International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014

Enhancing Security of Stored Biometric Data

Manmohan Lakhera
Assistant Professor, Computer Science
Omkarananda Institute of Management & Technology
Rishikesh, India
lakhman07@gmail.com

***Abstract*— a biometric system is weak to a different type of attacks targeted at undermining the reliability of the verification process. These attacks are either imposter or irrevocability. Imposter means information stored in database, can be abused to construction of artificial biometric and replace it for fake authentication and irrevocability means once compromised, biometric not be updated, reissued or destroyed. In this paper we present a general architecture with the help of Digital Signature that guarantees privacy protection of biometric data. We specifically focus on secure a biometric data at the time of authentication and storage.**

Keywords-component; — Encryption, Public Key, Private Key, Verification, Password

I. INTRODUCTION

The main concern of how to secure stored biometric data is the vital design challenge that is addressed by this paper. Main vision of this paper is to secure stored biometric data with help of password. It focuses on secrecy of passwords in the case where password stored in personal computer's database in normal text format is compromised that's why passwords are not stored in normal text format, and only the hash code of password is stored. The hash is effectively impossible to invert. During verification a user enter password, which insert at the time of enrollment. Permission is only granted when the hash value of the new inserted password have matches the hash value of the stored password which had entered at the time of enrollment. The secrecy of password never compromised even if attacker studies about the stored hash value because of the non-invertible features of hash value. Basically biometric system divides into different modules. The sensor module obtained an individual's row biometric data in the different form like audio, video, image. Required Biometric data is extracted by extraction module. During user enrollment the extracted biometric data, label with the user's individuality, is stored in the database and is known as a biometric template. At the time of user verification the corresponding module compares the set biometric data extracted during verification with the stored biometric data and produces match result. Produces result is verified by the decision module this match either verified individual identity or rejects the verification request. Thus, the biometric system behaves like a pattern recognition system which contains two different classes genuine and fake. These classes identified that user is original user or fake user. If fake then corresponding class reject the request and if genuine then corresponding accept the request and provide access to the required system or database.

II. RELATED WORK

The biometric data attack is categorized in various categories which contain different type of threat and is possibly destroy or modify the stored biometric data or the biometric verification system from where the biometric data is obtained for match. Attacks on the stored biometric data can lead to the following weaknesses.

Jain et al [1] [2] summarized that stored biometric data can be replaced by a fake's Biometric data to gain illegal access. A physical spoof, basically a set of fake biometric data, can be used to gain illegal access to the database. The stolen set of biometric data can be replayed to the matcher to achieve illegal access. Stored biometric data composed with the data identifying an individual in a database in Biometric verification systems for later comparison. The biometric data is presented in the database's lookup for an individual's verification. If a record is found with biometric data that is appropriately close to the one presented, the person is known and hence authentic. Hence the verification system creates serious risk for biometric data protection. Because of this risk the internal and external attack are effects the privacy of stored biometric data.

Rudolf et al [3] [4] [5] identified the threat. When a verification system issued on a big scale, stored database has to be made accessible to many different verifiers, who are general and cannot be trusted. Particularly in a networked situation, database is not secure from different serious threat. Matsumoto et al. [6] Shown that biometric data stored in a database could be mistreated to make artificial biometrics meant to impersonate people. Fake biometric construct when some part of stored biometric data is available. Hill [7] if some data of biometric (minutia) are available, then there is some possibility to effectively build artificial biometrics that pass verification. Schneier [8] briefly summarized that if the biometric data of an individual is theft, it means the identity of an individual is theft. This means that once the biometric feature is compromised, user lost their identity, so the security of biometric data is more important. Biometrics contains sensitive personal information this is another type threat. [9][10][11] Shown that fingerprints hold some genetic information. Ratha et al. [12]find out the different type of attack that can be produce against a biometric system (i) the artificial finger used at the sensor using false biometric attribute, (ii) the biometric data resubmitted which is modified

by attacker (iii) Biometric feature extractor may be swapped by a Trojan horse program that produces prearranged biometric attribute sets, (iv) real biometric set of attribute may be replaced with fake set of biometric attribute, (v) Trojan horse program replace the matcher which create a problem at the verification time so the security required for biometric security, (vi) the biometric data stored in the database may be modified or removed, or new biometric data may be inserted in the database, (vii) the final result output by the biometric system may be dominated and (viii) the data may be modified in the network at time when various Communication channel communicate with biometric system. An artificial biometric (such as an artificial finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of attack. The biometric data detector do not take the real values obtained from the sensor but instead it is forced to generate the value which is given by the attacker. The biometric attribute extracted using the data obtained from the sensor is replaced with a fake biometric attribute set. The matcher component could be attacked to produce high or low matching scores, regardless of the input biometric set. The channel between the database and matcher could be negotiated to alter transferred biometric data. One of the attacks is to change the final matcher result itself. All of these attacks have the risk to reduce the integrity of a Biometric system [13]. Sun et al. [14] projected a template called KMT, or Key-Mixed Template. The basic idea behind the projected template is to use the template in combination with a secret key to create a new Biometric template. Template and secret key is combined at the use end and verified at the server side with database. By having a separate secret key per verification system, having a template compromised does not necessarily mean the attacker can gain access to all systems that use that biometric template. This new template can help to prevent backend attacks, snooping, and tamper attacks without a performance hit. Andrew B. J. Teoh et al. [15] was proposed the concept of cancelable biometrics to express biometric templates that can be cancelled and restored with the addition of another independent authentication factor. A kind of cancelable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The quantized random projection collection on basis of the Johnson-Linden strauss Lemma was employed to accomplish the mathematical foundation of Bio Hash. Depending upon this model, they have explained the characteristics of BioHash in pattern recognition in addition to security viewpoints and provided some methods to resolve the stolen-token problem. [16] The two major requirement of biometric template protection is cryptosystem and cancelable biometrics which is also known as helper database and feature transformation respectively

Incapable of being reversed: It may be impossible to reconconstruct the secure biometric template from stored referenced biometric data (feature). While normal biometric template can be easily generated.

Observability: multiple versions of protected biometric secure template not allow to reconstruct while normal Templates can be regenerated by same biometric data.

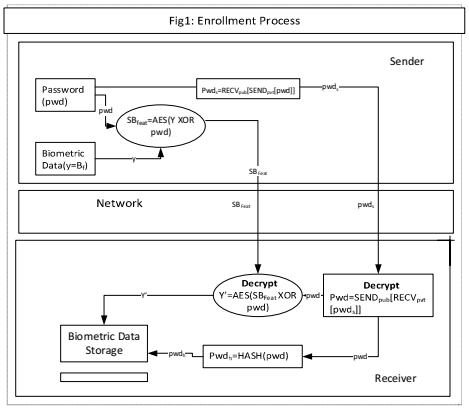
III. NOTATIONS

In this paper we are using the following notations:

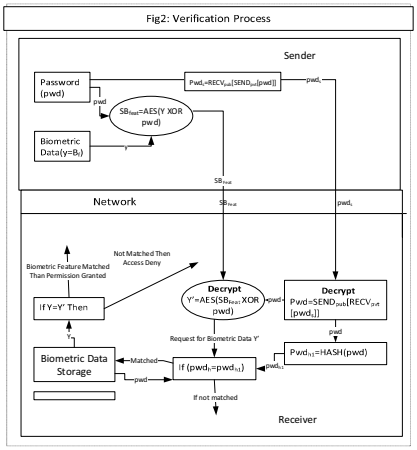
B_f for Biometric Feature by nature, y for combined sensing, feature extraction and quantization, SB_{Feat} for secure biometric feature, $send_{pvt}$ for sender private key, $send_{pub}$ for sender public key, $recv_{pvt}$ for receiver private key, $recv_{pub}$ for receiver public key, pwd for password, pwd_s for secure password, pwd_h for hash value of stored password

IV. BLOCK DIAGRAM

Enrollment process: In this process we need a user biometric feature and password. The password used as a key for AES algorithm. Received password (pwd) and biometric feature (B_f) are encrypted with help of AES Algorithm. Encrypted cipher text SB_{feat} is send via public channel and password send through public channel. This process shown in the following figure (Fig1)



Verification process: Fig2 shows that the biometric data is fetch from the database, if the hash value of sender password and hash value of stored password is matched.



V. EQUATIONS

Sender Side:

$$\sum_{i=0}^{n} B_f \qquad (1)$$

$$SB_{feat}=E^{AES(Y,pwd)} \quad (2)$$

$$pwd_{s'} = E^{k(send_{pvt})}(pwd) \quad (3)$$

$$pwd_s = E^{k(recv_{pub})}(pwd_{s'}) \quad (4)$$

Receiving Side:

$$pwd_{s'} = D^{K(RECV_{pvt})}(pwd_s) \quad (1)$$

$$pwd = D^{K(send_{pub})}(pwd_{s'}) \quad (2)$$

$$Y' = D^{AES(SB_{feat},pwd)} \quad (3)$$

$$pwd_h = HASH(pwd) \quad (4)$$

VI. Algorithm Follow By Security for Stored Biometric Data

Enrollment process:

Step1 Accept biometric data and password from user.

Step2 Accepted data B_f from user are secure via AES algorithm and the password used as a key. Finally the Encrypted data SB_{feat} output as a cipher text. The cipher text send to the destination via public channel.

Step3 Password is secured by sender's private key after that secured by receiver's public key. Resultant secure key pwd_s send to the destination via public network

Step4 SB_{feat} and pwd_s are accepted by receiver.

Step5 pwd_s Decrypt into original password for further processing.

Step6 SB_{feat} decrypted into normal data and store it into system database.

Step7 Generate a hash code pwd_h from pwd and store it.on system database

Request for verification:

Step1 Enter biometric data.

Step2 For any communication or data fetching from the system database, System require the biometric data and password, which had given at the time when user enrolled so both biometric data and password are received by the system.

Step3 Accepted user biometric data (B_f) and password (pwd). AES (B_f, pwd) generate a secured biometric data SB_{feat} (Cipher text) where pwd is used as a key for algorithm and send it to destination via public network

Step4 Password (pwd) is secure by public key cryptography (sender private keyand receiver public key) and generated pwds send to the destination via public channel

Step5 SB_{feat} and pwd_s are accepted by receiver.

Step6 pwd_s converted into normal data for further processing.

Step7 SB_{feat} decrypted into normal data.

Step8 Before fetching data from system database system require authentication.

Step9: Generate hash code from pwd_{h1} from current received password (pwd) and send request for stored hash value of old password.

Step10: if ((stored password)pwd_h = pwd_{h1} (current password)){Match then
Requested biometric Data fetch from System database}
Else ($pwd_h \neq pwd_{h1}$) then
{The request is denied
For biometric data.}

Step11:(If *Y (stored data) =Y' (accepted data)) then {*
Access is granted.}
(If Y *(stored data)* ≠Y' *(accepted data)*) then {
Access Denied}

VII. Conclusion

We have discussed how to secure stored biometric data. We have specifically highlighted techniques that can secure biometric feature from attacker or unauthorized person. We discuss the importance of Public Key Cryptography and AES principles to enhance the confidentiality of biometric data. Security for stored biometrics may be used to protect the stored biometric data when the user's biometric data is compromised. Also, this technique provides security at the time when user claim for their biometric data for verification process. The verification process is also undergoing via security process.

References

[1] A. K. Jain, A. Ross and U. Uludag. "Biometric Template Security Challenges and Solutions". Proc. European Journal, September 2005.

[2] A.K. Jain, K. Nandakumar, and A. Nagar,"Biometric Template Security",Proc. EURASIP Journal on Advances in Signal Processing, Article ID 579416 ed, New York, NY, United States, January 2008

[3] Rudolf M. Bolle, Jonathan Connell, Sharathchandra Pankanti, Nalini K. Ratha, Andrew W. Senior
"Biometrics 101," IBM Research Report, RC22481, June 10, 2002

[4] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar, "Handbook of Fingerprint Recognition", *New York: Springer-Verlag,* New York, 2003.

[5] Keuning, Ton van der Putte and Jeroen, "Biometrical fingerprint recognition: Don't get your fingers burned," *Academic Publishers* New York: Kluwer, 2000.

[6] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," *Proc. SPIE, Vol. 4677*, Optical Security and Counterfeit Deterrence Techniques IV, 275, April 18, 2002.

[7] Hill, Chris J, "Risk of Masquerade Arising from the Storage of Biometrics" *Australian National University: s.l. Bachelor of science thesis*, Dept. of CS, Nov 2002.

[8] Schneier.,"Bruce., Inside risks: The uses and abuses of biometrics," *Communications of the ACM*, Vol 42 ed, ACM New York, NY, USA, August 1999.

[9] Babler, "W.J, Embryologic development of epidermal ridges and their configuration," *Birth Defects Original Article Series*, Vol. 27(2). ed., New York, 1991.

[10] Mulvhill, J.J, "The genesis of dermatoglyphics," *Published by Elsevier Inc,* 4 ed, October 1969.

[11] Penrose, L.S. "Dermatoglyphictopology," *Nature,* Vols. 205:545–546 ed, s.l, 06 February 1965.

[12] N. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," *Proc. Audio and Video-based Biometric Person Authentication(AVBPA)*, pp. 223–228 ed, June 2001

[13] U.Uludag, A.K.Jain, "Hiding biometric data," *IEEE Transactions On Pattern Analysis And Machine Intelligence,* 11 ed., Michigan State Univ., USA, Nov.2003,

[14] S. Sun, C Lu, and P. Chang, "Biometric Template Protection: A Key Mixed Template Approach," Digest of Technical Papers. International Conference, Las Vegas, NV: Consumer Electronics, 2007. ICCE 2007, 10-14 Jan. 2007.

[15] Teoh AB, Yuang CT, "Cancellable Biometrics Realization with Multispace Random Projections", *IEEE Trans Syst,* pp:1096-106, ed, 2007.

[16] Christian Rathgeb and Andreas Uhl, "A survey on Biometric Cryptosystems and Cancelable Biometrics," *EURASIP Journal on Information Security*, Austria, 2011.