Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 2 ~ Issue 11 (2015) pp: 04-07
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Investigation of the Security and Privacy of Biometric Data

[1]Godwin Okechukwu Ogbuabor, [2]Okwo Josephat Ani
[1]*Department Of Computer Science, Michael Okpara University of Agriculture, Umudike*
[2]*School of Science and Technology National Open University of Nigeria*

ABSTRACT:- The growing use of biometric has given concern on the privacy and security of the stored biometric data. Due to the uniqueness of biometric feature of individual, if the template is compromised, is not possible to replace it. Biometric data is the extracted biometric features stored in a central database or smartcard which can be used to identify or verify individuals. The biometric data are the major target of the hackers which can be at the database level or the interconnecting channel level. Unlike password, when biometric data are compromised, it is not possible for the legitimate user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. Due to this irrevocable nature of biometric data, an attack against the stored templates constitutes a major security and privacy threat in a biometric system. The goal is to investigate the strategies to enhance security of the biometric data; it should be computationally difficult to recover the original biometric template from the stored template. This will go a long way to ensure that hackers do not fabricate a physical spoof of the biometric treat from the stolen template.

Keywords:- Biometric Data, Security, Privacy

I. INTRODUCTION

Biometric data is widely used in systems that attempt to identify a specific user or other human through unique characteristics. Computer image processing is one form of biometric analysis that uses biometric data. Digital fingerprint analysis also relies on the use of biometric data for identification purposes. In most biometric analysis systems, there is demand for a large amount of biometric data. This data must be stored and somehow secured from unauthorized access. These systems rely on complex algorithms that sort data in ways that will achieve an identifying result in a given application. Developers use key features that are unique from one person to another in order to make biometric identification effective (Janssen, 2014).

Some of the questions raised about the use of biometrics data, particularly in connection with authentication, relate to the trust that can be placed in the biometric authentication process itself, or to the protection of the biometric data that is used by the system and which is private and personal to the users. It is this latter concern that marks out biometric systems as different from the traditional password, PIN and token based authentication technologies.

The success that biometric technology and systems have in meeting the tough security challenges they face will be crucial in determining their suitability for use by organizations. Many government applications will demand high levels of trust in the authentication process with widespread interaction with citizens, the privacy and data protection issues will assume major significance. For example, a user providing a fingerprint for the purpose of authenticating an e-vote will want to be assured that an impostor cannot masquerade as him/her, and that the data is not being supplied to a 3rd party (e.g. the police) for checking against a criminal database.

The aim of this paper is to explore these issues in more detail, highlighting a number of commonly expressed security concerns, discussing the possible threats that they pose, and what can be done to eliminate or at least mitigate them.

II. BIOMETRIC SECURITY THREATS

The features extracted from the individuals are sensitive information that is unique to the person. If the template is stolen, is stolen forever since it has no duplicate. This has raised security issues about the use of biometric for identification and verification of individuals. Applications available on the web can be accessed by anybody that has internet connectivity; both good and bad personalities have access to the system. Since this is available online, there are serious security threats. Hackers and attackers can gain access to the database and compromise the templates.

Attacks

Ratha et al (2001) identified eight possible attacks in biometrics system. These possible attacks are discussed below

1. Presenting fake biometrics at the sensor: reproduction of the biometric feature is presented as input to the system in this mode of attack e.g. fake finger.
2. Resubmitting previously stored digitized biometrics signals: In this mode of attack, a recorded signal is replayed to the system, bypassing the sensor e.g. the presentation of an old copy of a fingerprint image.
3. Overriding the feature extraction process: in this mode, the feature extractor is attacked using a Trojan horse, so that it produces feature sets preselected by the intruder.
4. Tampering with the biometric feature representation: The features extracted from the input signal are replaced with a different, fraudulent feature set (assuming the representation method is known). Often the two stages of feature extraction and matcher are inseparable and this mode of attack is extremely difficult. However, if minutiae are transmitted to a remote matcher (say, over the Internet) this threat is very real.
5. Corrupting the matcher: The matcher is attacked and corrupted so that it produces preselected match scores.
6. Tampering with stored templates: The database of stored templates could be either local or remote. The data might be distributed over several servers. Here the attacker could try to modify one or more templates in the database, which could result either in authorizing a fraudulent individual or denying service to the persons associated with the corrupted template. A smartcard-based authentication system, where the template is stored in the smartcard and presented to the authentication system, is particularly vulnerable to this type of attack.
7. 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.
8. Overriding the final decision: If the final match decision can be overridden by the hacker, then the authentication system has been disabled. Even if the actual pattern recognition framework has excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the match result.

Countermeasures

Ratha et al (2001) also presented the following countermeasures to prevent the possible attacks identified in biometric system.

1. Finger conductivity or fingerprint pulse at the sensor can prevent attackers from presenting fake biometrics at the sensor.
2. Encrypted communication channels will go a long way eliminating attack on the biometric features.
3. Encrypting the extracted template will prevent using the template to gain access except if the hacker has the encryption key.

Template Protection

To properly protect the biometric template, the protection techniques should have the following properties as outline by Jain et al (2008).

a. **Diversity**: The protected template should by no means allow cross matching in the databases. This is to ensure that user's privacy is not compromised.
b. **Revocability**: It should be possible to revoke a template when it is compromised by the hackers and reissue different one based on the biometric information.
c. **Performance:** The template protection techniques should not reduce the performance of the system.
d. **Security**: it should be computationally difficult to recover the original biometric template from the stored template. This will go a long way to ensure that hackers do not fabricate a physical spoof of the biometric treat from the stolen template.

The template protection techniques can be classified into two categories: Feature transformation and bio cryptosystem.

Biometric Feature Transformation

Here, transformation function is applied to the biometric data and the transformed template is stored in the database (Jain et al., 2008). The transformation function may have different characteristics and use certain parameters such as password. During verification, the verification feature set is equally transformed in the same way as the enrolment template and the comparison of the fingerprint takes place in the transformed space (Maltoni et al., 2009).

This category can be divided into two: Non-invertible transform and Salting

Non-invertible transform

This category usually applies a one-way function to the unprotected template in such a way that it will be computationally difficult to reverse the protected template even when any of the parameters of the transforms are stolen or revealed (Maltoni et al, 2009).

This technique provides better security than Salting since it is very difficult to recover the original biometric template even if the template is compromised (Jain et al., 2008).

Hashing technique is used in password based authentication system; in this case password is hashed and stored in the database on the process of enrolment. Then during verification, the user also enters the same password and it is hashed and compared with the existing password.

It will be very difficult to recover the original password even if the exact transformations as well as transformed password are known since the transformation is non-invertible in the cryptographic point of view (Maltoni et al., 2009).

In the same way, it can be applied in fingerprint. Instead of storing the template of the fingerprint, the hashes of the template should be stored; then during verification, the verification feature set is also hashed and compared in the non-invertible transform space. But significant different exist between password and fingerprint. "Password are exactly the same during different authentication attempts, but fingerprint image at different acquisitions (different verification attempts) are never identical, and this prevent the same hash to be obtained" (Maltoni et al., 2009). Therefore, matching in the non-invertible transform space is big problem. Recovering the correct alignment between the two fingerprints: the template and the query feature set is a major problem in comparing hashed fingerprint templates (Maltoni et al., 2009). One method to solve this problem is to pre-align the feature set before the transformation (e.g. registering them with respect to the core point).

Salting

In this approach, biometric features are transformed using a function defined by a user-specific key or password. The transformation is invertible to some extent, therefore the key need to be securely stored or remembered by the user and present it during authentication (Jain et al., 2008). The need for additional information in form of key increases the entropy of the biometric template, therefore, makes it difficult for hackers to guess the template. The Entropy of biometric template is a measure of the number of different identities that are distinguishable by a biometric system (Jain et al., 2008). In this approach multiply templates can be generated for the same user (diversity) by using different keys since the key is user specific. Again if template is compromised, it can be replaced by generating new template (revocability).

Biometric Cryptosystem

These techniques were originally designed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features (Jain et al., 2008). They can also be used as a means of biometric template protection. Here, some details about the biometric template are stored in the database. These details are known as helper data; therefore, biometric cryptosystem is also referred to as helper data-based method.

This technique can be further classified into two categories: Key generation and Key binding.

Key-Binding Biometric Cryptosystem

In this approach, a cryptographic and an unprotected fingerprint template are bonded together within a cryptographic framework to generate the helper data. It is computationally difficult to decode the key or the template from the helper data without the knowledge of the user's fingerprint data. The helper data is usually obtained associating the enrolment template with codeword obtained from an error correcting code using the key as the message. A codeword recovered from a feature set that is similar but not identical to the template is affected by a certain amount of error correction code, the exact key is recovered from the codeworld that contain some errors. If the correct key is recovered, it means that the feature set and the protected template result in a match (Maltoni et al., 2009).

Key Generation Biometric Cryptosystem

A key is derived directly from the biometric signal in this approach. The major advantage is that there is no need for user-specific keys or tokens as required by 'Biometric Salting approach'. But the problem with this approach is that is very hard to generate key with high stability and entropy.

III. CONCLUSION

Biometric data are not usually held in isolation. They are typically associated with other personal data that may form part of the identification and authentication process itself. Associated data is normally not unique

to biometric authentication systems, and is commonly stored centrally on nonbiometrics applications, not apparently eliciting equivalent concern.

A potential solution can be achieved by storing of personal data on secure tokens or smart cards that are held by the users themselves. The assumption is that this will obviate the need for a central database of biometric data, and therefore negate any privacy concerns. This is attractive because it promotes the idea of anonymous authentication.

However, anonymous authentication has its limits and may not be tenable in many circumstances. For example in government applications, it will typically not be sufficient to know that the person applying for the benefit payment/passport/driving license is who they claim to be. It will also be necessary to check that they are entitled to the service or payment requested and not enrolled multiple times under different identities. To do this a central database of claimants will almost certainly be needed, even if a token or smart card is used as part of the authentication process. In these cases, the privacy protection advantage ascribed to user-held tokens or smart cards will be largely illusory.

To mitigate the risk of functional creep, the biometric data can be bound to the application through the use of cryptographic signature techniques.

REFERENCES

[1]. Ahmad, S. M., Ali, B. M., & Adnan, W. A. (2012). TECHNICAL ISSUES AND CHALLENGES OF BIOMETRIC APPLICATIONS AS ACCESS CONTROL TOOLS OF INFORMATION SECURITY. International Journal of Innovative Computing, Information and Control, 8(11).

[2]. Jain, A., Ross, A., & Uludag, U. (2005). BIOMETRIC TEMPLATE SECURITY: CHALLENGES AND SOLUTIONS. proceedings of European Signal Processing Conference .

[3]. Jain, A., Nandakumar, K. & Nagar, A. (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing, pp. 1-17.

[4]. Janssen, C. (2013). Biometric Data. Retrieved January 2, 2015, from http://www.techopedia.com/definition/26991/biometric-data

[5]. Kaur, M., Sofat, D. S., & Saraswat, D. (2010). Template and Database Security in Biometrics Systems: A Challenging Task. International Journal of Computer Applications.

[6]. Maltoni, D., Maio, D., Jain, A. & Prabhakar, S.(2009). HandBook of Fingerprint Recongnition. 2nd ed. s.l.:Springer.

[7]. Ratha, N., Connell, J. & Bolle, R.(2001). Enhancing Security and Privacy in Biometric-based Authentication Systems. IBM Systems Journal.

[8]. Vetro, A., Draper, S., Rane, S., & Yedidia, J. (2009). Securing Biometric Data. MITSUBISHI ELECTRIC RESEARCH LABORATORIES.

[9]. Yakubu, O., & Adjei, O. (2014). Reliability of Fingerprint Verification in Ghana. International Journal of Computer Applications, 107(10).