ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient Secure Authentication Policies using Biometrics

Ajay Jangra
CSE department U.I.E.T.
Kurukshetra University,
Kurukshetra, India
er_jangra@yahoo.co.in

Vedpal Singh*
CSE department U.I.E.T.
Kurukshetra University,
Kurukshetra,India
vedpalsiet101@gmail.com

Priyanka
ECE department, Kurukshetra
Institute of Technology & Management,
Kurukshetra ,India
priyanka.jangra@gmail.com

Anu Kundu
CSE department U.I.E.T.
Kurukshetra University,
Kurukshetra,India
anu.haryana@gmail.com

Abstract: There is no absolute secure system exist. Systems only claim security and privacy but they cannot give any guarantee. On looking the past history of every system it founds that security arrangements always encountered with some cracks or loopholes time-by-time. Even if, password / pin code can also be hacked, in same direction biometric security mechanism provides new heights to security and privacy based on individual's characteristics and behavior. In this paper we analyze various biometric based security mechanisms, classification and compare is present in systematic manner. We analyze the advantages and drawbacks of various biometric secure authentication policies. The process, hardware/software requirements, expensiveness are describe in this paper.

Keywords: Biometrics authentication, Physiological authentication, Behavioral authentication, security.

I. INTRODUCTION

Biometrics is an automated method of recognizing a person, based on physiological or behavioral properties. ***Physiological biometrics*** is based on measurements and data collected from direct measurement of a part of the human body like as fingerprint; iris-scan, retina-scan, hand geometry, and facial recognition. *Behavioral characteristics* are based on an action taken by a person. ***Behavioral biometrics***, are based on measurements and data derived from an action, and indirectly measure characteristics of the human body like as voice recognition, keystroke-scan, and signature-scan. [11] In the recent years, there is a trend of using the mechanism of biometrics for security purpose. For improving the security, we use the different types of biometric authentication techniques. Biometrics systems are superior because they provide ***nontransferable*** biometric properties. ***What is Biometrics?*** Biometrics measures and analyzes physical and behavioral characteristics for identity verification. A very ***first verification*** system is ***Anthropometry de***veloped by ***Alphonse Bertillon***. Biometrics recognition consists of *identification* and *verification.* Identification refer to the answer of question *"who is X?"*. Verification refers the answer of question: *"Is this X?"*. Biometric authentication performs both identification and verification both but other authentication schemes performs only identification but not verification.
Biometric-based authentication applications include network and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures. Utilizing biometrics for personal authentication is more accurate than current methods (such as the utilization of passwords or PINs).

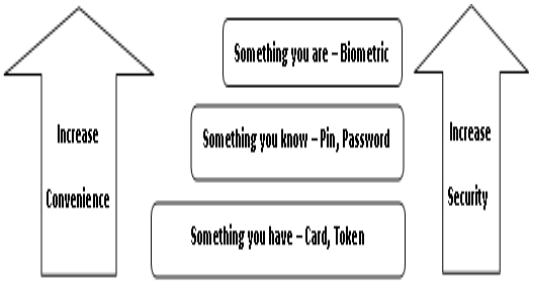

Figure 1: Increasing security and convenience in various authentication schemes.

Authentication may be defined as "providing the right person right authority". From figure 1, combination of all three authentication schemes provides highest security and convenience. [1] After analyze the figure 1 it is sure that biometric systems are more convenient and highly secure.

Good about biometric authentication: i) authenticate the user ii) non-transferrable characteristics iii) highly secure iv) biometric objects cannot be stolen v) fast processing. Not always good but it also contains some drawbacks as i) inconsistent performance ii) Fail to enroll rate brings up another important problem iii) biometrics data can not considered secret iv) sensors are costly & low battery iv) user's privacy may be effected v) lack of biometric systems vi) miscellaneous people without hands cannot use hand based systems or people without eyes cannot use Iris Recognition etc. [10]

A. Biometrics technique classification

Biometric techniques are classified in to two groups, **A**. *Physiological Biometrics* **B**. *Behavioral biometrics.* A. **Physiological Biometrics** is based on physiological characteristics on an individual. Various physiological biometric techniques are

(a) Fingerprint recognition:

Each human has a unique pattern of friction ridges and valleys. Each person has a unique fingerprint for every finger. Fingerprint technology mostly used for identification. Fingerprint identification based on the ***minutiae***, location and direction of ridge ending and bifurcations along a ridge path. [15, 19]

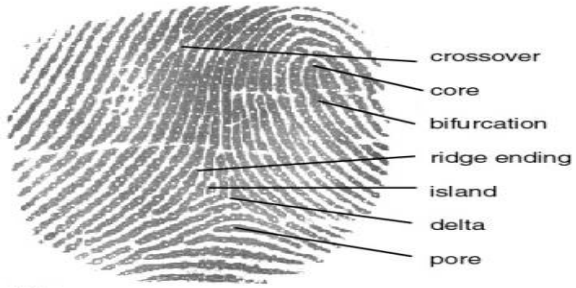

Figure 2: Various patterns of a fingerprint

Figure 2, shows the various patterns of a fingerprint. The human fingerprint is made of various types of ridge patterns, classified according to the decades - old Henry system: left loop, right loop, arch, and whorl. Loops make up nearly 2/3 of all fingerprints, whorls are nearly 1/3, and perhaps 5-10% are arches. This fingerprint is a right loop. In figure Minutiae, the discontinuities are the basis for most fingerprint authentication. Many types of minutiae, including dots, islands, ponds or lakes spurs, bridges and crossovers exist. Fingerprints are used in forensic applications: large-scale, one-to-many searches on databases of up to millions of fingerprints. AFIS (Automated Fingerprint Identification Systems) - commonly referred to as "AFIS Systems". ***Hardware*** used for obtaining the digital image of a finger a variety of sensors are used – like – optical, capacitive, ultrasound and thermal. ***Software*** used for fingerprint recognition used the two different matching techniques: Minutiae based matching and Pattern matching. Fingerprint templates independent that not depend on the emotional state. Finger has the ***low degree of distinctness***. The identification technology not well suited for identification applications because of their shortcomings. Finger recognition system has ***low EER***. For the computation of fast Fourier transformation the system needs to have a ***co – processors***.

(i) Algorithm

Figure 3, shows the user authentication based on fingerprint. Suppose p and f public elements.

Where p, a large prime number, f is a one – way hash function, IDi, identity of legel user Ui.

Sk1 and sk2 are the secret keys. Authentication is done in three steps: Registration, login, authentication. [9]

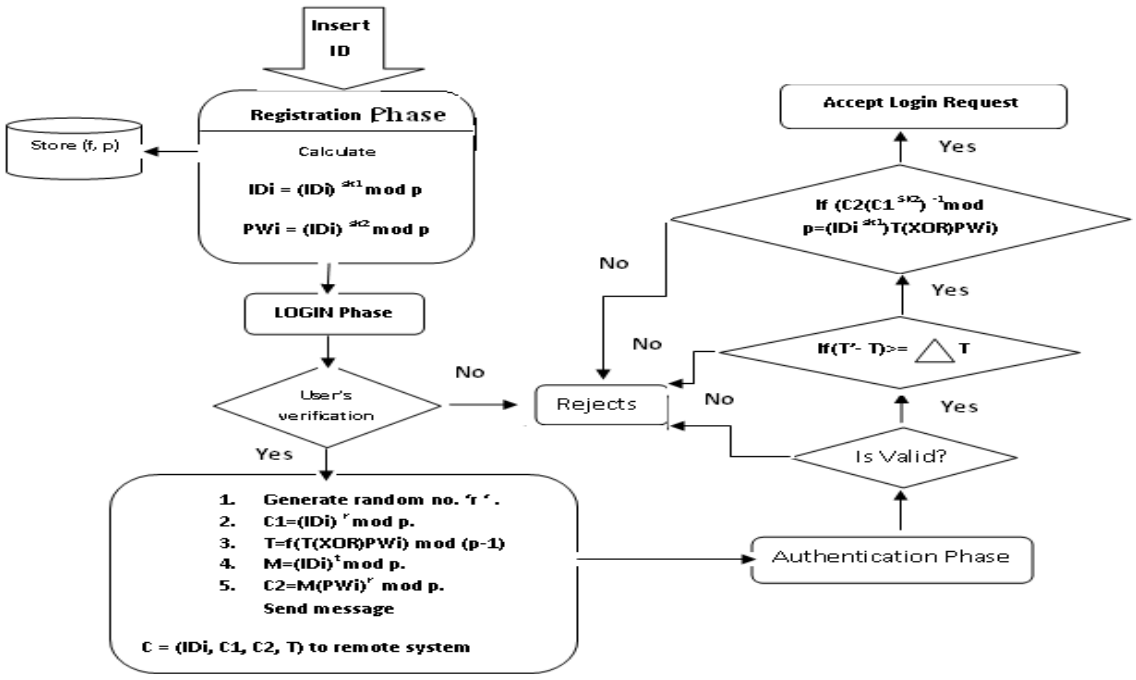

Figure 3: fingerprint authentication

Firstly, user inserts ID. In registration phase, calculate IDi and PWi by using inserted ID by the user. In login phase, user verification is calculated. If user is not valid reject the request. If user is valid then calculate the parameters (C1, C2, T, M) and send the message C = (IDi, C1, C2, T). After the login phase, authentication phase is occurring, in this phase check again that user is valid or not. If user is valid, then verify two conditions: if these both conditions are satisfied, accept the login request otherwise not.

Fingerprint authentication is more mature because many algorithms are available for fingerprint authentication.

Fingerprint authentication may be flexible then the other kinds of biometric authentication techniques such as face recognition. This can be performed by considering two factors; Space complexity & Time complexity. [9]

(ii) Fingerprint processing

There are the some restrictions are when we use the fingerprint based authentication. The two big restrictions are clock frequency and data transmissions. [17] Figure 4, represents fingerprint processing into the following steps:

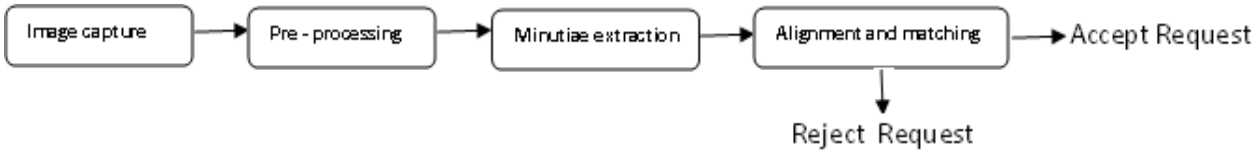

Figure 4: Fingerprint processing

(iii) Image capturing: For capturing the image used the fingerprint sensors such as semiconductor sensors that obtain the image quality over 500dpi. This type of sensors suffer from different types of problems like latent fingerprint, death finger etc. For reducing the problems use the same anti – fraud elements.

***(iv) Pre processing*:** For adaption of the image and reduced image data use pre – processing. In the pre – processing method, firstly, a gradient map is captured. By the segmentation reduced image with valleys and ridges is obtained. Segmentation is performed based on the data available at the gradient map. In the next, enhancement step, finger pressure and humidity are reduced that affects the brightness and contrast. By using orientation map of the finger image finds the tangent angles of all ridges.

(v) Minutiae Extraction: [13] Different methods available for fingerprint feature extraction and recognition. For the minutiae extraction we use the special kind of algorithm called ***"Ridge Following Algorithm"***. This algorithm searches the ridges iteratively. For minutiae extraction uses a method that uses *three steps*: Locate the fingerprint centre, Extract the minutiae points, Create the final set of minutiae points. After locating the centre point (0, 0), then create the co – ordinates for the fingerprint. Then we find the reference point that is the nearest minutiae point to the centre point. Then we recomputed the location of minutiae points. If we rotate or translate the fingerprint image then the centre point (0, 0) is not affected. In the final step, we create a final set of minutiae points.

(vi) Matching and authentication: Fingerprint authentication has two phases: Registration phase & Authentication phase. In the registration phase, user's finger scan at the time of registration and scanned data is stored into the database for future authentication purpose. In the authentication phase, user's fingers are scan by the fingerprint scanner. In authentication phase, matches previously stored templates with the current input templates. If the input template is match with the previously stored template then the user is authentic otherwise not. For the fingerprint verification we use the ***"Elastic Matching Algorithm"*** because the elasticity of the fingers introduces new variations. For example, distance between ridges and valleys may vary. [11]

(b) Iris Recognition

Iris recognition pattern utilizes the iris muscle to perform verification. A highly real-time and high cognitive identification of a person is provided by the iris recognition. Iris recognition is more good, suitable and reliable technique for identification than face, fingerprint and voiceprints. Iris recognition techniques are non–intrusive, non-invasive, expensive technique, highly robust, most accurate and reliable. It is not easily stolen, iris protected from the external environment behind the corner and eyelid. Iris has the ***highest degree of robustness***, ***low false acceptance and rejection rates*** and easy to use. Iris recognition technology is not very intrusive as there is no direct contact between the subject and the camera technology. This techniques use the ***NIR (Near Infrared Light).*** [19]

(i) Authentication using the Iris Recognition

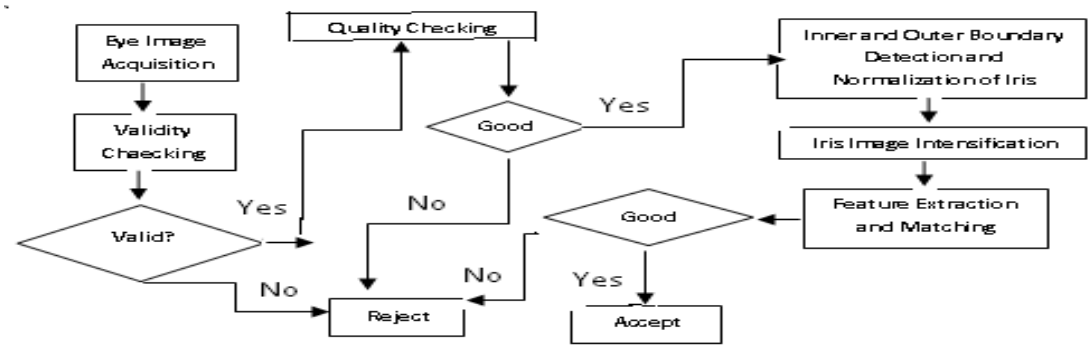

Figure 5: Authentication using the Iris Recognition

In figure 5 shows the Iris Recognition Algorithm, in this algorithm first do acquisition of eye image, then check the validity of the image, if the image is valid then we check the quality of the image, otherwise reject. If the image quality is valid or good then found out the inner and outer boundary and normalize the image. Image intensification based on the

spatial domain approach. In the next step, feature extraction and iris matching algorithms, if it is successful, then accept request otherwise reject. [13]

Figure 6: Iris Scanning

Figure 6 shows the iris-scan process begins with a photograph. A specialized camera, very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes only 1 – 2 seconds and provides the details of the iris that are imaged, recorded and stored for future authentication. *Advantages: 1)* non-invasive *2)* It produces no difficulty for iris recognition of those people that wear glasses or contact lenses *3)* error rate very low *4)* Scalability and speed *5)* This technology takes no longer time for authentication and comparison. And *disadvantages are* : *1)* In the case of when subjects are blind or have cataracts can produce difficulty in the iris recognition *2)* If the used camera has no enough amount of illumination, then we can get a inaccurate image. [14]

(c) Palm Recognition

Palm identification based on the information that obtained from the friction ridge impression. Palm vein authentication uses the vascular pattern of an individual's palm as personal identification data. Palm has a broader and more complicated vascular pattern. Palm an ***ideal part*** of the body for the palm recognition technology; it normally does not have hair and less probability of color change of skin, unlike a finger or back of the hand.

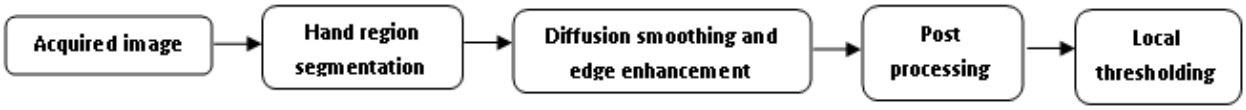

Figure – 7: block diagram of hand veins processing stage [2]

Figure 7, shows the hand veins processing, firstly acquired high quality image. In the next step segmentation is performed on the captured image. After segmentation, smooth image and enhance the edges of the image, then perform local thresholding and post processing on the output result after the smoothing and edge enhancement of the image. **[2, 5, 7]**

(i) Palm Authentication Process

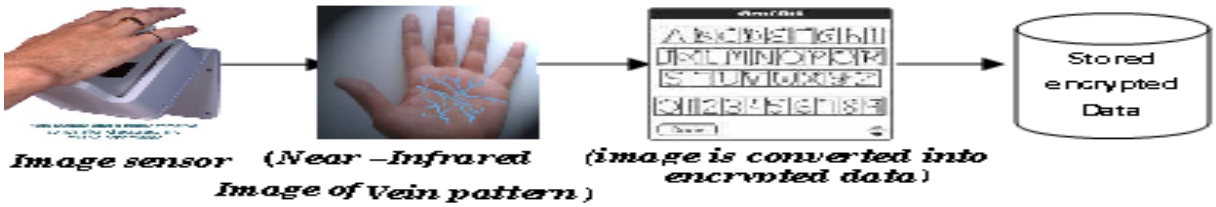

Figure 8: palm authentication process

Figure 8, represents the palm vein authentication process. Firstly by using the image sensor sense the image and get the high resolution image of the hand, and then near – infrared image of vein pattern is captured. Then captured near – infrared image is encrypted. Encrypted data stored into database for future matching and authentication purpose. [7] *Advantages*: *1)* Easy to capture *2)* highly stable pattern over the adult life span. *Disadvantages*: *1)* Use requires some training *2)* system requires a large amount of physical space *3)* low degree of ***distinctiveness*** *4)* This technology not well suited for identification applications. [19]

(d) Face Recognition

An automated method used for recording the spatial geometry of distinguishing features of the face. Cooperative behavior by the user and environmental factor such as lighting conditions can degrade performance of this technology. Facial recognition technology perform work in standard biometric sequences of image acquisition, image processing, distinctive characteristics location, template creation and matching. Facial recognition is non - intrusive, hands free, continuous and accepted by most users. [2, 4, 15]

(i) Face Recognition process

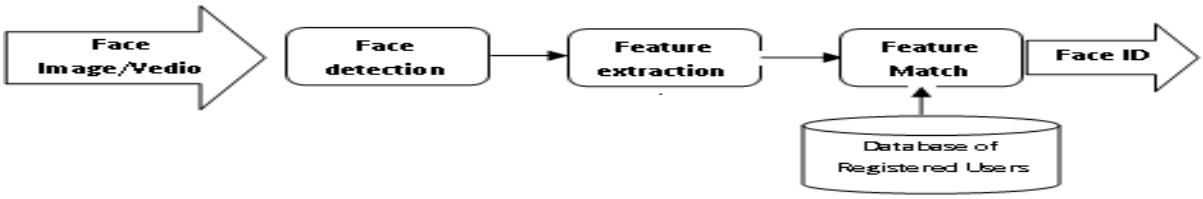

Figure 9: Face Recognition Model

Face recognition model as shown in figure 9, it uses three steps for authentication of a person's face, in the first step, *face detection*, locating the position of the face in the given photo or video and removing the unwanted details from the background. In the second step, *feature extraction*, extracting those features that are required for recognition. In the last step, *feature match*, comparing scanned information with the already stored data into the database. If the match is possible, then ID of corresponding user is returned. *Advantages*: *1)* No contact required *2)* Commonly available sensors (cameras) *3)* Easy for humans to verify results. *Disadvantages: 1)* Face can be obstructed by hair, glasses, hate, scarves, etc *2)* sensitive to change in lighting *3)* expression and pose *4)* face change over time. [19]

B. *Behavioral Biometrics (it uses the individual's behavior to recognize tool.)*

(a) Voice Recognition

Method of using vocal characteristics to identify individual's using a pass phrase called ***voice recognition***. Voice recognition uses the acoustic features of speech. The acoustic features differ person to person. ***Acoustic features*** depend on the size of the throat, mouth, voice pitch and speaking style. Voice affected by the ***emotional and other physical states of the speaker***. Voice recognition badly affected by ***noise***. Speech recognition has introduced problems with persons who are ***husky or mimic*** another voice. Voice recognition may be used to dictate text into the computer or to give commands to the computer. Voice recognition uses a neural net to "learn" to recognize your voice. Telephone or microphones are the sensors for this technique. [2, 5, 15]

(i) Digitizing the Human Voice

Scientifically, the human voice is a complex acoustic wave, because of the high capacity of the Human ear and brain can easily understand the human voice. Technically, voice is an analogue signal, is defined as one with a physical value. Figure 10, represents sine wave of human voice. [6]

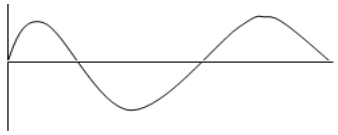

Figure 10: Sine Wave of Human Voice

Conversion of analogue sound signal into a digitizing form: Firstly, by using microphone sound is converted into electrical waves. In the next step, discrete continues measurements series converted into continuous waves by the sampling.

(b) Keystroke Dynamics: (Not what you type, but how you type)

Keystroke dynamics, an automated method of examining on individual's keystroke on a keyboard. Keystroke dynamics is totally based o the behavior of the user. Keystroke dynamics use a ***keyboard***, compatible with PCs. By using the keystroke dynamics technology only authentic user use the computer. Several measurements included in keystroke dynamics are: *1*) Duration of the keystroke or key hold time *2)* Inter keystroke time *3)* Typing errors *4)* Force keystroke *5)* Rhythm of Typing *6)* Finger placement etc. Types of keystroke analysis: ***Static*** and ***dynamic.*** [2, 8]

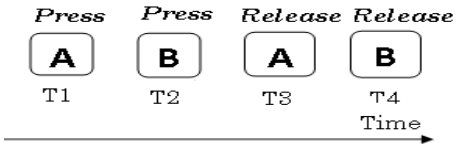

Figure 11: Information Capturing when pressing the Key

Figure 11, represents the raw information captured at rime when we press or release A and B keys. The captured information consists of timestamp of the event, code of the key, typing speed etc. Here we focus ***not what you type, but how you type.*** Keystroke dynamics is almost free – required only a keyboard. It controls the ***access*** of computer. [16]

(i) Keystroke Dynamics Authentication algorithm

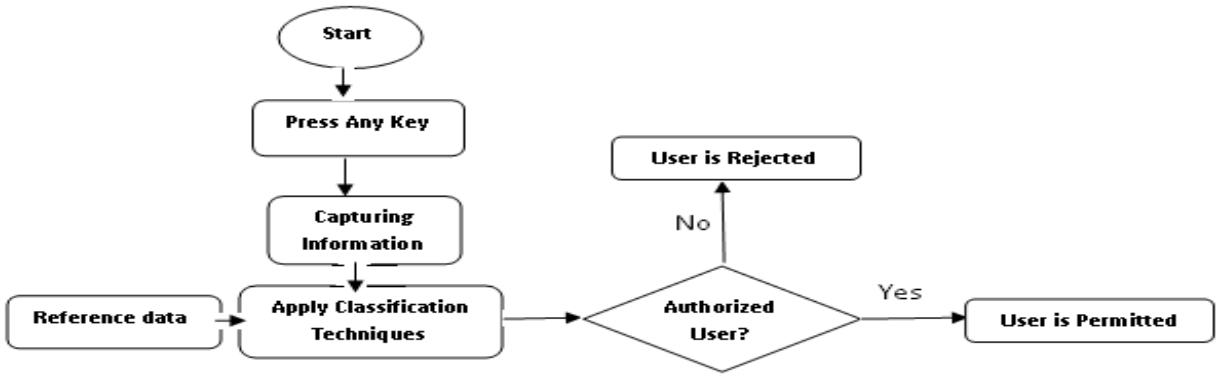

Figure 12: Keystroke Dynamics Authentication algorithm

Figure 12, shows the authentication using keystroke dynamics, when we press any key, then in the next step capturing the information like typing speed, typing pressure, time stamp of the event, code of the key, etc. On captured information apply classification techniques. Captured information compared with reference data. If match is occurred, the user is authorized, otherwise not.

(c) Signature Recognition

In the signature verification we use the dynamic analysis of a signature to authenticate a person. ***Measurements*** are

speed, pressure, total time of the signature and angle used by a person affects the signature verification. ***Signature verification*** is mostly based on the e–business applications and other applications. As shown in Figure 13, shows the user authentication based on the

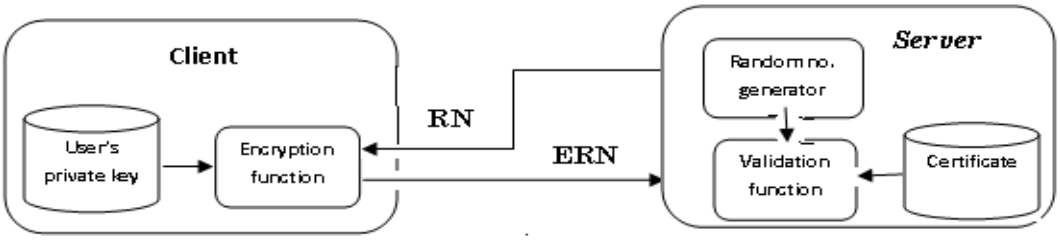

Figure 13: User Authentication based on Signature

User's private key. CA (Certificate Authority) issue the user's public and private key, that stored by the client. Here user's private key is like the signature of the user. A random number (RN) generated by the server is encrypted with the private key by client, then the encrypted random number (ERN) is validated in the server side with both CA's and user's certificate. [15, 20]

C. Biometric Techniques Comparisons:

On the basis of various parameters a comparison of above discussed biometric techniques is given in tabular format. [2]

Table 1: Comparison of Biometrics Techniques

Biometric Techniques	Identify / Verify	Robustness	Distinctiveness	Intrusive	Dependency on emotion	Cost	Error rate
Fingerprint	Either	Medium	Low	Touching	No	Medium	medium
Iris	Either	High	High	12+inches	Yes	High	Low
Palm	Verify	Medium	Low	Touching	No	Medium	medium
Keystroke	Verify	Low	Low	Touching	Yes	Less	High
Voice	Verify	Medium	Low	Remote	Yes	Medium	High
Face	Either	Medium	Medium	12+inches	No	Medium	medium
Digital signature	Verify	Low	Medium	Touching	Yes	Less	medium
Gait Recognition	Either	Low	Low	Remote	Yes	Medium	Low

II. CONCLUSION

Recent advances in biometric technology have resulted in increased accuracy and security at reduced cost. Biometric technologies are highly secure identification and personal verification systems. Today's biometric solutions provide a means to achieve fast and user – friendly authentication with high level of security and at low cost. This paper discussed the various biometric authentication techniques and highlights their features. Comparisons of biometric techniques tell that what technique is accurate for a particular application and also gives usage cost. After the comparisons of all biometric authentication techniques we find that they lead to best authentication technique with highly robust and distinctive properties.

III. REFERENCES

[1] Ajay Jangra, Vedpal Singh, Priyanka & Chander Diwakar "SECURITY AND PASSWORD MANAGEMENT ISSUES FOR REMOTE – USER AUTHENTICATION USING SMART CARDS" International Journal of Information Technology and Knowledge Management, July – December 2010, Volume 3, No.2, pp. 719 – 721.

[2] "A Primer on Biometric Technology" in Proceedings of the CardTech/SecureTech Conference '98,May 1998, Army Biometric Applications, pp. 9-19.

[3] Chitra, R. Bremanath "Efficient Identification Based on Human Iris Patterns" V1.4b , 2003, pp. 1 – 15.

[4] Edmund Spinella "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning" SANS Institute InfoSec Reading Room, 28 May 2003.

[5] Gerik Alexander von Graevenitz` "About Speaker Recognition Technology".

[6] Heinz Hertlein, Dr. R. Rrischholz, Dr. Elmar Noth "Pass Phrass Based Speaker Recognition for Authentication" 2003 working Group BIOSIG, www.biosig.org

[7] R.Jeyaprakash, Jin Lee, S.Biswas, J.M.Kim "SECURE SMART CARD USING PALM VEIN BIOMETRIC ON-CARD-PROCESS" International Conference on Convergence and Hybrid Information Technology 2008, June14, 2010, pp. 548-551.

[8] M.Karnan, M.Akila "Personal Authentication based on Keystroke Dynamics using Ant Colony Optimization and Back Propagation Neural Network", IJCNS,Vol. 1,No. 2,November 2009, pp. 8-15.

[9] J.K.Lee, S.R.Ryu and K.Y.Yoo "fingerprint based remote user authentication scheme using smart cards" Electronics Letters 6th June 2002, Vol. 38, No. 12, pp. 554 – 555.

[10] Y.Matyas, Z.Riha "BIOMETRIC AUTHENTICATION – SECURITY AND USABILITY" pp- 1-13.

[11] Y.S.Moon, H.C.Ho, K.L.Ng "A secure card system with Biometrics Capability" in proceedings of the 1999 IEEE Canadian conference on Electrical and Computer Engineering Shaw Conference Center, Edmonton, Alberta , Canada may 9-12-1999, pp. 261-266.

[12] Nguyen Minh Duc and Bui Quang Minh "Your face is not your password - face authentication ByPassing Lenovo – Asus – Toshiba " http://security.bkis.vn

[13] NGYUYEN Thi Hoang Lan, NGYUYEN Thi Thu Hang "An approach to protect private key using fingerprint Biometric Encryption key in BioPKI based Security System.

[14] Penny Khaw "Iris Recognition Technology for Improved Authentication" SANS Institute InfoSec Reading Room, SANS Security Essentials (GSEC) Practical Assignment Version 1.3, SANS Institute 2002,pp. 1-15.

[15] F.L.Podio, J.S.Dunn,"Biometric Authentication Technology: From the movies to your desktop" http://www.biometrics.org , pp. 1-8.

[16] Romain Giot, Mohamad El – Adeb, Christophe Rosenberger "Keystroke Dynnamics with Low Constraints SVM Based Passphrase Enrollment" published in "IEEE International Conference on Biometrics: Theory,Applications and Systems (BTAS 2009) Washington : United States, hal – 00432775, version 1 – 17, Nov 2009.

[17] R. Sanchez – Reillo, C. Sanchez – Avila and L. Mengibar – Pozo "Microprocessor smart cards with fingerprint user Authentication" IEEE, 14June 2010, pp. 46 – 49.

[18] M. Watanabe, T.Endoh, M.Shiohara, S.Sasaki "Palm Vein authentication Technology and its applications" 2005, pp. 347-350.

[19] White Paper "Biometrics Foundation Documents" National Science and Technology Council, http://www.biometricscatalog.org/NSTCSubcommittee, pp. 1-166.

[20] Yoichi Seto "development of personal Authentication Systems using fingerprint with Smart Cards and Digital Signature Technologies" Seventh International Conference on Control, Automation, Robotics and Vision (ICARCV '02), Dec 2002, Singapore, pp. 996 – 1001.