Security in e-Governance using Biometric

Piyush Morwal
MSc CS
Department of Computer Science, Central University of Rajasthan
Ajmer, India

Parvinder Singh
M Tech
Department of Computer Science and Engineering, Central University of Rajasthan
Ajmer, India

Rajkumar Tripathi
MSc CS
Department of Computer Science, Central University of Rajasthan
Ajmer, India

ABSTRACT
e-Governance is refers to the use of Information and communication technology to provide the improvement in government services, transactions, interaction with citizens, business and other arm of government. In this paper we identify the requirements of biometrics in e-governance and what are the possible attacks on biometric systems. We also provide some scheme to reduce the vulnerabilities in the system. We suggest implementing multibiometric system and methods for template protection to make system more robust.

General Terms
Unique-identification, e-Governance.

1. INTRODUCTION
Several services are provided by the government, but to accessing the government services in developing countries is very much difficult task. The citizens spent there long time and they need to go through long procedure for accessing government services such as passport services, information sharing, bill payment, tax filling, banking etc. The whole systems are manual so they are very slow and time consuming systems. So there is canonical need of bringing in efficiency, transparency and reliability in government system. The government system use the information technology to provide batter services to the citizen it is called e-Governance. In every country when government provides e-services it is essential to identify the citizen for authorization purpose. In generic cryptography the authentication is based on the credential such password and user ID. But there are many limitations in traditional or manual identification such as they are difficult to memorize, most of password are easy to guess thus, compromise the security; complex passwords are difficult to remember so people store them at easily accessible location. One solution to this problem is to design unique-id for every citizen. Such as UIDAI has been setup by the Government of India with a mandate to issue a unique identification to all residents in country. UIDAI propose to create a platform to first collect the biometric detail and then to perform authentication that can be used by several government and commercial service providers.

1.1 e-Governance
e-Governance is a technology-mediated relationship between citizens and their governments from the perspective of potential electronic deliberation over civic communication, over policy evolution and in democratic expressions of citizen will [1]. In developing countries access to the government service is not convenient and simple task. The services are citizenship records, police records, ration card application, agriculture services, hospital services, BPL services and pension scheme. There a long procedure of to get these services and it takes lots of time of citizen. The situation is same all over across the India. The main reason behind it is manual work. For complication of application it needs to be processed through many persons and departments. The new approach as the solution to all these problems is e-Governance (electronic governance), also known as e-government, online government, digital governance. E-Governance provides services, transactions and interactions with citizens, business and other arms of government with the use of information and communication technology. E- Governance offers full service (24*7) available. In this case the person does not need to go to government offices to get services; it results into reduced service cost. E-Governance ensures transparency, efficiency and reliability of services into reduced cost.

1.2 Biometrics
Biometrics refers to automatic identity authentication of a person on a basis of one's unique physiological or behavioral characteristics [2]. A biometric system is a pattern recognition system that functions by acquiring biometric data from an individual, extracting a feature set and comparing this feature set against the template set stored in the database. Depending on context the biometric systems may function either in verification mode or identification mode.

In verification mode, the system authenticates a person's identity by comparing the obtained biometric data against biometric template(s) stored in the system database. Verification is positive recognition; where the aim is to avoid multiple people from using the same identity. While in identification mode, the system distinguishes an individual by searching the templates of all the users stored in the database for a match. Identification is negative recognition: prevent a single person from using multiple identities. While convention techniques of personal recognition such passwords, PINs, tokens and keys may work for positive recognition, negative can only be ascertained through biometrics.

Description of the commonly used biometrics is given below:

1.2.1) Face recognition: The most common biometric characteristic used by human for personal recognition is facial image. All biometric systems use the same information for face recognition [3]. The most accepted approaches are based on:

a) The position, shape and size of facial features, such as eyebrow, eyes, nose, lips, chin and their spatial association.

b) The overall analysis of face image that represents face as a combination of a number of objects (patterns).

1.2.2) Fingerprint: Fingerprints are graphical flow-like ridges on human fingers. Individual epidermal ridges and valleys have different characteristics for different fingers. The configuration and minute details of individual ridges and furrows are permanent and unchanging for a given finger[4]. So fingerprints are the effective biometric trait.

1.2.3) Iris: The iris, is a kind of physiological feature with genetic independence, contains extremely information-rich physical structure and unique texture pattern, and thus is highly complex enough to be used as a biometric signature[5].

1.2.4) Voice: Voice is a combination of physical and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g. vocal tracts, mouth, nasal cavities and lips) that are used in the synthesis of the sound [3].A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what he or she speaks.

1.2.5) Hand and finger geometry: It is convenient and acceptable for uses to make identification by hand. There are several features of the hand available for identification such as hand geometry, fingerprints, palm prints, palm vein and so on [6].

1.3 Requirement of biometric in e-Governance

Biometric has been widely used in forensics, such criminal identification and jail security and has the possibility to be widely adopted in a very broad range of government services

1) banking security, such as electronic fund transfers, ATM security, check cashing and credit card transactions;
2) physical access control, such as airport access control;
3) information system security, such as access to database via login privileges;
4) government benefits distribution, such as welfare disbursement programs;
5) national-id systems, which provide a unique id to the citizens and integrate different government services;
6) voter and driver registration, providing registration facilities for voters and drivers
7) customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated

Service system (INSPASS) which permits faster immigration procedure based on hand geometry.

2 Attacks on biometric systems

A biometric system is vulnerable to different type of attacks that cam compromise to the security afforded by the system, therefore resulting in the system failure.

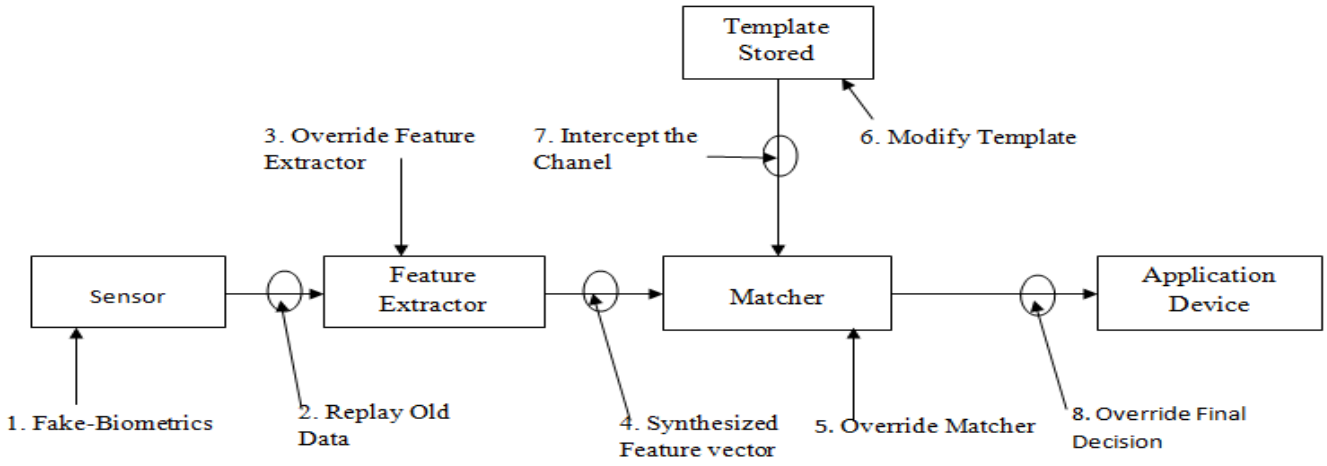

Fig 1: Possible attacks on biometric system [7].

Several different levels of attacks that can be launched against a biometric system are depicted in (Fig 1). These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system.

1) a fake biometric trait , where the fake artificial biometric objects are used during the identification checking process. The fake biometric is the reproduction of original biometric and contains the same properties, such as an artificial finger may be presented at the sensor; an unauthorized individual changes his or her biometric to appear like an authorized one.
2) The biometric data of an authenticate user is hacked and this data is submitted to the system repeatedly. It results into make the system into busy state, so that the legitimate user will never get access to the services of system.

3) The feature extractor program is changed with another program that generates specific output feature sets. It degrades the system performance and hence the legitimate user will also suffer from denial of service problem.

4) The feature sets generated by the feature extractor may be replaced with another feature sets during the transmission of data from feature extractor to the matcher. Now the matcher will get the synthetic feature set in the place of legitimate feature sets.

5) The matcher program may be changed with another program that results always true. Then the unauthorized user may also have the access to the system.

6) The modification of the template in the database may also result into security break. New templates may be replaced by with old templates.

7) The data may be altered when transmitting between various modules of the system.

The final output of the system may be overridden and result will be the complement of the original result. Now the authorized user will suffer with denial of services and the unauthorized use will get the advantage.

3 . PROPOSED SYSTEM

We provide some solution for secure authentication in e-Governance system. Figure 2 shows these approaches.

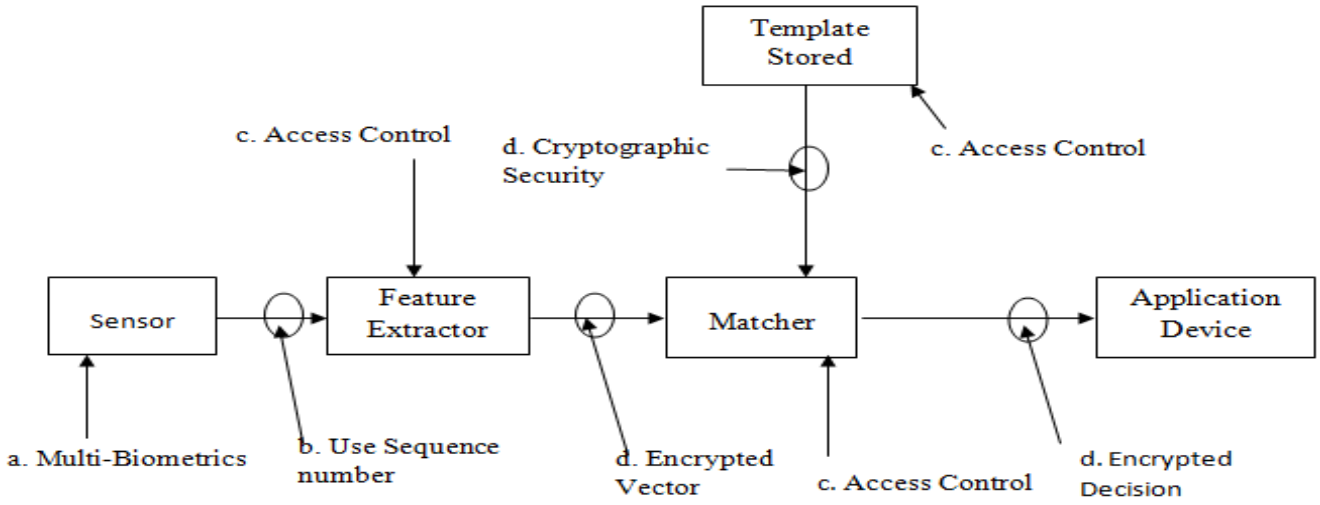

Fig 2: Solution to remove vulnerabilities in system

a) If a fake biometric is presented (camouflage attack) on biometric authentication system, the solution is to use multi-biometrics. In multi-biometric system more than one biometric trait are required for authentication purpose such as fingerprint, face, iris and voice all together.

b) The protection to reply attack can be provided by using the sequence number, if a system or person request enters the same trait more than specified time, simply reject its request.

c) By the use of multilevel security some attacks can reduced. Implementation of proper access control results into resistance to the attacks on stored template, feature extractor and matcher. Access to data and permission to change the structure of program will require privileges.

Data should be encrypted before transmission on the communication channel. Encrypted data should be stored in the database. It should be decrypted only when the actual processing is required.so that if any eavesdropper have access to the data it will get the encrypted form of data that is difficult to interpret.

4. CONCLUSION

We have discussed the e-Governance and biometric system. We also describe how the biometric systems are useful in e-Governance projects. Some security threats on the biometric systems are addressed and solutions to these problems are suggested. Proposed solutions are very much effective in terms of both theory and experiments. If these approaches are used in the e-Governance system they will ensure system's accuracy, reliability, security and efficiency. The proposed system can be implemented in e-Governance services like citizenship records, police records, ration card application, agriculture services, hospital services, BPL services and pension scheme, recruitment, online exams and results.

5. ACKNOWLEDGMENTS

We are thankful to Dr. O. P. Rishi sir for their great support and useful suggestions. We also wish to acknowledge our university Central University of Rajasthan, for providing us the required resources.

6. REFERENCES

[1] Frank Bannister and Regina Connolly, "New Problems for Old? Defining e-Governance", proceedings of the 44th Hawaii International Conference on System Sciences - 2011

[2] Wen-Shiung Chen, Kun-Huei Chih, Sheng-Wen Shih and Chih-Ming Hsieh, "Personal Identification Technique based on Human Iris Recognition with Wavelet Transform",2005 IEEE ,Page No. II -949, ICASSP 2005.

[3] Anil K. Jain, Arun Ross and Sahil Prabhakar, "An Introduction to Biometric Recognition", IEEE transactions on CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL., 14, NO. 1, January 2004.

[4] Anil K. Jain, Lin Hong, Sharath Pankanti and Ruud Bolle, "An Identity-Authentication System using Fingerprints", IEEE VOL 85, NO. 9, SEPTEMBER 1997

[5] A.K. Jain, R. Boole and S. Pankanti, "Biometrics: Personal Identification in Network Society". Kluwer Academic Publishers, 1991.

[6] Lang Zhai and Qi Hu,"The Research of Double-biometric Identification Technology Based on Finger Geometry & Palm print", IEEE 2011

[7] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength." In Proc. SPIE-EI Security , Steganography and Watermarking of Multimedia Contents VI, San Jose, CA, Jan. 2004, pp. 622-633.