International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec 2018 www.irjet.net p-ISSN: 2395-0072

A Review on Security Attacks in Biometric Authentication Systems

Arpita Sarkar[1], Binod Kr Singh[2]

[1,2]*Dept. of CSE, NIT Jamshedpur, India*

Abstract - *Biometric authentication system is a provable solution in identity management system. Different representations of identity such as passwords and ID cards are not sufficient for reliable identity management as they can be easily misplaced, shared, or stolen. On the other hand biometric recognition authenticates a person on basis of his/her anatomical and behavioral traits. There are certain increasing concerns about the security and privacy of this biometric authentication system. These systems are vulnerable to different security attacks. These security issues related to recognition system is need to be addressed for the noble purpose of ensuring integrity and public acceptance of these systems. This paper presents a review on different attacks of biometric authentication systems. These attacks may compromise the biometric template resulting in reducing the security of the system and motivates to study existing biometric template protection techniques to resist these attacks.*

Key Words: Biometrics authentication systems, Biometric Attacks, Biometric Traits, Biometrics Template security, Template Protection Techniques.

1. INTRODUCTION

Traditional authentication techniques such as passwords, pin number, token number, ID cards has been used to validate the identity of an individual. User must have to remember passwords or pin number. So these methods of identity management can be forgotten, stolen or hacked by an attacker. The advantage of biometrics over traditional authentication scheme is biometrics is determining an identity based on the physiological or behavioral traits of an individual. These traits include fingerprints, facial features, iris, hand geometry, voice, signature, etc. So for establishing identity in biometrics user no need to remember any password, pin number or carry any token or ID card. Biometric traits have a number of advantageous properties with value to their use as an authentication token, namely, reliability, convenience, universality, and so forth. These characteristics have led to the well-known operation of biometric authentication systems. There are still some issues concerning the security of biometric recognition systems that need to be addressed in order to make sure the integrity and public receipt of these system. A typical biometric authentication system [2] is broadly categorized in five different modules sensor, feature extractor, template database, matcher, and decision module. A pictorial representation of biometric authentication system is represented in Figure 1.

Sensor: -It is the interface between the user and the authentication system. It scans the biometric trait of the user.

Feature extraction module:- This module extracts the salient feature from scanned biometric data. It is useful in distinguishing between different users. In some cases, the feature extractor is preceded by a quality assessment module which determines whether the scanned biometric trait is of sufficient quality for further processing.

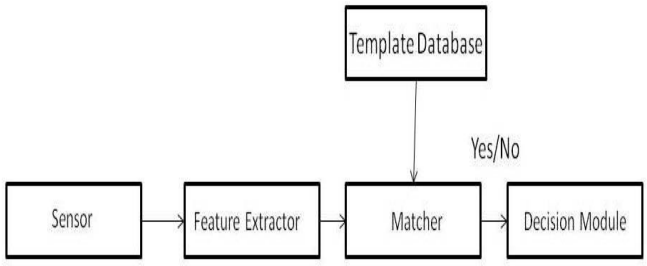

Fig:-1 Biometric Authentication Systems

Template database: - The extracted feature set is stored in a database as a template indexed by the user's identity information.

Matcher module:-It is usually an executable program, which accepts two biometric feature sets one is stored template from template database and a query template as inputs, and outputs a match score indicating the similarity between the two sets.

Decision module: - It takes the identity decision and initiates a response to the query whether it is accepted or rejected.

The rest of the paper is systematized as follows: A review of different attacks in biometric systems is discussed in Section 2. Section 3 deliberates about the reason of biometric system failure. The effects of system failure are discussed in Section 4. Countermeasures to different attacks are discussed in section 5. Finally, there is a conclusion at Section 6.

2. ATTACKS IN DIFFERENT MODULE OF BIOMETRIC SYSTEMS

Biometric systems offer great advantages over traditional systems but they are vulnerable to attacks [1,2,3,4]. One of such attacks is adversary attacks. Adversary attacks generally take advantage of the system vulnerabilities at one or more modules or interfaces. Different modules are (i) user interface , (ii) interfaces between modules, (iii) software modules, and (iv) template database.

2.1. Attacks at the user interface

When the sensor is unable to different between fake and genuine biometric trait the adversary take advantage of it and easily intrudes the system using a false identity. Liveness detection is of probable solution for resisting such kind of attacks.

2.2. Attacks at the interface between modules

An adversary can place a jammer to obstruct a wireless interface and intercept or modify the data being transferred through some insecure channel. Communication channel can be secured by cryptographically encoding all the data sent through the interface using public key infrastructure, because insecure channel are vulnerable to different security attacks like hill climbing or replay attack. But in spite of using encoding data an adversary can perform a replay attack by intercepting the encrypted data passing through the interface when a legitimate user is interacting with the system. Whenever attacker wants to break a system use the intercepted data to the desired module. Timestamp or challenge/Response mechanism can be used to resist such kind of replay attacks.

2.3. Attacks on the software modules

Adversaries can change the executable program at a module such that it always outputs the values desired by the adversary. These types of attacks are known as Trojan-horse attacks. For this purpose secure code execution practices or specialized hardware which can enforce secure execution of software are used. Another component is related to algorithmic integrity. This implies that the software should be able to handle any input in a desirable manner. This vulnerability might not affect the normal functioning of the system but an adversary can exploit this loophole to easily breach the security without being noticed.

2.4. Attacks on the template database

This kind of attack is one of the most potentially damaging attacks on a biometric system. Biometric templates stored in the system database can lead to the following three vulnerabilities.

- A template can be replaced by an impostor's template to gain unauthorized access.
- A physical spoof can be created from the template to gain unauthorized access to the system as well as other systems which use the same biometric trait).
- The stolen template can be replayed to the matcher to gain unauthorized access.

Cross matching is one of such potential abuse of biometric identifiers where the biometric identifiers are used for purposes other than the intended purpose. For example a fingerprint template stolen from a bank's database may be used to search a criminal fingerprint database or crosslink to person's health records. Passwords and PIN have the property that if they are compromised, the system administrator can issue a new one to the user. This same property of cancelability or revocability is also desirable with biometric templates.

3. REASON OF BIOMETRIC SYSTEM FAILURE

The modes failure of a biometric system can be categorized into two classes: intrinsic failure and failure due to an adversary attack. Intrinsic failures occur due to inherent limitations in the sensing, feature extraction, or matching technologies as well as the limited discriminability of the specific biometric trait. When a resourceful hacker attempts to hack the biometric system for personal gains that is known as adversary attack. This type of attacks can be classified into three types. These factors include system administration, nonsecure infrastructure, and biometric overtness.

3.1. Intrinsic failure

When the biometric system takes an incorrect decision and due to this security lapse is known as intrinsic failure. In a biometric verification systems two types of errors are there namely false accept and false reject. A legitimate or authenticate user may be falsely rejected by the biometric system due to the large differences in the user's stored template and query biometric feature sets (see Figure 4). These intrauser variations may be due to incorrect interaction by the user for example changes in pose and expression in a face image or due to the noise introduced at the sensor. False accepts are usually caused by lack of individuality or uniqueness in the biometric trait which can lead to large similarity between feature sets of different users. Most of the cases intrauser variations and interuser similarity may also be caused by the use of nonsalient features and nonrobust matchers. Sometimes, a sensor may fail to acquire the biometric trait of a user due to limits of the sensing technology or adverse environmental condition. Sometimes it may happen that a fingerprint sensor may not be able to capture a good quality fingerprint of dry/wet fingers. This is the reason behind failure-to-enroll (FTE) or failure-to-acquire (FTA) errors occurs. On the other hand zero-effort attack, a serious threat which occurs when the false accept and false reject probabilities are high. Further research is needed at reducing the probability of intrinsic failure by designing of new sensors that can acquire the biometric traits of an individual in a more reliable, convenient, and secure way. Further development of invariant representation schemes and robust and efficient matching algorithms, and use of multibiometric systems are need to be developed.

3.2. Adversary attacks

In this attack an adversary intentionally stages an attack on the biometric system and can be successful if there is any drawback in the system design and the availability of adequate computational and other resources to the adversary. Adversary attacks are also categorized into three

main classes namely administration attack, non secure infrastructure, and biometric overtness.

3.2.1 ADMINISTRATIVE ATTACK

The administrative attack occur due to the improper administration of biometric recognition system. Suppose the system administrator have the privileges to register the biometric template and make the exceptions for the individual whose biometric sample cannot be obtain by the system due to some injury or disease then this type of attack may occur. This attack may be occur using the integrity at the time of enrolment process by the administrator or a authorize user or may be improper processing procedure.

3.2.2 NON SECURE INFRASTRUCTURE

Hardware infrastructure, software infrastructure or communication channel of different module of a biometric system are the reason of non secure infrastructure. An opponent can attack the biometric infrastructure by various way so that the security may be break through the biometric infrastructure. Ratha et al.[6,7] identified eight different point of attack in a generic biometric system. Anil K. Jain et al. [3,4,5] categorize the different types of biometric infrastructure attack into following four categories which are already discussed in section 2

3.2.3 BIOMETRIC OVERTNESS

When an opponent can acquire the biometric traits of legitimate user and use them to create copy of that biometric trait to gain some unauthorized access causes this type of attack. In this situation biometric system cannot identify or distinguish live biometric trait and physically artificial spoof.

4. EFFECTS OF BIOMETRIC SYSTEM FAILURE

Biometric system failure can lead to two main effects firstly denial-of-service and secondly intrusion.

Denial of service is kind of active attack where an authorized user is prevented from avail services that are assigned to him. An opponent can cause harm to the infrastructure so preventing these users from accessing the system. Native failures like false reject, failure-to-capture, and failure-to-acquire lead to such a denial-of-service.

Intrusion refers to an attack where an unauthorized person gaining illegal access to the system which results in defeat to privacy. Biometric system vulnerability like intrinsic failure, administrative abuse, nonsecure infrastructure, and biometric overtness can results in intrusion.

5. COUNTERMEASURE TO SECURITY ATTACKS

All the techniques used for resisting attacks in biometric systems are discussed in this section.

5.1. Liveness detection

This technique is use to prevent attacks at sensor. Liveness detection can detect that input sample feature is provided by live human being or not. It can distinguish between real input sample feature provided by living human being and a fake input feature provided by an artifact. Liveness detection can be applied using software or hardware means. Use of extra hardware to implement means to measure various life signs like pulse detection, blood pressure, temperature for fingerprints and movements of face, eyes for face recognition. The limitation of using extra hardware makes the system too much expensive. Using software means to use the information already captured to detect life signs. The only used method is to use information about sweat pores. For this a scanner that can acquire a high-resolution image is required. It is practically impossible to reproduce the exact size and position of the pores on an artificial mold.

5.2. Biometric cryptosystems

This technique combines biometrics and cryptography to take advantages from the strengths of both the fields [4]. This is used for securing the biometric template. Cryptography provides higher degree of security and biometrics eliminates the need to remember any passwords or to carry any tokens. Biometric cryptosystems are subdivided into key generation and key binding [8]

- Key generation: In this helper data is only obtained from the biometric traits and the cryptographic key is directly generated from the helper data.
- Key binding: In this helper data is obtained by binding a key with biometric template.

5.3. Steganography and Watermarking

Steganography and watermarking are used to prevent attacks on attack points on the channel between sensor and feature extractor and attack on channel between matcher and application device. These two techniques are same in their hiding method, but differ in the characteristics of the embedded data, host image and medium of data transfer. Watermarking is used in the authentication of ownership claims. Steganography can be used for transferring critical biometric information from a client to a server.

5.4. Cancellable biometrics

Cancellable biometrics is a technique that involves intentional and systematic distortion of biometric template based on a selected non-invertible transform [10]. If transformed template is stolen or hacked then it can be cancelled and re-issued by changing parameters of template. Cancellable biometrics is used to prevent attacks at template database.

5.5. Visual Cryptography

Recently, various approaches that utilize visual cryptography [9] to secure the stored template and impart privacy to the central databases have been introduced. The use of visual cryptography is explored to preserve the privacy of biometric data by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available, further, the individual component images do not reveal any information about the original image. In this process during the enrolment process, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two images and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are superimposed in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking , steganography , or cryptosystem approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image. Naor and Shamir [21] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

5.6. Homomorphic Encryption:

This technique was first introduced into biometrics by Ye et al[11]. Homomorphic encryption (HE) schemes allow a "limited subset of computation on the encrypted data."Combining HE with biometric recognition systems would meet the requirements of template protection schemes without degrading the accuracy. Ye et al. [11] presented "Anonymous Biometric Access Control (ABAC)" which uses "k-Anonymous Quantization (kAQ) framework." kAQ uses a lookup table to recognize k candidates. HE-based matching protocol is applied on these k candidates. Erkin et al. [21] proposed a privacy-preserving face recognition system for eigen-faces by using the "Paillier homomorphic encryption scheme". Later, Sadeghi et al. [12] improve the efficiency of this system. Rane et al. [13] presented Hamming distance calculation for fingerprint applications. Barni et al. [14,15,] demonstrated a distributed biometric system by exploiting "cryptosystems, homomorphic encryption on Fingercode templates in a semi-honest model." Osadchy et al. [16] proposed a "secure hamming distance based HE for face biometrics. The system is called SCiFI". Kulkarni et al. [17] proposed a HE method by calculating values stored on server by performing XOR operation between biometric template vector and corresponding user's key. Karabat et al. [18] introduced "THRIVE: threshold homomorphic encryption based secure and privacy-preserving biometric verification system" that is applicable to any biometric. Barrero et al. [19] presented a "Paillier's homomorphic probabilistic encryption" on online signature systems.

6. CONCLUSION

In this paper a biometric authentication system along with its modules and then various security attacks on biometric systems are discussed. It is also found that most of the attacks makes target to the biometric templates which are stored in database. This paper also discussed various techniques to oppose attacks that can be used to protect biometric templates and also brief about the reason and effects of biometric system failure. There are few techniques available for biometric template protection scheme like steganography, watermarking, cancellable biometrics, biometric cryptosystems and visual cryptography which are also discussed. It is found that there is no security technique which can satisfy all the properties of an ideal biometric template protection scheme. There is still need to do research effort in this field so that a proficient and foolproof security technique is designed.

REFERENCES

[1] Raffaele Capplellin, Alessandra Lumini. Darion Maio, "Fingerprint Image Reconstruction from Standard Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No.9, pp. 1489-1503, 2007.

[2] Arun Ross, Anil Jain, "Biometric Sensor Interoperability: A Case Study in Fingerprints", Proc. of international ECCV Workshop on Biometric Authentication (BioAW), LNCS Vol. 3087, pp 134-145, Springer Publisers, May 2004.

[3] Jain, A.K., Uludag, U., Ross, A.: Biometric template selection: a case study in fingerprints. In: Proc. of 4th Int'l Conf. on Audio and Video-based Biometric Authentication (A VBP A).Volume LNCS 2688., Guildford, UK, Springer (2003) 335–342.

[4] Anil K. Jain, karthik Nandakumar, and Abhishek Nagar, "Review article Biometric Template Security", Hindawi Publihing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008, Article ID 579416, 17 pages, doi: 10.1155/2008/579416.

[5] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.

[6] Nalini K. Ratha, Shaoyun Chen, and Anil K. Jain. "Adaptive flow orientation based texture extraction in finger print images". Pattern Recognition, Vol. 28, 28(11): 1657–1672, November 1995.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01), pp. 223–228, Halmstad, Sweden,June 2001.

[8] Shenglin Yang, Ingrid Verbauwhede, "Automatic Secure fingerprint verification system based on fuzzy vault scheme",Proceedings in (ICASSP '05). IEEE InternationalConference on Acoustics, Speech, and Signal Processing, pp- v/609 - v/612 Vol. 5, DOI-10.1109/ICASSP.2005.1416377, 2005

[9] A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, March 2011. doi: 10.1109/TIFS.2010.2097252

[10] N. Ratha, J. Connell, R. M. Bolle and S. Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints," 18th International Conference on Pattern Recognition (ICPR'06), Hong Kong, 2006, pp. 370-373. doi: 10.1109/ICPR.2006.353

[11] S. Ye, Y. Luo, J. Zhao, S.C.S. Cheung, Anonymous biometric access control. EURASIP J.Inf. Secur. 2009, 2:1–2:17 (2009)

[12] A.R. Sadeghi, T. Schneider, I. Wehrenberg, Efficient privacy-preserving face recognition, in Information, Security and Cryptology (Springer, Berlin, 2009), pp. 229–244

[13] S.D. Rane, W. Sun, A. Vetro, Secure distortion computation among untrusting parties using homomorphic encryption, in 16th International Conference on Image Processing (ICIP)(2009), pp. 1485–1488

[14] M. Barni, T. Bianchi, D. Catalano, M.D. Raimondo, R.D. Labati, P. Failla, D. Fiore, R.Lazzeretti, V. Piuri, A. Piva, F. Scotti, A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates, in International Conference on Biometrics: Theory Applications and Systems (BTAS) (2010), pp. 1–7

[15] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore,R. Lazzeretti, V. Piuri, F. Scotti et al., Privacy-preserving fingercode authentication, in Proceedings of the 12th ACM Workshop on Multimedia and Security (2010), pp. 231–240 M.

[16] Osadchy, B. Pinkas, A. Jarrous, B. Moskovich, SCiFi-a system for secure face identification, in Symposium on Security and Privacy (SP) (2010), pp. 239–254

[17] R. Kulkarni, A. Namboodiri, Secure hamming distance based biometric authentication, in International Conference on Biometrics (ICB) (2013), pp. 1–6

[18] C. Karabat, M.S. Kiraz, H. Erdogan, E. Savas, Thrive: threshold homomorphic encryption based secure and privacy preserving biometric verification system. EURASIP J. Adv. Signal Process. 2015(1), 1–18 (2015)

[19] M. Gomez-Barrero, J. Fierrez, J. Galbally, Variable-length template protection based on homomorphic encryption with application to signature biometrics, in 4th International Conference on Biometrics and Forensics (IWBF) (2016), pp. 1–6

[20] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.

[21] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, T. Toft, Privacy-preserving face recognition, in Privacy Enhancing Technologies (Springer, Berlin, 2009), pp. 235–253