ISSN:2249-5789
Kamal Deep, International Journal of Computer Science & Communication Networks,Vol 1(2), 176-185

Various Authentication Tecniques for Security Enhancement

Kamaldeep
Assistant Professor
Savera Group of Institutions (Gurgaon)
kamalmintwal@gmail.com

***Abstract*— Authentication is the art of confirming the truth of an attribute of an entity. Entity may be a person. If a entity is a person it can authenticate with the help of its traits such as his facial attribute, fingerprinting attribute, retina attribute, palm attribute, signature of a person, password, token attributes etc. There are so many attacks to which these techniques are vulnerable. So, today the security of the authentication system is becoming a burnt issue. Keeping in the view, the importance of the authentication systems, we analyze various authentication techniques in our paper. And try to find out various advantages and disadvantages of various authentication systems. This paper gives the emphasis on the various issues involved in the various authentication techniques.**

Keywords- Biometrics, Authentication, Knowledge based,Token based, Security etc.

I. INTRODUCTION

In the present era, many application areas need secure scheme for authentication. .The authentication system has been deployed in various areas in the industry as well as in military and in the e-commerce etc. Traditionally, passwords and ID cards have been used to authentication to systems. However, security can be easily break in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user). The emergence of biometrics has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. By using biometrics it is possible to establish an identity based on 'who you are', rather than by 'what you possess' (e.g., an ID card) or 'what you remember' (e.g., a password). Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo grams, signature, voiceprint, palm print, etc. to establish a person's identity [1,2]. While biometric systems have their limitations [3], they have an edge over traditional security methods in that it is significantly difficult to lose, steal or forge biometric traits.

In the current digital world, our biometrics system has a variety of attacks which makes the biometrics system insecure for authentication and communication. With the wide spread utilization of biometric identification system, establishing the authenticity of biometric data itself has emerged as an important research issue. The fact

that the biometrics system is not replicable and is not secret, combined with several types of attacks that are possible in a biometrics system, makes the issue of security/integrity of biometric data extremely critical. As the biometrics system uses the image in its processing and image also travels on the communication channel i.e. carrier image, hence steganography and watermarking can be the solution of these problems.

The rest of the paper is organized as follows:

In section 2, various methods of authentication system is discussed. Section 3 gives biometrics system performance. Section 4 indicates various characteristics of biometrics system. Section 5, comprise traditional verses biometrics system some emphasis is given on conclusion and future work.

II. METHODS OF AUTHENTICATION

A person can be identifies on the basis of "what he knows? (Password etc)", "what he has? (ID card, key etc)" and "what he is? (Biometrics)". On the basis of above information the authentication methods are classified in the following three ways.

- Knowledge based Authentication method.
- Token based Authentication method.
- Biometrics Authentication method.

The knowledge based and token based authentication systems are called traditional authentication system.

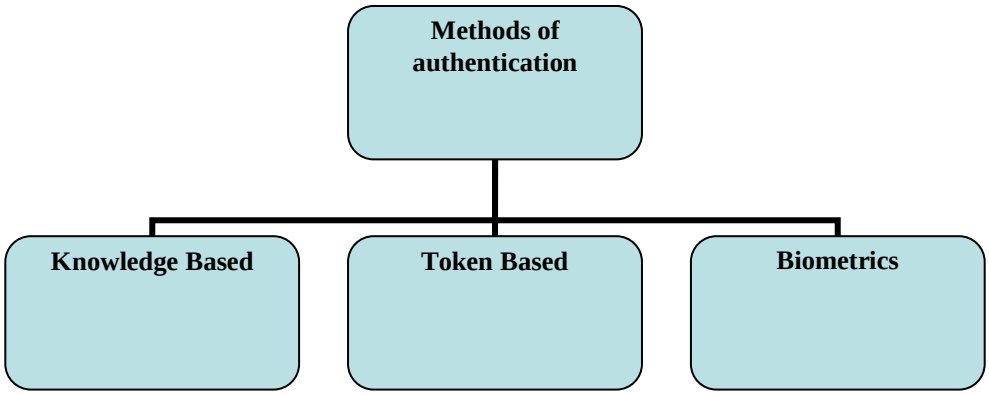

Fig. 1 Classification of Authentication Methods

KNOWLEDGE BASED AUTHENTICATION METHOD.

This type of authentication depends upon the knowledge of a person i.e. what he knows? It comes under the traditional authentication system. It is also called password-based method. In the password-based scheme the user submits a password, which is generally passed through a one-way hash function (this assures that even users with super-user privileges cannot access passwords). This, along with the identity is saved in a database during enrollment. During verification, the user submits the password, whose hash value *is* calculated, the hash

value retrieved from the database. A “Yes" decision is the output if and only if the two hashes are the same. Otherwise a “no” decision is the output. The diagrammatical representation of this method is shown below by the figure 2 and figure 3. Figure 2 shows the enrollment process of knowledge based authentication method and figure 3 shows the verification process of knowledge based system.

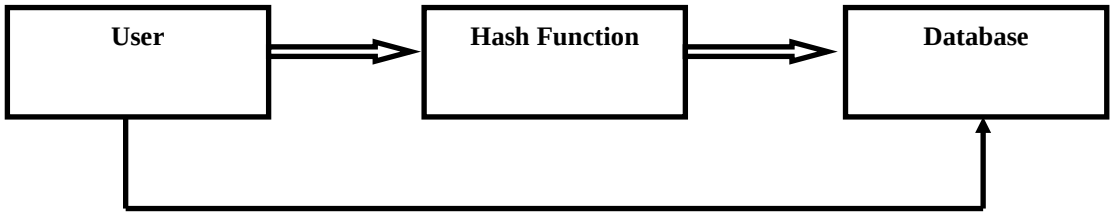

Fig. 2 Enrollment Process of Knowledge Based Authentication Method

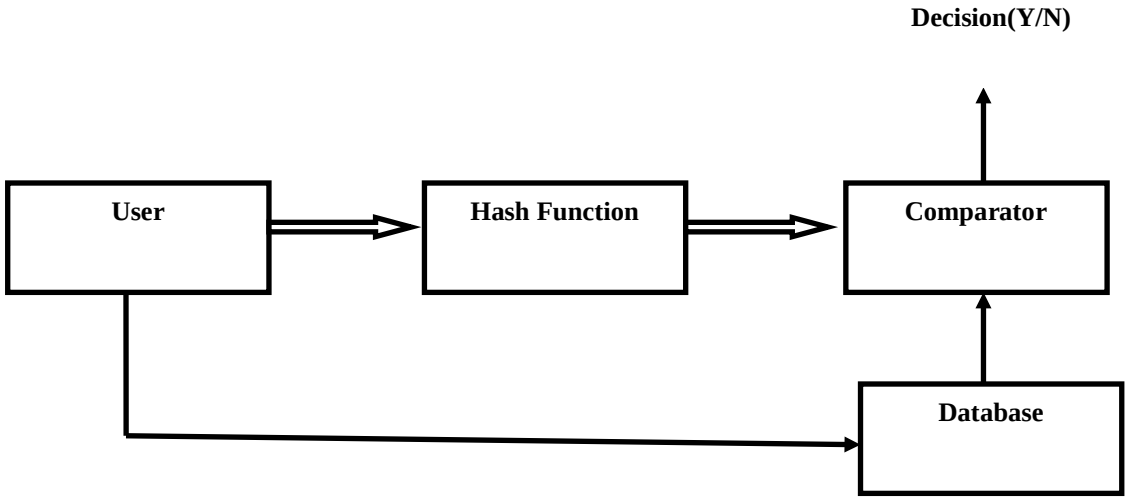

Fig.3 Verification Process of Knowledge Based Authentication Method

TOKEN BASED AUTHENTICATION METHOD.

This type of authentication depends upon the knowledge of a person i.e. what he has? It also comes under the traditional authentication system. It is also called token-based method. In the Token-based scheme, the user's identity and credentials (e.g., her birth certificate, diploma, signature) are checked by the authenticating institution (e.g., a university registrar's office), which stores this information in a database. This token can also contain entities to bind the token only with the authenticating institution, such as an embossed seal, specific logo, or bar code to eliminate illegal reproduction of the token.

In a supervised authentication application (where a human attendant is available), the user's card *and* her credentials (e.g., signature) are checked for consistency by a (human) supervisor: if these data match, the supervisor accepts the user.

In an unsupervised application, just the presence of the card is checked. The diagrammatically representation of this scheme is given below by the help of figure 4 and 5 respectively.

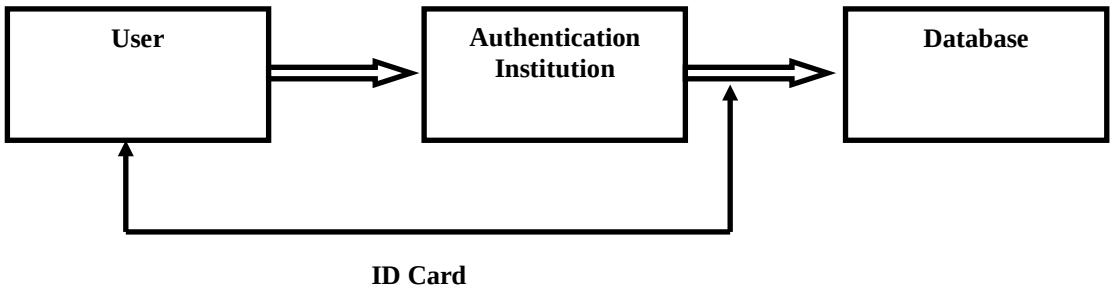

Fig. 4 Enrollment Process of Token Based Authentication Method

Supervised Verification

Unsupervised Verification

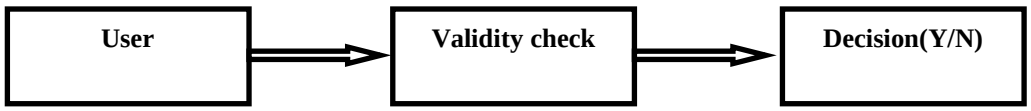

Fig. 5 Verification Process of Token Based Authentication Method

BIOMETRICS AUTHENTICATION METHOD

Biometrics is basically a pattern reorganization system that is used to identify or verify users based on his or her unique physical characteristics. Traditional techniques for identification and verification are based on 'What you know' such as passwords, PINS which can be forgotten and 'What you have' such as tokens, ID which can be stolen or lost.

In the enrollment process for an individual, using a biometric to be identified or verified, a copy of the individual's signature has to be stored in a database at the enrollment stage. Figure 6 presents the block-diagram of the enrollment stage.

Biometric identification is based on physiological or behavioral characteristics that provide information about 'Who you are'. And the output is the person identity. Figure 7 presents the block diagram of identification

Biometric verification is based on physiological or behavioral characteristics that provide the decision accepted or rejected. And the output is “yes” if accepted and “No” if rejected. Figure 8 presents the block diagram of verification.

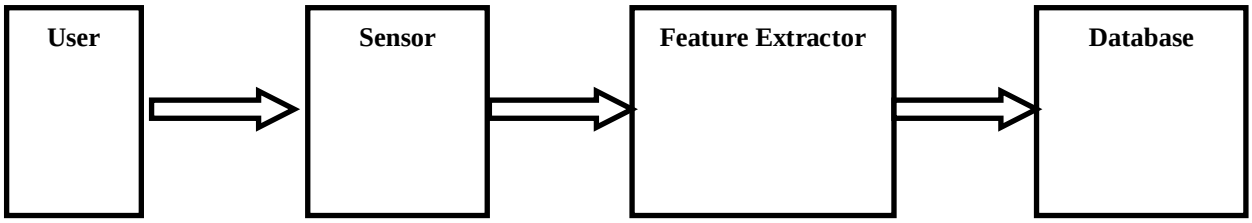

Fig. 6 Enrollment Process of Biometrics Authentication Method

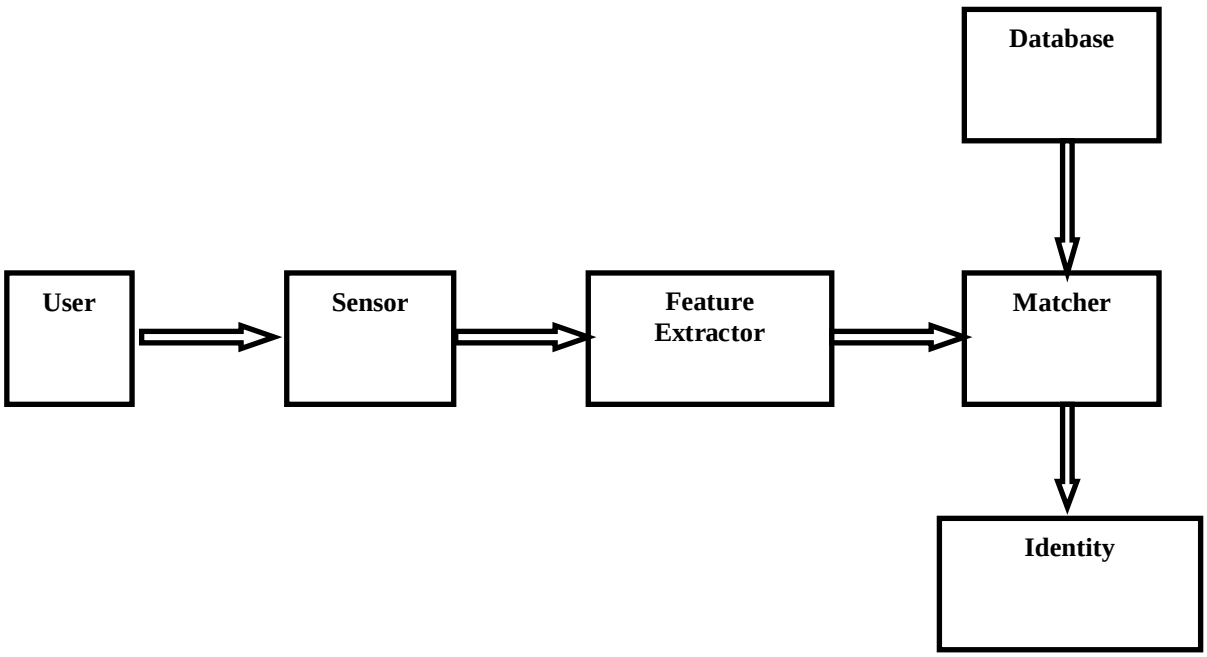

Fig. 7 Identification Process of Biometrics Authentication Method

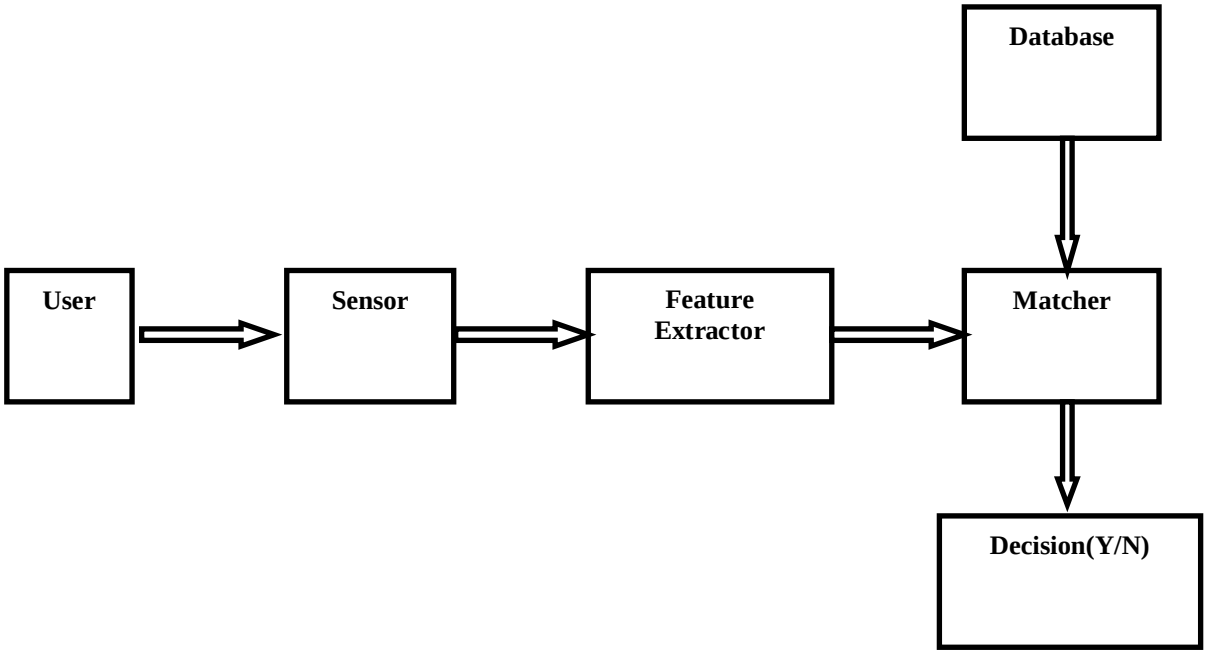

Fig. 8 Verification Process of Biometrics Authentication Method

BASIC STRUCTURE OF A BIOMETRIC SYSTEM

Every biometric system consists of four basic modules. These module is describe by Parvathi Ambalakat in his paper ”security of biometrics authentication system”, which are given below.

ENROLLMENT MODULE

The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual’s biometric characteristic to produce its digital representation.

FEATURE EXTRACTION UNIT

This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

MATCHING UNIT

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user’s master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one to many matching).

DICESSION MAKER

This module accepts or rejects the user based on a security threshold and matching score.

III. BIOMETRIC SYSTEM PERFORMANCE

The performance evaluation of a biometric system depends on two types of errors – matching errors and acquisition errors. These are defined by Ambalakat in his paper "security of biometrics sytem" The matching errors consist of the following:

FALSE ACCEPTANCE RATE (FAR)

Mistaking biometric measurements from two different persons to be from the same person.

FALSE REJECTION RATE (FRR)

Mistaking biometric measurements from the same person to be from two different persons.

The acquisition errors consist of the following:

FAILURE TO CAPTURE RATE (FTC)

Proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality.

FAILURE TO ENROLL RATE (FTE)

Proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality. This includes those who, for physical or behavioral reasons, are unable to present the required biometric feature. All of the above are used to calculate the accuracy and performance of biometric system. Biometric systems like any authentication system are not completely foolproof. It has its own drawbacks. While a biometric is a unique identifier, it is not a secret and biometrics, once lost is lost forever (Lack of secrecy and non-replace ability).

IV. CHARACTERISTICS OF BIOMETRICS

PERMANENCE

The biometrics traits must be permanent. It should be not changing frequently. And remain constant for a long interval of time.

UNIQUENESS

The biometrics tait must be unique in nature. God has gifted us some traits which are unique in nature for example fingerprint, retina, etc. we can use these traits for authentication. It distinguish one person from another.

COLLECTABILITY/MEASURABILITY

The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

UNIVERSAL

Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

PERFORMANCE

The biometrics traits It is the measurement of accuracy, speed, and robustness of technology used.

ACCEPTABILITY

The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body. Circumvention- Ease of use of a substitute.

V. TRADITIONAL Vs BIOMETRICS SYTEM

Biometrics-based personal authentication systems are becoming increasingly popular, compared to traditional systems that are based on tokens (say key) or knowledge (say password) [4,5]Jain et at (1999)].
Schneier [Schneier et al(1999)] compares traditional security systems with biometric systems. Schneier said that though biometrics is known as uniquely identifiers, but they are not secrets. We leave our fingerprints on everything we touch, and our iris patterns can be observed anywhere we look.

- Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges (say key, password) of a genuine user and the genuine user himself.
- The password in traditional system is easy to guess.
- Biometric authentication systems can be more convenient for the users since there is no password to be forgotten or key to be lost.
- The password in traditional system is easy to share.

VI. CONCLUSION AND FUTURE SCOPE

in this paper, various authentication scheme has been discussed which have their own advantages and disadvantages. In the past traditional authentication systems were used. But as the computer growing very rapidly, these traditional authentication systems are replaced by the other advance system like biometrics authentication system. The biometrics system also has also many vulnerable on it. And also having various limitation on the biometrics system. So, in the future we will try to overcome these limitation and vulnerable. And try to make the system more robust.

REFERENCES

[1] Jain, A.K., Bolle, R., and Pankanti S.,"Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[2] Wayman, J.L., "Fundamentals of biometric authentication technologies", International Journal of Image and Graphics, vol. 1, no. 1, pp. 93–113, 2001.

[3] Gorman, L.O., "Seven issues with human authentication technologies", in Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), (Tarrytown, New York), pp. 185–186, Mar 2002.

[4] Jain, A.K., Bolle, R., and Pankanti S.,"Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[5] Schneier and Bruce, "Inside risks: the uses and abuses of biometrics," August 1999 Communications of the ACM, Volume 42 Issue 8.

[6] Ambalakat ,P."Security of Biometric Authentication Systems", 21st Computer Science Seminar SA1-T1-1

[7] Bruderlin, R. "What is biometrics?", Paper, 1999-2001.

[8] Dabbah, M. A., Woo, W. L., and Dlay S. S., "Secure Authentication for Face Recognition," In Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Apr. 2007. USA, pp. 121 - 126.

[9] Ganorkar S.R., Ghatol A. A., "Iris Recognition: An Emerging Biometric Technology", In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp. 91 – 96.

[10] Gorman, L.O., "Seven issues with human authentication technologies", in Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), (Tarrytown, New York), pp. 185–186, Mar 2002.

[11] Im S., Park H., Kim Y., Han S., Kim S., Kang C., and Chung C., "A Biometric Identification System by Extracting Hand Vein Patterns", Journal of the Korean Physical Society, Korean Publication, Volume 38, Issue 3, Mar. 2001, pp. 268-272.

[12] Jain A. K., Ross A., and Prabhakar S., "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[13] Jain, A. K., Sarat Dass C., and Nandakumar K., "Can soft biometric traits assist user recognition?" Proceedings of SPIE -- Volume 5404, August 2004.

[14] Jain, A.K., Bolle, R., and Pankanti S.,"Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[15] Jain, A.K., Uludag, U., "*Hiding biometric data*", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.

[16] Jain, Anil K. and Arun Ross, "*Multibiometric systems*," Communications of the ACM," January 2004, Volume 47,Number 1 (2004).

[17] Jain,A.K. and Arun Ross, "Multibiometric systems," Communications of the ACM," January 2004, Volume 47, Number 1 (2004).

[18] Kumar A., Wong D. C., Shen H. C., and Jain A. K., "Personal Verification using Palmprint and Hand Geometry Biometric", In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, Jun. 2003, pp. 668 - 678.