

# 1

## Integration of Biometrics with Cryptographic Techniques for Secure Authentication of Networked Data Access

*Abanti Cyrus Makori*

---

*The modern Information Technology evolution demands the use of computer networks with strict security performance. The password-based authentication system and the token-based systems that are current deployed, are not able to meet this performance. Achieving higher levels of security requires authentication. Today's standard security mechanism is a password that you create, remember it, and change it frequently. These passwords are not foolproof because they can be stolen, forgotten, cracked, sniffed and even tampered with. In fact it is quicker to gain access to electronically held data, copy or print it out than it is to search through or photocopy manually held files.*

*The problems of traditional personal authentication systems may be solved by biometric systems. Biometric identification is extremely effective authentication. It is an important weapon to protect against credit card fraud and phantom withdrawals. Biometrics can identify a person's unique physical characteristics, including fingerprints, facial features, voice pattern, retinal, irises DNA and keystroke.*

*The problem with biometrics approach is that the biometric properties cannot reasonably be kept secret. Although biometric systems have advantages over traditional system, one of the unsolved issues is how we can combine cryptography with biometrics to increase overall system security The objectives of this paper are:*

- 1. To critically examine the attacks on traditional personal identification authentication systems in order to determine the risks of using password based authentication..*
  - 2. To examine the biometric technologies and how they are used in authentication with an aim to improvise a secure model.*
  - 3. To apply cryptographic techniques in biometric system with a view to increase its security on networked data access.*
- 

### 1. Introduction

The Information Technology (IT) revolutions such as the Internet, wireless communication, and e-commerce have led to organisational data to be accessed online and offline. The major headache is how to securely authenticate identity of the people they are dealing with. Identification and authentication requirements are steadily increasing in both online and offline. There is the urgent need of both the public and private sector entities to know who they are dealing with. Andrew [2003] has defined authentication as a technique by which a process verifies that its communication

partner is who it is supposed to be and not an impostor. Technology demands that either you fully automate or semi-automate the operations. This means that the data is electronically stored

Authentication is the binding of an identity to the principal. Network-based authentication mechanisms require a principal to authenticate to single system either local or remote. According to Bishop [2003], subjects act on behalf of some other external entity. The identity of that subjects control the action that subjects may take. The subject must bind the identity of that external entity. The trick lies on the proving that the identity supplied for authentication indeed proves the subject to be the real subject.

The current security model for verification of identity, protection of information and authentication to access data or services is based on using a token or password, tied to and thereby representing an individual to either authenticate identity or allow access to information [Ann et al, 2007]. This token may be password or shared secret (something you know), an identity card (something you have) or biometric (something you are). In all this cases, the details of the token are held by a third party whose functions is to authorise and at times allow the transaction to proceed if the details of an individual's token match those stored in a database.

According to Andrew [2003], William [2000], Simson [1997], Kaufman et al [2002], O'Brien [2004], Turban and Wetherbe [2000] and Haag et al [2002], have identified noticeable weaknesses of the traditional-based authentication. The password which is the most commonly used technology for authentication may be guessed by hackers, eavesdropped, forgotten, stolen, wired among others. Bishop [2003] in particular identified a number of password categories that are easy to guess. Kessler [1996] in his paper that appeared in the internet and internetworking security published in 1997 identified the password weaknesses as password guessing, blacklisting, password theft, login spoofing, monitoring the traffic between the user and the computer, and replay attack.

To secure the password-based authentication, a secret that has 64 bit randomness is desirable. This means that the users are required to have much long password that is difficulty to remember. Research has also shown that many organisations are becoming sceptical on the other person they are dealing with. Turban and Wetherbe [2000] noted that vulnerability of information system is increasing day by day as we move towards a highly networked and distributed computing.

Kaufman et al [2002] identified authentication systems such as password-based, address-based and cryptographic authentication all of which have some weaknesses. Many researchers have proposed the use of biometric-based authentication as the most secure and privacy way to access data on the network. [Haag et al 2004, William 2003, Bishop 2003, Ann et at 2007, Umit 2006].

## **2. Authentication**

Authentication is a technique by which a process verifies that it's communicating partner is who it is supposed to be and not an impostor [Tanenbaum 2003]. According

to Bishop [2003] authentication is the binding of an identity to a principal. Verifying the identity of a remote process in the face of a malicious active intruder is surprising difficult and requires complex protocol based on cryptography. Authentication deals with the question of whether you are actually communicating with a specific process. Network based authentication mechanism requires a principal to authenticate to a single system either local or remote [Bishop 2003]. On such a case subjects act on behalf of some other external entity. The identity of that entity controls the actions that its associated subject must bind to the identity of that external entity.

Authentication is used to verify the identity of users in order to control access to resources, to prevent unauthorized users from gaining access to the system and to record the activities of the users in order to hold them accountable for their activities [Mathew 2002]. This is the reason why external entity must provide information to enable the system to confirm its identity. Authentication process consists of obtaining the authentication information from an entity, analyzing the data and determines if it is associated with that entity. The information comes from (i).What the entity knows (Password, secret information), (ii). What the entity has (Badge or card), (iii).Where the entity is (Terminal), and (iv).What the entity is (Fingerprint, odour, retina, hand geometry).

### **2.1. Password-Based Authentication**

Password is information associated with an entity that confirms the entity's identity [Bishop 2003]. This is an example of authentication mechanism based on what the people know. The user supplies a password, and the computer validates it. If the password is one associated with the user's identity, the identity is authenticated. If not the password is rejected and authentication fails. Kaufman et la [2002] argues that password based authentication is not who you know, its what you know. In the middle ages castles and fortress were building to protect the people and the valuable properties inside [Pfleeger and Pfleeger 2007]. This traditional way of providing security was characterised by strong gate or door to repel invaders; heavy walls to withstand objects thrown or projected against them; surrounding moats, to control access; arrow slit to let arches shoot approaching enemies; crenulations to allow inhabitants to lean out from the roof and pour hot or vile liquids on attackers; draw bridge to limit access to authorised people; and gatekeepers to verify that only authorised people and goods could enter.

Turban et al [2003] has defined access control as the restriction of unauthorised user to access to a portion of a computerised user or to the entire system. Access to a computer consist of physical, access to system and access to specific commands, control transaction privileges , programs and data. Password cracking is a technical vulnerability attacks to a system [Scott et al 2003]. Each user account represents a potential vulnerability. In spite of all efforts, even difficult-to-guess password become essentially worthless with the advent of fast cheap computer, utilities like crack and network sniffers. Breaking into the system is no longer a big deal anyone can do that, even a script kiddie [Fadia 2003]. According to Pfleeger and Pfleeger [2007] network

environments needs authentication, but this is difficult to achieve securely because of the possibility of eavesdropping and wiretappings.

Password authentication has a number of weaknesses making authentication to fail. This is due to the way to control password distribution, password is simple and easy, naïve implementation, brute force attack, eavesdropping and guessing [Mathew 2003, Comer 2004, William 2006, Tere and Null 1999, Pflieger and Pflieger 2007]. The passwords that are easily guessed as put forward by Bishop [2003] are those based on Account names; Usernames; Computer names Dictionary words; Reversed dictionary words; Pattern from keyboard; Shorter than six characters and Containing only digits. All these passwords can be learned by: (i). Try default passwords used with standard account that are shipped, (ii). Exhaustively try all short passwords, (iii). Try words in the systems online dictionary or list likely passwords, (iv). Collect information about users. (v). Use Trojan horse, and (v). Tap line between remote use and the host [William 2006].

In the context of communication across networks the attackers that have been by William [2006] are disclosure, traffic analysis, masquerade, content modification, timing, sequence source and destination repudiation. The main disadvantage of password is that they can be stolen and forgotten. Hence to help cap this problem, biometric technologies are used as discussed in the following section.

### **3. Biometric Technologies**

The problems of password authentication can be solved by biometric [Laudon and Laudon 2006]. Biometric has been describe by [Bishop 2003] as the identification by physical characteristics. Using such a feature for computer to authenticate would eliminate errors in authentication. These feature are physiological (fingerprint, hand geometry, eye (iris and retina), face and ear), behavioural biometric (such as voice, signature, keystroke, and gait) and esoteric biometric (facial thermographs, DNA, odour and palm vein). These biometric advantage and disadvantages are discussed in the section that follows.

#### **3.1. Physiological biometric**

##### **a. Fingerprint**

When you touch something with your fingers, you leave a specific impression on the touched item. This is called a finger print. A fingerprint has been defined by Oxford Dictionary as an impression on a surface of the curves formed by ridges on fingertip, especially such an impression made in ink and used as a means of identification. One of the most common forms of biometrics available is the fingerprint. The strengths associated to this are that it is more widely accepted, convenient and reliable.

A foetus' fingerprints are normally fully developed already after seven months. Except for big injury, disease or decomposition after death the specific characteristics on one's finger does not change throughout a lifetime [Henning, 2005].

During the years of working with fingerprint matching, examiners have come up with three levels of detail in fingerprint [Bolle et al 2001 and Bishop 2003]: **Level 1, Global or Galton Level:** If you have a look at your fingerprint you will see it is a

“landscape” full of papillary lines. The higher and lower parts of the papillary lines are called ridges and the valleys respectively. According to [Henning, 2005] the formation of these ridges and valleys are combination of several environmental and genetic factors. The direction in the skin formation is given in the DNA structure but final structure of the fingerprint is formed by different random events such as the position of the foetus in the womb, and the composition and density of the surrounding amniotic fluid. This is why fingerprints, unlike DNA, are different on identical twins. The flow of the ridges and valleys, together with singular points, core and delta, ridge count and orientation all belong to the set of features that can classify and index a fingerprint at the first level [Henning, 2005]. The pattern is classified using the Henry classification system. **Level 2, Local Level:** At the local level the examination process looks closer at different local ridge characteristic, so called minutiae. A minutiae characteristic is a ridges termination, where a ridge ends or a ridge bifurcation, where a ridge diverges into two new branch ridges. The NIST standard for Forensic Identification definition of minutiae is “friction ridge characteristics that are used to individualise that print. Minutiae occur at points where a single friction ridges deviate from an uninterrupted flow. Deviation may take the form of ending division or immediate origination and termination”. **Level 3, Very Fine Level:** At this level, intra-ridge details can be detected. These are essentially the shape and position of the sweat pores which are considered highly distinctive and can help identify a person. It requires high resolution.

The fingerprint scanners are fairly cheap. The FBI certified fingerprint scanners are Indentix, DBI, Crossmatch, Veridom, Infineon and Authentec [Bolle et al, 2001]. However the error rate associated with this is approximately one in one hundred. The fingerprint biometric technology merits are: Long tradition of use as immutable identification in law enforcement; large existing database; Good for forensic investigation; can be collected using low-technology- means and converted into digital forms; and Low cost readers. However fingerprint have problems including Presentation of fingerprint, Elasticity of the skin, Pressure, Bad quality fingerprint, Impostor attacks, Public un acceptance in some countries as it is associated with criminal activities, Contact based sensing and Can be hard to get a good read with old, cold, greasy, cut, or bruised fingers.

#### **b. Eyes (Iris and Retina)**

Current research suggests that it might be possible to use iris scan to determine not only that a woman is pregnant but also the sex of the unborn child. According to Haag et al [2007] future transaction processing systems will be integrated with biometric processing system (BPS). The BPS will capture and process physiological characteristics of the person performing the transaction. The physiological characteristics may include the presence of alcohol, illegal drug, hair loss, weight gain, low blood sugar, vitamin deficiencies, cataracts and even pregnancy.

#### **c. Hand Geometry**

Hand geometry is the measurement and comparison of the different physical characteristics of the hand. According to Bolle et al [2001], Hand geometry is one way of identifying a person. It involves computing the widths and lengths of the fingers

at various locations, using the capture image. These metrics define the features of the user's hand. Hand geometry has been used for physical access and time attendance at a wide variety of location. For example it has been used at Citibank data centre, 1996 Atlanta Olympics, New York university dorms, University of Georgia to verify students when they use their meal cards, Walt Disney World and US Department of immigration and naturalisation has installed it at Fastgate Bermuda International Airport.

The hand scan is manufactured by Recognition System Inc. (RSI)-patent a division of Giant Ingersoll-Rand. Founded in 1986. It is a popular means of biometric authentication due to public user acceptance, good for verification, and easy for self administration.

. Although hand geometry doesn't have the high degree of performance or individuality, they are limited by poor for identification, no international database, and contact based sensing

#### **d. *Face Recognition***

Face recognition is the process of authentication of a person based on different characteristics on his or her face. Humans often recognise each other by their faces, but no one knows which are the most significant characteristics used when a human recognises another human face. This is the reason why there is no unified theory on how to best represent and recognise a face in an automated biometric authentication system. However the fundamental structure of the face is mostly used and most systems are invariant to variables like position, pose, expression, facial hair or glasses.

Face recognition software can operate in different environments, from well controlled environments to uncontrolled environments. The controlled environment is when a person sits in front of the camera and is looking straight into the camera without any special expressions. This method is usually used for verification (confirming claimed identity, such as with a computer logon, or an ATM). The surveillance cameras, at a football match; scanning the faces of the crowd, looking for known hooligans is an example of face recognition system. This is usually used for identification (picking one person out in a database of many). Face application include surveillance, database lookup, video indexing, secure computer logon, airport and banking security. The main advantages of face recognition are: Public acceptance; No intrusive or contact less; Works with photographs, videotapes or other image source; and Good for verification. The disadvantages of face recognition are: need good lighting, poor for identification, and individuals have option of disguising the face.

It is to understand that the face recognition has some challenges. A face is detected according to shape and features in the image, such as eyes, ears, and mouth. To cope with some of these problem, neural networks is often used in face recognition software. This allows the software to "learn" how to perform classification tasks base directly on patterns in data [Orlan, 2003]. The top suppliers of facial recognition system are Viisager Technology, and Visionic

### **3.1. Behavioural biometrics**

### **a. Voice recognition**

Voice recognition is a very common biometric technology. The goal of voice recognition is to understand spoken words- that the contents of what is being said [Orlan et al 2003]. The voice recognition technology will be valuable in systems that require hands free system, such as hand free set for mobile phones and voice command interpretation in automated telephone call centre. Other potential uses include computers, cars, consumer electronics and even appliances [Orlan et al 2003].

Voice recognition has unique advantage over other biometric because it relies on human speech, which is primary modality in human-to-human communication, and provides a non-intrusive method for authentication. By extracting appropriate features from a person's voice and modelling the voiceprint, the uniqueness of the physiology of the vocal tract and the articulatory properties can be captured to high degree and used very effectively for recognising the identity of the person. Recognising the user based on voiceprint is commonly known as speaker recognition in academic community, encompassing speaker verification, speaker identification, speaker classification, speaker segmentation and speaker clustering.

Speaker recognition has improved over the years hence it is very favourable with respect to fingerprint recognition and other biometric [Mansfield et al 2001]. IBM has developed conversational biometrics which combines acoustic voiceprint recognition with knowledge-based recognition and more than 60 invention disclosures have been filed, covering various aspects of robust acoustic voiceprint recognition knowledge-based recognition [Ramaswamy2003].

The major vendors are T-Netix, Naunce, and Veritel of America. There are two modes which voice recognition can operate in. The most common is the constrained mode or text-dependent mode, where the user is restricted to predetermined single words or short phrases. In unconstrained verification mode where the speech input is free, or text-independent, the user is not required to say the same sentence during each access, but this mode has a higher error rate than constrained mode [Orlan et al 2003]. The advantages of voice recognition are: Very high accuracy and flexibility when combined with knowledge verification; Non-intrusive authentication; Incremental authentication-waits for more voice/knowledge data when higher degree of recognition confidence is needed; Continuous authentication, maybe embedded in natural dialogue; Background authentication; Public acceptance; and Inexpensive hardware, suitable for pervasive security management. The disadvantages of voice recognition are: Performance degrades under severe environmental noise; Lack of public awareness; and Not robust enough to determine an identity by itself as is vulnerable to tape recorders mimicry by humans [Malt et al, 2003].

When using voice authentication error mainly occur due to the following factors like age, sickness, acoustic, misread/misspoken utterance, emotional states and placement or distance to microphone or use of different microphone.

### **b. Signature**

Signature dynamics is how a personal signature is generated what features it holds. Geometry, curvature and shape information of words and characters are all features provided by signature itself, while pressure metrics, stroke direction, speed and pen up and pen down events say something about how signature was generated [Orlan et al 2003]. Signature verification may be divided into two groups. (i) Off-line signature verification: These are signatures that only have a static visual record, such as signature on traditional paper, painting etc, often written with ink and (ii). On-line/digitised signature verification: This signature is where pen trajectory and /or dynamics are captured by electronic devices and digitised.

Transformation and atomisation of off-line signatures to digitised media is a complex process, and hence a reliable verification of the signature is not possible. The verification of the on-line signature is on the other hand feasible, and is more and more used authentication in the business world. The signature has weaknesses. It is mostly used for one-to-one verification, different signatures collected from the same person may vary, in shape and feature, shape and weight of the pen, surface on which the signature is written, personal and emotional factors at time of signing, and the signing is routine or not.

### **c. Keystroke**

The keystroke dynamics is to identify users based on his/her typing techniques using traditional pattern recognition and neural network techniques [Bolle et al 2001]. One of the advantages of keystroke dynamics compared to signature is that no traditional equipment is required. Keystroke dynamics recognition system can either be used for single authentication or for continuous monitoring. For single authentication the user typically is required to type a phrase as he/she normally would do, and the software compares this provided template with the one previously stored for this user. In a continuously monitoring system, the software monitors the keystroke dynamics detected on the keyboard. If the user for example left his working station unattended and another person started using the computer (typing on the keyboard), the system could immediately recognise this as a different user, lock the system and ask for re-authentication.

One of the purposes of using the keystroke dynamics for authentication is to make passwords more secure. Because keystroke dynamics require the user to type the password in a certain way, with regard to speed, hold time, press and release pattern among others. It would be more difficult for an impostor to falsely authenticate to the system, even if he/she knows the password.

## **3.1. Esoteric Biometrics**

### **a. Facial Thermographs**

Facial thermography biometric recognition uses cameras sensitive in the infrared spectrum to recognise patterns of facial heat. Facial heat is caused by the blood flow under the skin, and makes a distinct pattern. Facial thermograms yields the same blood vessel pathways that are the underlying vein and tissue structure, but the dynamics nature

of the blood flow causes fluctuation due to environment conditions such as variation in temperature, ingestion of alcohol, drugs and cigarette smoke.

Facial thermography has special feature that other biometric characteristics cannot provide, the image can tell if the person is present or absent, alive or death, attentive or not attentive, physically rested or fatigued, relaxed or anxious [Orlan et al 2003]. It functions from either short distance. It is in place in several airport terminals and at any border crossing to help determine the identity of individuals at a distance who may be involved in criminal activities without alerting the individual that they being monitored.

#### ***b. Deoxyribonucleic Acid (DNA)***

This is a molecule that carries the genetic information necessary for organisation and functioning of most living cells and control the inheritance of characteristics. DNA is a way of biometric characteristics, but differs from standard biometric characteristics in the following ways: DNA requires a tangible physical sample as opposed to an impression, image or recording. DNA matching is not done in real-time and currently not all stages of comparisons are automated. DNA matching does not employ template or feature extraction, but rather represent the comparison of actual samples.

#### ***c. Palm Vein Pattern***

This system uses infrared beam to penetrate the user's hand as it is waved over the system. It relies on using a special camera together with an infrared light. The camera captures the image of the vascular pattern made by the blood vessels everyone has on the back of their hand. These patterns are developed at the foetus stage; differ even between identical twins except from overall size, consistent throughout life. It has high level of authentication accuracy due to the complexity of vein pattern.

## **4. Integration of Biometric with Cryptography**

### **4.1. Attacks on biometrics system**

Authentication with biometric has advantages over password because biometric cannot be stolen, lost, forgotten, lent or forged and is always available, always at hand to speak (Fadia 2003). However biometric have problems such as: Are relatively new and some people may find their use intrusive (resisting), Devices are costly, Readers use sampling and establish a threshold for match is close enough to accept (variation reduces accuracy), can become sing point for failure, False reading, speed limits accuracy, and forgeries. These attack areas are (i). Type one attacks: involves presenting fake biometric e.g. fingerprint made from silicon, face mask, fake iris texture to the sensor, (ii). Type Two attacks: Replay attack-because an interpreted biometric is submitted to the feature extractor, bypassing the sensor, (iii). Type three attacks: The feature extractor module is replaced with a Trojan horse program that functions according to its designer's specification, (iv). Type four attacks: Genuine feature values are replaced with values selected by the attacker, (v). Type five attacks: the matcher is replaced with Trojan horse, (vi). Type six attack: template database attack e.g. addition, modification, or removal of

template, (vii). Type seven attacks: templates are tampered with i.e. stolen, replaced or altered in transition medium between the template and the database, and (viii). Type eight attack: The matcher result (accept or reject) can be overridden by the attacker.

Biometric security is a fast growing area of computer security [O'Brien 2004]. Vulnerability of information systems is increasing as we move towards a networked computing [Turban et al 2000]. The need for security is now increasing because organisations are now recognising as corporate data is increasing being stored on computer and acceptance that any loss or unavailability of these data could prove to be disastrous [Cannony and Begg 2004]. To enhance biometric security, encryption techniques are examined in the next section.

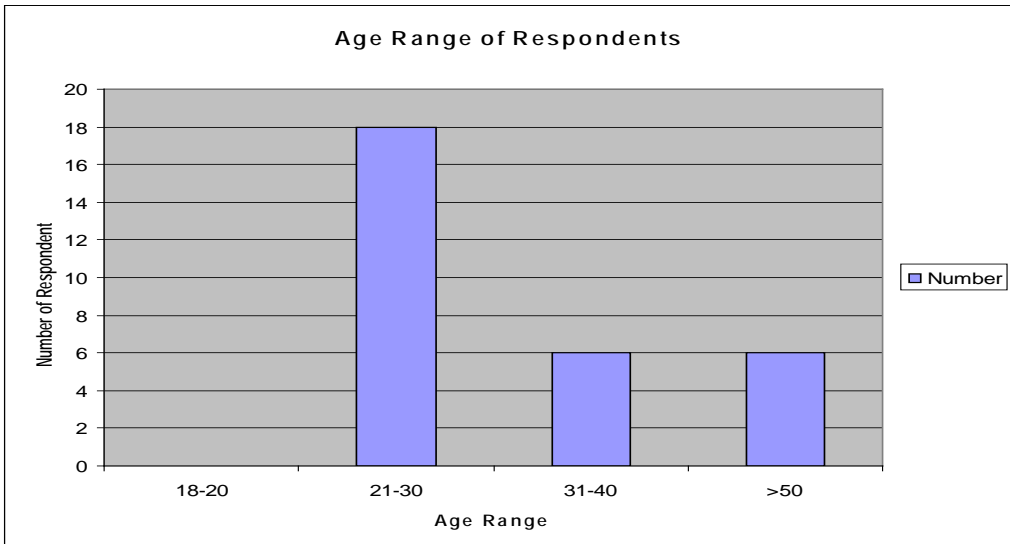
## **4.2. Biometric Encryption**

Cryptography is the science and art to transform message to make them secure and immune to attacks [Behrouz 2006]. Encryption is the encoding of the data by special algorithm that renders the data unreadable by any program without decryption key. Biometric encryption authentication is a strong, certainly far superior to passwords. The technology is mature, products exist standards define product's interface, reliability rate are acceptable and costs are reasonable [Pfleeger and Pfleeger 2007]. The cryptographic techniques those are available like public key infrastructure, hash algorithm, message encryption and Kerberos. These though have problems according to Simson [1997] such as: Private keys are not people; distinguished names are not people; there are too many Robert Smith; Today's digital certificate doesn't tell much; and X.509V3 does not allow selective disclosure.

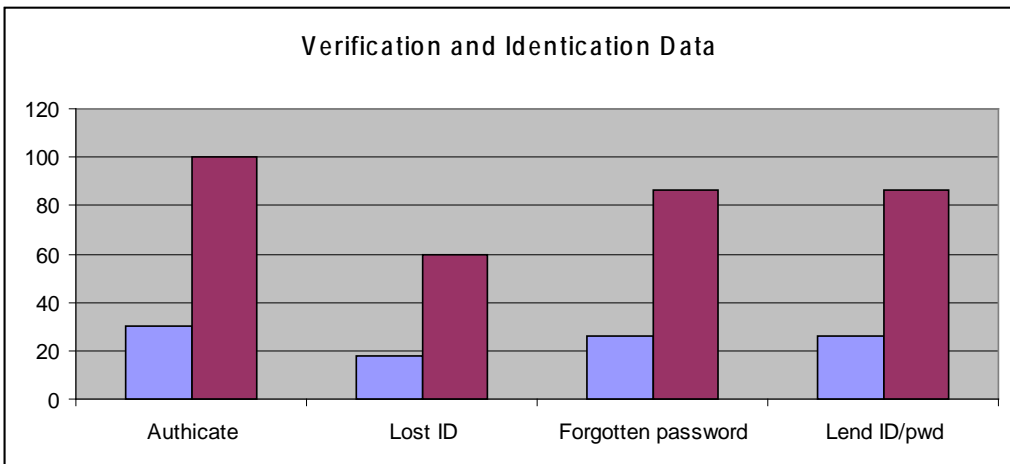
## **4.3. Survey Results Analysis**

Various studies and survey have been done as examined in the previous section in this paper. These studies however are from the developed countries with that have the latest technologies. In less developed countries like Kenya and others in Africa, the issue of biometric security is different. In a survey we did at Kabarak University Kenya reveals new challenges facing biometric application in less developed countries. Most active users of the electronic are between the age of 21 years and 30 years as shown on figure. This age bracket is aggressive in having an authorised access.

**Figure 1: Demographic Data**

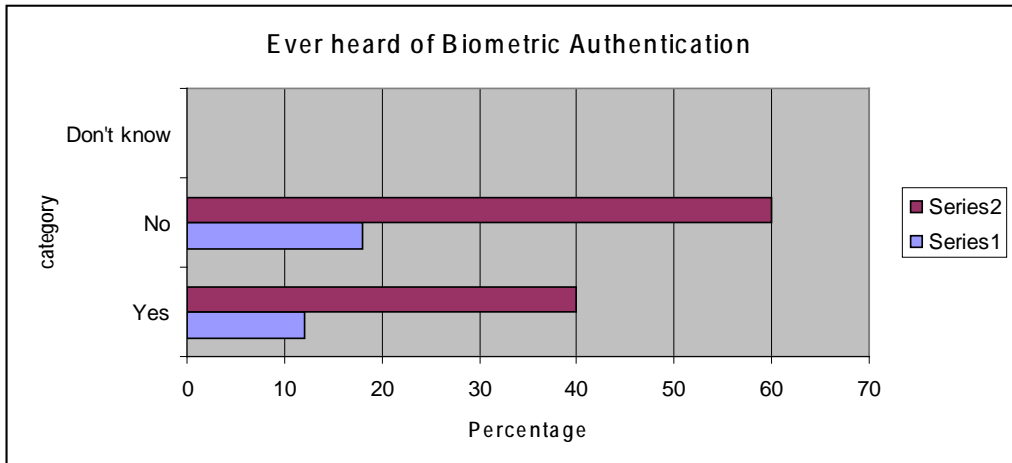


**Figure 2: Authentication and Passwords**



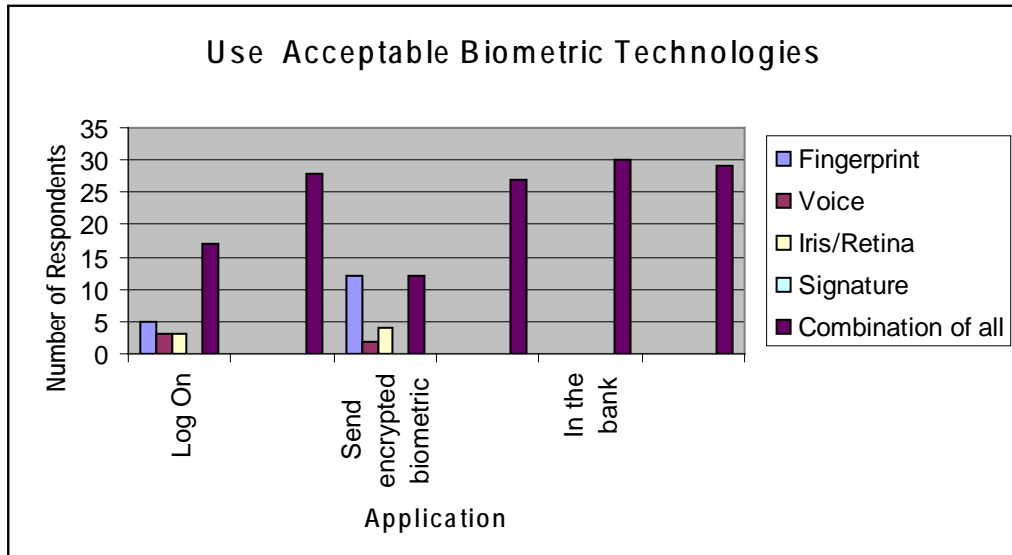
The users of the electronic resources at Kabarak University have to be authenticated before they can access the resources. This is probably due to the password requirement the system administrators. Figure 2 show that 100% of these users must supply their username and passwords before they can access the computer resources, of this 60% had lost their passwords, 84% have ever forgotten the password and similar percentage had given out their password. This presentation is shows clearly that the use of password is a threat to electronic resources.

**Figure 3: Participants with Biometric Authentication Information**



It is interesting to note that while no biometric system had been installed in the institution before this survey, 40 percent of the respondent had a theoretical understanding of biometric technologies as show in figure 3. The 60%, who had no idea about, are like to pause danger to authentication process. However, when asked which biometric they will prefer to use combined technologies as shown in figure 4.

**Figure 4: User Acceptance Level**



The survey done shows that security is of great concern for most of the electronic user. What the less developed countries need is brainstorming, availing the information. From 4 there are various reservations on biometric technologies. The signature and fingerprints have low acceptance level compared combined technologies. What the users need is system the assures the of the security of their data.

## 5. Conclusion

Modern Information Technology revolution that is heavily networked requires authentication that is the binding of an identity to the principal. The password which is the most commonly used technology for authentication has weaknesses. These weaknesses can be solved by biometric technologies such as fingerprints, hand geometry, facial thermographs, face recognition and DNA. The survey done also shows that there is need for combined biometric technologies. Though biometrics has problems; they can be enhanced by cryptographic techniques. An integration of biometrics with encryption provides an enhanced secure authentication system for our electronic resources. In less developed countries like Kenya and other African are willing to implement new authentication system. What are needed in the less developed countries are the willingness and knowledge availabilities.

## References

- ANKIT FADIA (2003). Network Security A Hacker's Perspective. Macmillan. New Delhi.
- BOLLE R., JAIN A., PANKANTI S. O. (2001). Biometric-Personal Identification in Networked Society. Kluwer academic publication.
- THOMAS CANNONY AND CAROLYN BEGG (4<sup>th</sup> ed) (2004). Database System a Practical approach to design, implementation and Management. Addison Wesley. New York.
- CHARLES P. PFLEEGER AND SHARI LAWRENCE PFLEEGER (4<sup>th</sup> ed) (2007). Security in Computing. Pearson Education. India.
- DOUGLAS E. COMER [2004]. Computer Networks with Application. Pearson Education. India
- STEPHEN DOYLE (3<sup>rd</sup> Ed) (2001). Information System for you. Nelson Thornes Ltd. Uk.
- STEPHEN HAAG, MAERE CUMMINGS, AND DONALD J. MCCUBBREY (3<sup>rd</sup> Ed)(2002). Management for Information Age. McGraw-Hill Irwin. Boston
- CHARLIE KAUFMAN, RADIA PERMAN and MIKE SPECINER (2<sup>nd</sup> Ed) (2002). Network
- KENNETH C. LAUDON AND JANE P. LAUDON (9<sup>th</sup> Ed) (2006). Management Information System Managing the Digital Firm. Printice-Hall New Delhi
- STREBE MATHEW (2002). Network Security Jumpstart. San Francisco. London.
- MATT BISHOP (2003). Computer Security Art and Science. Pearson Education. India.
- SIMSON GARFINKEL (1997). Web Security and Commerce. O'Relly and Associate. USA
- TANENBAAUN S.ANDREW (4th Ed) (2003). Computer Networks. Prentice Hall. India.
- PARNEL TERE AND CHRISTOPHER NULL (1997). Network Adminstrator's reference. McGraw-Hill. Osborne.
- MCLEAN,TURBAN AND WETHERBE (2nd ed) (2003). Information Technology fo management. Jonh Wiley and sons. New york.
- STALLINGS WILLIAM (2000). Network Security Essentials Application and Standards. Pearson Education. Singapore.
- WOODWARD JR. ORLAN AND N M. HIGGINGS P. T. (2003). Biometrics. McGraw-Hill Osborne. California.