposed system combines cryptography along with Biometric. Biometric cryptosystems [12] combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. Fingerprint patterns are stable throughout person's life time. In the proposed system the user must give both Username and Password for authentication purpose.

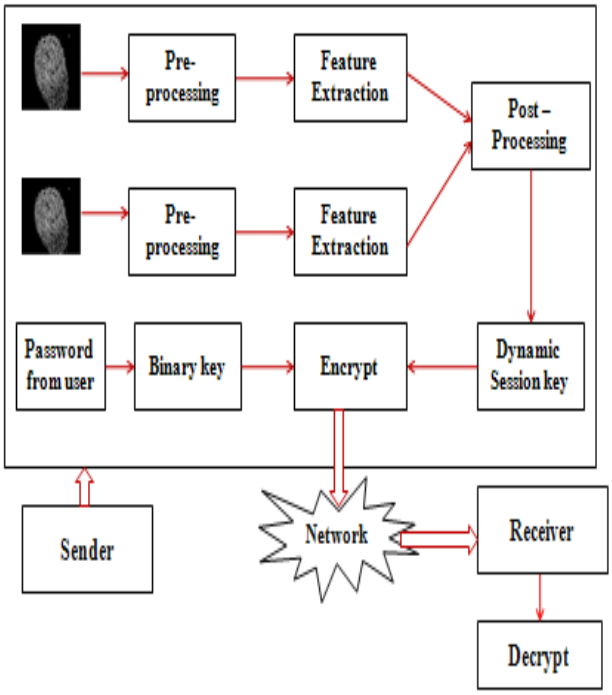


Fig 1. Overview of the proposed system

This system uses Multi Biometric features such as both left and right fingerprints of the user. Cryptography key is generated from a left and a right fingerprint is combined with the key generated from User's password. This Session key is encrypted using Some Cryptographic Algorithm with some key which is already shared by sender and Receiver. This Session key will be decrypted using the same key in receiver side. This system ensures Data Confidentiality (i.e., prevent the disclosure of information to unauthorized individuals or systems), Data Integrity (i.e., data cannot be modified undetectably), Authentication (i.e., to validate that both parties involved are who they claim they are), Access control (i.e., provides mechanisms to control over the protected data), Availability i.e., (the information must be available when it is needed).

III. DYNAMIC SESSIONKEY GENERATION

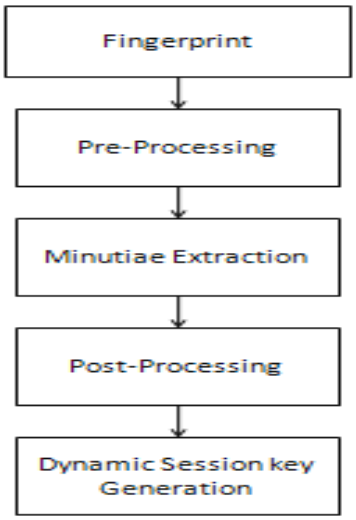


Fig 2. Steps in key generation

The fig shown deals with the first step called pre-processing and gives an insight into the process that has been followed for the enhancement of the input fingerprint image. The next step deals with the extraction of minutiae. In the third step called post-processing, false minutiae are deleted from the set of obtained minutiae and hence the actual minutiae required for dynamic session key are obtained.

A. Finger print

The lines that flow in various patterns across fingerprints are called *ridges* and the spaces between ridges are *valleys*. Different shape and structure of ridge and valley in each finger of an individual contributes to different global and local analysis.

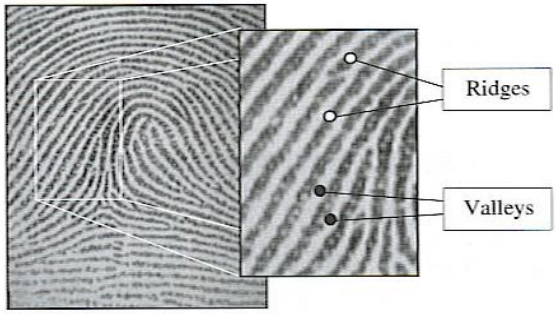


Fig 3. Ridges and Valleys of a Fingerprint image

Classes of Fingerprint Patterns are,

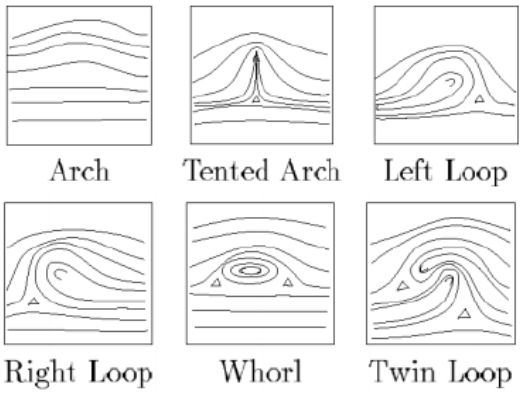


Fig 4. Classes of Fingerprint

B. *Image Pre-Processing*

i.) *Image Enhancement:* The Fingerprint enhancement is anticipated to improve the contrast between ridges and valleys and reduce noises in the fingerprint images [5]. High quality fingerprint image is very important for fingerprint verification or identification to work properly. In real life, the quality of the fingerprint image is affected by noise.

ii.) *Binarization:* Binarization is the process that translates a grey level image into a binary image. This enhances the contrast between the ridges and valleys in a fingerprint image, and consequently makes it possible the extraction of minutiae. Hence Binarization process involves analyzing grey level values of each pixel, if values is greater than the global threshold set binary value as 1 else 0. ‘

Fig 5. Fingerprint before and after binarization

iii.) *Thinning:* Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. Thinning is normally only applied to binary images, and produces another binary image as output.

Fig 6. Image after Thinning

iv.) *ROI Extraction:* In the fingerprint image, the region of interest (ROI) is the area of an image, which is importance for extraction of minutiae points. For ROI extraction two Morphological operations OPEN and CLOSE are used. The OPEN operation can expand images and remove peaks introduced by background noise The ‘CLOSE’ operation can shrink images and eliminate small variations.

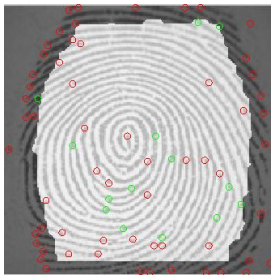


Fig 7. ROI Image

C. *Minutiae Extraction*

Fingerprint is distinguished with the help of minutiae (ridge ending and ridge bifurcation), which are the some abnormal points on the ridges.

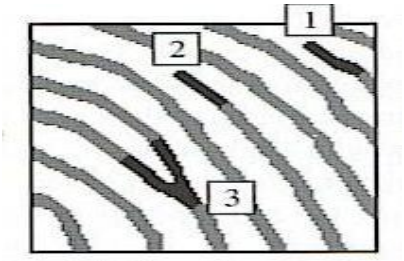


Fig 8. 1 and 2 are endings; 3 is bifurcation

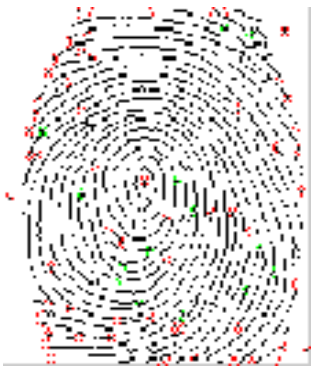


Fig 9. Minutiae Points Extraction

D. Post-Processing

The minutiae points obtained in the above step may contain many spurious minutiae. This may occur due to the presence of ridge breaks in the given figure itself which could not be improved even after enhancement. This results in false minutiae points which need to be removed. These unwanted minutiae points are removed in the post-processing stage. So to keep the recognition system consistent these false minutiae need to be remove. This process helps in removing false minutiae.

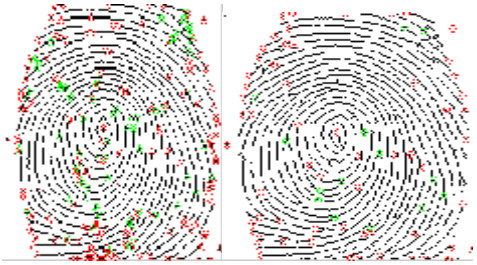


Fig 10. a) Minutiae points b) Real Minutiae points

IV. ENCRYPTION

Biometric Encryption algorithm provides a mechanism for the linking and retrieval of a binary key of the user's password with the Dynamic Session key from the user's fingerprint [16]. This algorithm generates the different key at each time. These values are encrypted using Blow fish algorithm. This increases the secrecy of key. Before the encryption process the sender and receiver must share their secret using RSA key exchange algorithm.

i.) *Blowfish Algorithm:* Blowfish is a keyed symmetric block cipher. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[2] It is a 16-round Feistel cipher and uses large key-dependent S-boxes.

ii.) *RSA Algorithm:* RSA is an algorithm for public key cryptography. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. This increases the secrecy of key. Before the encryption process the sender and receiver must share their secret using RSA key exchange algorithm.

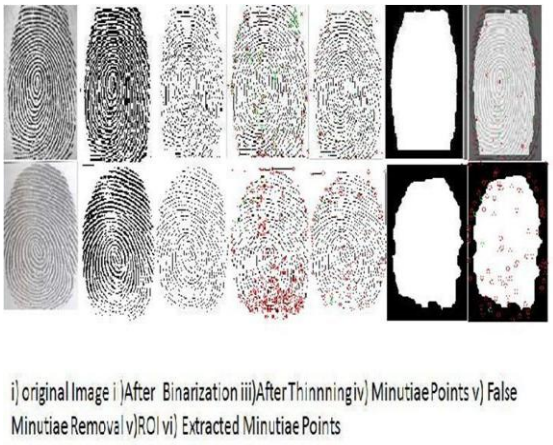
V. APPLICATIONS

1. Banking Security - ATM security, card transaction
2. Physical Access Control (e.g. Airport)
3. Information System Security
4. National ID Systems
5. Passport control (INSPASS)
6. Voting
7. Secure E-Commerce

VI. RESULTS

In this section, I have presented the experimental results of the proposed approach, which is implemented in MATLAB (Matlab7.5.0 (R2007b)) I have tested the proposed approach with different sets of input images.

.

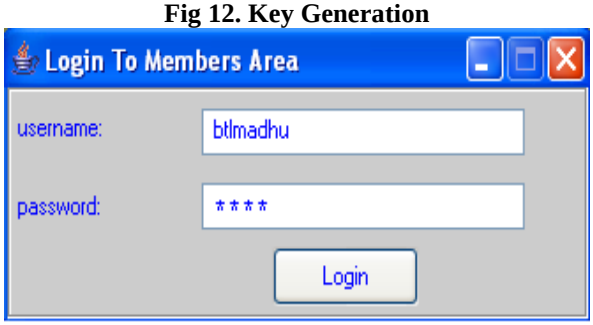


i) original Image i)After Binarization iii)After Thinnning iv) Minutiae Points v) False Minutiae Removal v)ROI vi) Extracted Minutiae Points

Fig 11.Minutiae Extraction Process

Figure 11 illustrates the different stage of the fingerprint image.

Fig 12. Key Generation



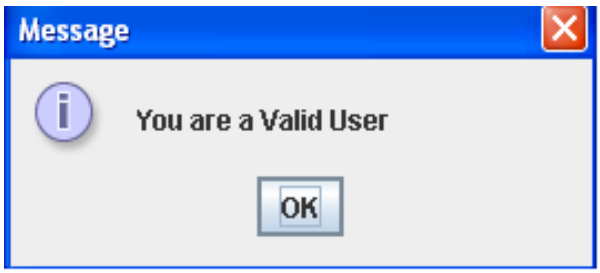


Fig 13. Authentication Process

VII. CONCLUTION

This system will provide multilevel security. It offers more convenient login experience, e.g., No ATT required. It is suitable for organizations of both small and large number of user accounts. Cryptographic keys are long so it is difficult to remember them, storing them in a data base may be insecure.

Hence the proposed method for generation of Dynamic Session key is using biometrics. The key is derived directly from the biometric data and is not stored in the database. Since it creates more complexity to crack or guess the crypto keys.

REFERENCES

1. Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot, Member, IEEE "Revisiting Defenses Against Large-Scale Online Password guessing Attacks" IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012.
2. S.M. Bellovin, "A Technique for Counting Natted Hosts," Proc. ACM SIGCOMM Workshop Internet Measurement, pp. 267-272, 2002.
3. Y. He and Z. Han, "User Authentication with Provable Security against Online Dictionary Attacks," J. Networks, vol. 4, no. 3, pp. 200-207, May 2009.
4. DHOLE S.A, PATIL V.H "Minutiae based Fingerprint Identification" Journal of signal and Image Processing ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 3, 2012, pp. -122-125.
5. W. Y. Leng and S. M. Shamsuddin "Fingerprint Identification using Discretization Technique" International Journal of Computer and Communication Engineering 6 2012.
6. Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy and B.V.K. Vijaya Kumar "Biometric Encryption".
7. D. Ramsbrock, R. Berthier, and M. Cukier, "Profiling Attacker Behavior following SSH Compromises," Proc. 37th Ann. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN '07), pp. 119-124, June 2007.
8. SANS.org, "Important Information: Distributed SSH Brute Force Attacks," SANS Internet Storm Center Handler's Diary, http://isc.sans.edu/diary.html?storyid=9034, June 2010.
9. "The Top Cyber Security Risks," SANS.org, http://www.sans.org/top-cyber-security-risks/, Sept. 2009.
10. C. Stoll, The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, Doubleday, 1989.
11. Nimithachama, *Dept. of Electrical & Computer Engineering Clemson University,* "Fingerprint image enhancement and minutiae extraction".
12. Dr.R.Seshadri,T.RaghuTrivedi, "Efficient Cryptographic Key Generation using Biometrics" Int. J. Comp. Tech. Appl., Vol 2 (1), 183-187.
13. Sunil V. K. Gaddam, and Manohar Lal "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", *International Journal of Network Security, Vol.11, No.2, PP.6169, Sept. 2010.*
14. A. K. Jain, L. Hong, S. Pantanki and R. Bolle, "An Identity Authentication System Using Fingerprints", Proc of the IEEE, vol, 85, no.9,1365-1388, 1997.
15. Tanmay Bhattacharya, Sirshendu Hore, Ayan Mukherjee and S. R. Bhadra Chaudhuri, "A Novel data encryption technique by genetic crossover of robust biometric key and session based password", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

AUTHORS PROFILE

Asst. Professor T.Mekala, completed her ME CSE in Bannari Amman institute of Technology, Erode in 2012. And completed her BE CSE in PSNA college of engineering and technology, Dindigul in 2010. Her interested areas area cryptography (crypto- Biometric), Network Security and Biometrics.

Ms.N.Madhu Suganya, doing Final year ME CSE in M.Kumarasamy college of Engineering. She was completed her B.TECH IT in Periyar Maniammai College of Technology for Women, Thanjur in 2010. Her interested areas are Cryptography, Network Securtiy, Image Processing and Embedded Systems. She is member of Computer Society of India (CSI).