A Survey On Network Security In Biometrics

[1]D.Sathiya Priya, [2] Dr.S.Manju Priya
[1]Research Scholar, [2]Associate Professor
[1]Department of Computer Science,[2]Department of Computer Science
Karpagam University, Karpagam Academy of Higher Education,Coimbatore,India

Abstract--In this present era, system and network technology is considered as a key tool for a wide variety of applications. Network security affects many organizations, and it becomes one of the major tasks. Biometric is one of the most secure and suitable authentication tools. By using biometrics in a correct way, many problems can be solved by using user identification and passwords. This paper analyses the security related issues, security threats and challenges in biometrics.

Keywords--Network Security, Biometrics

I. INTRODUCTION

Network security becomes a more important to personal computer users and the organizations [2]. With the advent of the internet, security becomes a major concern. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. When considering network security, it must be emphasized that the whole network is secure.

Biometrics refer to the automatic authentication of a person's physiological or behavioral characteristics. A biometric system is a pattern recognition system that retrieves biometric patterns from an individual, extracts biometric feature sets from them and thereafter stores them as biometric templates in a database [10].

It refers to the quantifiable data related to human characteristics and traits. Examples, including fingerprints, face recognition, DNA, palm prints, hand geometry, iris, retina, odor/scent, typing rhythm, gait, and voice. Biometrics-based authentication can be used in user identification and access control. Biometric information cannot be lost or forgotten and it is very difficult to copy, share, forge or distribute. In addition, biometric information cannot be easily guessed and such coding is more difficult to break than other types[1].

II. NEED FOR NETWORK SECURITY

The necessity for network security is growing on day-to-day environment. The information security is needed for the following reasons: [11]

- To protect the confidential information from other users on the net.
- To protect the information from unwanted editing, accidentally or intentionally by unauthorized users.
- To protect the information from loss and make it to be delivered to its destination properly.
- To protect the message from unwanted delay in the transmission lines/route in order to deliver it to the required destination in time, in case of urgency.
- To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

III. ISSUES AND CHALLENGES IN BIOMETRIC SECURITY

Some of the issues which occur in a biometrics are:

- The features extracted from the input signal are replaced with a fraudulent feature set.
- Presenting fake biometrics or a copy at the sensor, for instance a fake finger or a face mask. It is also possible to try and resubmitting previously stored digitized biometrics signals such as a copy of a fingerprint image or a voice recording.
- Attacking the channel between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified.
- Corrupting the matcher: The matcher is attacked and corrupted so that it produces pre-selected match scores.
- Tampering with stored templates, either locally or remotely.
- Overriding the match result.

III. EXISTING SECURITY METHODS

Some of the existing security methods are as follows:

Younsung Choi and Dongho Won proposed Improved Biometric-Based User Authentication Scheme. Jiping et al. proposed an improved authentication scheme to solve the problem of vulnerabilities in Das's scheme.. In this paper, the cryptanalysis of Jiping et al.'s biometric-based user authentication scheme for the client/server system is analysed. However, Jiping et al.'s scheme has some remaining security problems: the server-masquerading attack,stolen smart-card attack and authentication without login phase [5].

Tarik Zeyad Ismaeel and Ahmed Saad Names proposed Data Encryption Algorithm using Asymmetric Key Derived from Fingerprint Biometric Features**.** In which, encryption method depending on the distribution of the hells and valleys of the finger print. Since this distribution differs from one finger to another. The feature vector is converted to encryption key.

In general, encryption algorithms used this fingerprint key to encrypt and decrypt the data. The technique of protecting data by converting an encrypted message into an unreadable format is called cipher text. Only those who possess a private key can decipher or decrypt the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis and is also called code breaking. In short, using cryptography data is first encrypted into another form and then transmitted.

There are different steps in Cryptography as follows:
1. Encryption of the message.
2. Processing of the message is done with the help of private key.
3. At last, the encrypted message is decrypted by using private key.

The fingerprint encryption offers a new mechanism for key security by using a fingerprint to secure the cryptographic key. Instead of entering a password to access the cryptographic key, the use of symmetric key is guarded by fingerprint encryption. When a user wants to access a secured key, the user will be prompted to allow for the capture of a fingerprint sample, then the key is released and can be used to encrypt or decrypt the desired data[2].

Subhas Arman and Debasis Samanta proposed Fingerprint-based crypto-biometric system for network security. The biometric-based cryptographic key generation has some difficulties: privacy of biometrics, sharing of biometric data between both communicating parties (i.e., sender and receiver), and generating revocable key from irrevocable biometric. This work addresses the above-mentioned concerns.

It generates cryptographic key from cancelable fingerprint template of both communicating parties. Cancelable fingerprint templates of both sender and receiver are securely transmitted to each other using a key-based steganography. Both templates are combined with concatenation based feature level fusion technique and generate a combined template. Elements of combined template are shuffled using shuffle key and hash of the shuffled template generates a unique session key.

In this approach, revocable key for symmetric cryptography is generated from irrevocable fingerprint and privacy of the fingerprints is protected by the cancelable transformation of fingerprint template. The stego key is used by both parties for securing steganographic use. Sender uses the public key of receiver to encrypt and sends to receiver. Receiver can decrypt the shuffle key and password using his own private key, and they are used for key generation and template sharing, respectively [3].

Irene Getzi S proposed Minutiae Based fingerprint matching Scheme. It analyses the different minutiae based schemes which includes several stages such as pre-processing, thinning, and alignment based matching schemes. The first step of the algorithm is Pre-processing the finger prints to enhance its quality and Binarization of pre-processed fingerprint to highlight the ridges and furrows and then thinning of binarized image to be done.

The next step is to extract the minutiae points. The fingerprints captured through sensors normally of poor quality and may contain noise signals. Pre-processing is done to enhance the quality. The general processing approaches may not be suited due to non-static nature of fingerprints.

Hence, the popular preprocessing techniques such as histogram equalization, contrast stretching is the first step followed by filtering which applied after dividing the image into sub regions. Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows.

The binarized image is thinned to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. After getting two set of transformed minutia points, the elastic match algorithm is used to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.
Elastically matching the minutia is achieved by placing a bounding box around each template minutia. If the minutia is matched within the rectangle box and the direction discrepancy between them is very small, then the two minutiae are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia.

The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint [4].

Joseph Mwema and Michael Kimwele proposed Deriving Encryption Keys from Fingerprints. The technique involves a two-step enrollment and authentication of fingerprints while encrypting fingerprint templates with encryption keys derived from other biometric fingerprint templates before archiving them to a database.

First, the system prompts for user details i.e. user names and national identity card no. The system will not advance to the next steps until these details are provided. Once user particulars are supplied, system proceeds to the second step where capturing of fingerprints take place. Fingerprints registration process is divided into two other sub processes.

The first one is where the user supplies their first fingerprint for enrolment preferably any of their index finger. Once the finger is captured, the system extracts a fingerprint template from it and then the biometric fingerprint encryption modules extract a unique biometric key from it. The system then prompts the user to present the second fingerprint for enrolment after which it extracts a biometric fingerprint template from it.

Once the user's details are entered, fingerprints captured for enrolment and biometric encryption key ***is*** derived from the first enrolled fingerprint, the system then encrypts the second user's fingerprint template with the encryption key derived from the first fingerprint template to encrypted template which is now secured.

This step completes with the system saving the first fingerprint template to database and saving of the encrypted fingerprint template together with the supplied user details to database.

A biometric fingerprint encryption and decryption software tool that could derive encryption and decryption keys from biometric fingerprint templates was built.

In this, biometric templates encryption and decryption tool, encryption and decryption keys have to be derived from biometric fingerprint templates in order to be used. This tool achieved a secure way of obscuring encryption keys in biometric templates away from hackers prying eyes and would be adversarial attacks determinedly targeting to access biometric decryption keys in a biometric system[5].

The summary of the existing security methods is shown in below table1.

TABLE 1 : SUMMARY OF VARIOUS SECURITY SCHEMES FOR BIOMETRICS

S.NO.	AUTHOR	METHODS	RESULTS
1	Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, and Dongho Won	Cryptanalysis of Jiping et al.'s biometric-based user authentication scheme	To solve the problem of vulnerabilities in Das's scheme
2	Tarik ZeyadIsmaeel, Ahmed Saad Names	Fingerprint Image Enhancement, Preprocessing and Feature Extraction	Fingerprint cryptosystem can work effectively
3	Subhas Barman, Debasis Samanta and Samiran Chattopadhyay	Feature Extraction, Cancelable templategeneration, Steganographic encoding, Steganographic decoding	Random cryptographic key using fingerprint biometric of sender and receiver and the privacy and security of fingerprint data are provided with cancelable template.
4	Joseph Mwema,Stephen Kimani, ,Michael Kimwele	Advanced Encryption Standard (AES)Cypher Algorithm	To generate random cryptographic key using fingerprint
5	Irene Getzi S	Minutiae-Based Matching Method	Working effectively and well tested in other environments

V. CONCLUSION

Fingerprint biometrics provide a very strong preference for a biometric technology. It provides a higher security to networks and easier method to the users. Biometric security systems are a fortunate thing to the developing IT sectors. In this paper, some of the exiting methods have been analyzed. The analysis shows that large key space to be avoided and some of the attacks and noisy nature of the fingerprint image to be removed and it can be further extended to gray scale biometric data. Network security for biometrics are to be further explored.

REFERENCES

[1] Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, and Dongho Won, "Cryptanalysis of Improved Biometric-Based User Authentication Scheme for C/S System",International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015

[2] Prof. Dr. Tarik ZeyadIsmaeel,and Ahmed Saad Names, "Data Encryption Algorithm using Asymmetric Key Derived from Fingerprint Biometric Features",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.

[3] Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, "Fingerprint-based crypto-biometric system for network security" Barman et al. EURASIP Journal on Information Security (2015)

[4] Irene Getzi S, "Authentication Using Minutiae Based Fingerprint Matching Scheme for Smart Phones",Irene Getzi S et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2937-2939

[5] Joseph Mwema,Stephen Kimani and Michael Kimwele, "A Conceptual Technique for Deriving Encryption Keys from Fingerprints to Secure Fingerprint Templates in Unimodal Biometric Systems",International Journal Of Computer Applications · May 2015

[6] Divya and Vijayalakshmi ,"Analysis of Multimodal Biometric Fusion Based Authentication Techniques for Network Security", International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 239-246

[7] Blessy Rajra and Deepa," A Survey on Network Security Attacks and Prevention Mechanism", Journal of Current Computer Science and Technology, Volume 5, No. 2, February 2015

[8] Thijs Laarhoven,"Asymptotics of fingerprinting and group testing: capacity-achieving log-likelihood decoders", Laarhoven EURASIP Journal on Information Security (2016)

[9] Jincey John and Ashji S.Raj," Reliable Biometric Data Encryption Using Chaotic Map", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015

[10] Joseph Mwema, Michael Kimwele and Stephen Kimani," A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates", International Journal of Computer Trends and Technology (IJCTT) – Volume 20 Number 1 – Feb 2015

[11] Network Security-The Biggest Challenge in Communication- Ashima Jain- Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 3, Number 7 (2013), pp. 797-804 © Research India Publications