Generation of key for Session key Distribution Using Bio-Metrics

1. Dr.R.Seshadri
Director
University Computer Center
Sri Venkateswara University,Tirupati

2. T.Raghu Trivedi
Research Scholar,
Sri Venkateswara University, Tirupati.

Abstract

Biometric cryptosystem gives different methods in high secure applications. Cryptography is intended to ensure the secrecy and authenticity of message. Here we will consider symmetric key cryptography. For conventional encryption to work, the two parties must share a common key. Frequent key changes are desirable to limit the amount of data compromised if attacker learns the key. The strength of any cryptosystem rests with the Key Distribution Technique, a term that refers the means of delivering a key to two parties who wish to exchange data. Here KDC will generate a session key and distributes it to two parties. To distribute session key, KDC will use secret key shared between KDC and individual party. The key will be long, so it is difficult to remember providing Protection of this key is major issue. Instead of storing key we will generate the key dynamically with the help of biometrics. Here we will use Finger print to generate key, which is safe and fast.

Keywords: *Cryptography, Biometrics, Symmetric key, KDC, Session key, minutiae points, ROI.*

1. Introduction

Cryptography is considered to be one of the fundamental building blocks of computer security. Data encoded with cryptographic key which is large one and impossible to keep in mind [1].Typically we write down and store keys .Providing security to theses keys is difficult. It is possible to solve this problem with the help of biometric.

A biometric system is a standard method for identify and verification of a human being based on the personal or physical identification of characteristics. In recent years there is a rapid growth in use of biometrics for user authentication applications; Cryptography and biometrics are merged in biometric cryptosystem [2]. Biometric key system can be used broadly in to two distinct ways

1. Biometric based key generation 2.Biometric matching. Input biometric signals and registered templates are utilized in the release of secret key.

We use the biometric concept in key distribution scenario. To distribute the session key generated by KDC to the two connecting parties the KDC will use Symmetric key cryptography .To generate this symmetric key we are using biometric finger print. .Biometric cryptosystems can operate in one of the following three modes, (i) key release, (ii)key binding and (iii) key generation [3]. Here we are using Key generation mode, in which key is derived directly from the biometric data and is not stored in the database.

2. Key Distribution Center

For conventional encryption to work the two parties to exchange must share the same key, and the key must be protected from others. Frequent key changes are usually desirable. Key distribution can be done in number of ways. Here we consider the scenario in which the sender and receiver will have encrypted connection with third party. The third party will generate session key used to communicate data safely between sender and receiver. Here the third party is Key Distribution Center (KDC).

The KDC will work as follows.

Suppose X want to establish logical connection with Y. It requires a session key to protect data transmitted over this connection. Let X and KDC will share a key K_X, Y and KDC will share a key K_Y. The following steps indicate how X and Y communicate with each other [4].

1. X issue Request to KDC for session key. Request message includes Def.X and ID of Y, Unique identifier, N1 (Nonce).
2. KDC respond with the message which include two parts

First part Session key, original request message and second part session key and ID of
X Second part encrypted with K_Y and total message is encrypted With K_X.

3. X stores Session key and sends the message intended for Y to Y.
4. Y responds to X with N2 encrypted by session key.
5. X responds with F (N2) encrypted with session key

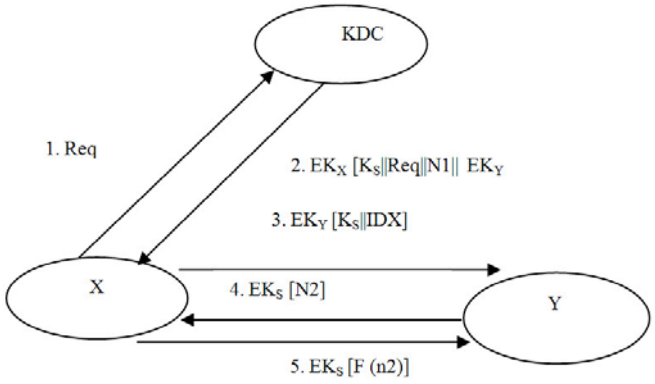


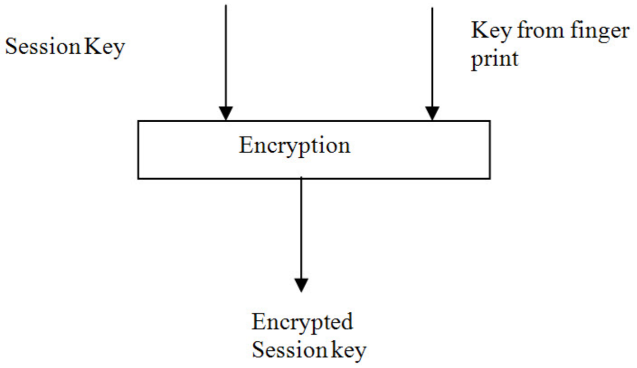
FIG.1 Describes about the KDC process

To Generate K_X and K_Y we are using the biometric Finger print.

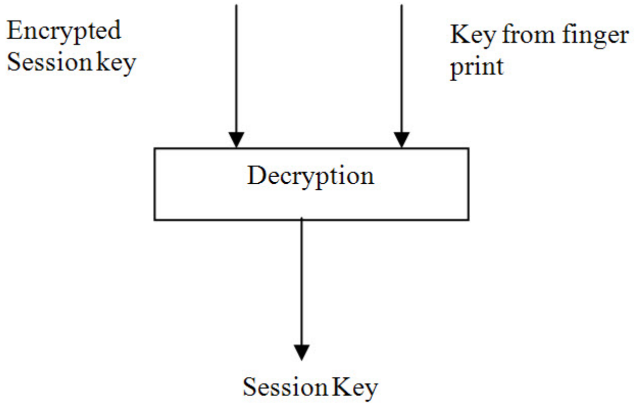
3. Biometric Crypto System

It provides the secure manner of information transfer. Authenticate message based on key. Here key will play a major role because it is used for encryption as well as decryption lengthy key is used for this purpose. Maintaining and sharing the key is critical problem, which can be overcome with the help of biometric system.

There are different techniques in biometrics like Irish pattern, Voice Recognition pattern, Face features pattern, Signature and Fingerprint. Here we concentrate on Fingerprint .Fingerprint biometric currently has three main application areas, which are Automated Finger Image System [AFIS], Fraud Prevention, Physical and Computer access [5]. We are using fingerprint patterns because it is stable throughout person's life time. It creates more complexity to the crack or guess the cryptosystem.



Encryption procedure



Decryption procedure

4. Key Generation from fingerprint:

Major stages in key generation from fingerprint are

1. Extracting Minutiae points
2. Matrix generation &Key generation

4.1 Extracting minutiae points

For extracting minutiae points we will use three level approach

- Image Preprocessing
- Region of Interest
- Minutiae extraction

4.1.1 Image preprocessing

For image preprocessing Histogram Equalization and Filters are used to enhance the image. Binarisation is applied on fingerprint image. Then Morphological operation is used to extract Region of Interest.

Histogram equalization: Histogram equalization increases the contrast of images, especially when usable data of the image represented by close contrast values. Perceptional information of the image is increased through Histogram equalization. It permits pixel value to expand. The used Fingerprint image use bimodal type. Histogram equalization converts range from 0 to 255 which will enhance visualization effect [6].

Fig2: Sample Finger Print

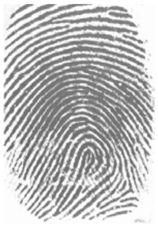


Fig3: After Histogram Equalization

Median Filter is non linear, digital filter methodology employed to eliminate noise from image or other signals. The values present in window are arranged into numeric order the median value, the sample in the center of the window is chosen as output. Oldest sample is abandoned, new sample is obtained and calculations are redone [7].

4.1.2 ROI

Binarisation

In Image black pixel denote ridges, White pixels denote valleys. A grey level image is translated into binary image in binarization. The contrast between ridges and valleys in fingerprint image is improved. 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.

***Morphological Operation**:*

The result of this approach is tightly bounded region just containing the bounded inner area. Binary morphological operators are applied on binarised fingerprint image. The unnecessary spurs, bridges, line breaks are removed by these operators. Different operators applied are clean, HBreak, Spur [8]. Thinning process is performed to reduce thickness of lines.

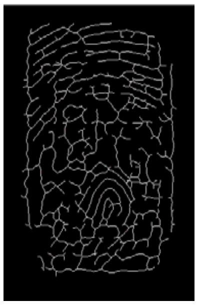


Fig4: Morphological operation

4.1.3 Minutiae point extraction

Thinning eliminates the redundant pixels of ridges till the ridges are just one pixel wide [9]. Ridge thinning algorithm is applied and in each scan of full fingerprint image , the algorithm marks down redundant pixels in each small window and finally removes all those marked pixels after several scans. After fingerprint ridge thinning minutiae points are marked easily.

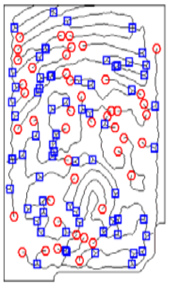


Fig 5: Fingerprint Image with Minutiae Points

4.2 Matrix & key generation:

Extracted minutiae points co-ordinates are maintained in a vector

M_p- Minutiae points set
S_p - Size of Mp
K_v -Key Vector
L_k -Length of key vector
Z - (X, Y) co-ordinate of a minutiae point

Step1: Represent extracted minutiae points as

$$Z_m = \{ Z_i \} \quad i=1, 2 \ldots S_p$$

Step2: Write Initial Vector

$$Kv = \{ X_i : Z(X_i) \} \quad i=1\ 2 \ldots L_k$$

$$\text{Where } Z(x) = Z_m[Z_m[i] \bmod Sp] \qquad i=1,2 \ldots L_k$$

Step 3: Convert initial vector into matrix of size $\sqrt{L_k}$ X $\sqrt{L_k}$ and name it as A_{km}

Step4: $A_{km} = a_{ij} \quad \sqrt{L_k}$ X $\sqrt{L_k}$

Generate intermediate vector as $I_v=\{K_i : Z(k)\}$ i=1,2 …L_k

Where $Z(k)=| SM_{ij}|$ $\quad SM_{ij}=A_{km}$ $\quad$ i, j : i+ Size , j + Size $-1< i < \sqrt{L_k}$

Step5: Final vector is formed as

$$Fky = 1 \text{ if } \quad I_v[i] > \text{mean}(I_v)$$
$$0 \text{ else}$$

The generated key is non reversible.

5. CONCLUSION

From the above discussion we have proposed a method for providing security to the Session Key Generated and Distributed by Key Distribution Center. The session key is used by the two parties to communicate securely in Distributed environment Different cryptographic techniques are used to secure the data. In the recent days, biometrics is used to recognize the user. Here system combines the biometrics and cryptography to provide the security for the Session key transmission process in the distributed environment. The system uses the biometrics technology as the security providing medium. This system uses the fingerprints for the security system. Password can be hacked by trial and error basis. But it is not possible to break the biometrics based security system.

6. REFERENCES

[1]. Sunil V. K. Gaddam and Manohar Lal ,"Effecient Cancellable Biometric Key Generation Scheme for Cryptography" *International Journal of Network Security, Vol.11, No.2, PP.57{65, Sep. 2010*

[2]. U. Uludag, S. Pankanti, S. Prabhakar, and A. K.Jain, \Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, pp. 948-960, 2004.

[3]. P.Arul, Dr.A.Shanmugam "Generate a Key For AES Using Biometric For VOIP Network Security" Journal of Theoretical and Applied Information Technology 2009.107-112.

[4]. William Stallings, "*Cryptography and Network Security Principles and practice*", 2nd Edition,Prentice Hall,

[5]. Mr.P.Balakumar, Dr.R.Venkatesan "Biometrics Based File Transmission Using RSA Cryptosystem" *International Journal of Computer and Network Security,Vol. 2, No. 4, April 2010*

[6]. Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-based fingerprint matching",IEEE Transactions on Image Processing, vol. 9, no. 5, pp: 846-859, May 2000, Doi:10.1109/83.841531.

[7]. J. Patrick Fitch, Edward J Coyle and Neal Gallagher,"Median filtering by Threshold Decomposition", IEEE Transactions on Acoustics, Speech and Signal Processing
(ASSP), vol. 32, no.6, pp. 1183 - 1188,1984

[8]. N.Lalithamani, K.P.Soman **"**Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme". European Journal of Scientific Research ISSN 1450-216X Vol.31 No.3 (2009), pp.372-387

[9]. L. Lam, S. W. Lee, and C. Y. Suen, \Thin-
ning methodologies-A comprehensive survey," *IEEETransactions on Pattern Analysis and Machine In-telligence*, vol 14, no. 9, pp. 879, Sep. 1992.

Authors Profile

Dr.R.Seshadri was born in Andhra Pradesh, India, in 1959. He received his B.Tech degree from Nagarjuna University in 1981. He completed his Masters degree in Control System Engineering from PSG College of Technology, Coimbatore in 1984. He was awarded with PhD from Sri Venkateswara University, Tirupati in 1998. He is currently Director, Computer Center, S.V.University,Tirupati, India. He published number of papers in national and international journals.

Mr.T.RaghuTrivedi received MCAdegree from Andhra University,Vizag He received his M.Tech in Computer Science from Nagarjuna University.He is a research scholor in S.V.University,Tirupathi, Andhra Pradesh.