International Journal of Recent Engineering Research and Development (IJRERD)
Volume No. 01 – Issue No. 06, ISSN: 2455-8761
www.ijrerd.com, PP. 01-08

Biometric Personal Data Security Systems: Trustworthy Yet?

Dr. Latika Kharb
Associate Professor (IT), JIMS, Sector-05, Rohini, New Delhi, INDIA

Abstract: In today's society, advances in technology have provided us higher levels of technical knowledge through the invention of different devices and thus made our life easier. However, each innovation has the potential of some hidden threats to its users like theft of private and/or personal data and/or information. In the mobile age, where personal information is available via multiple points of entry, there are a number of ways for hackers to get to someone's information like name, phone number, address, credit card numbers, bank account information or even their personal files. As digital data become more prevalent, users try to secure their information with highly encrypted passwords and ID methods. This increasing threat in cyber security has led to the birth of biometric security systems. In this paper, while outlining the main methods of biometric data security techniques used to verify user identities like fingerprint authentication, voice recognition, facial recognition detector, retina or iris scanner, veins recognition and DNA biometrics system; we also discussed about the advantages and disadvantages of personal data security systems. In brief, in this paper, we will take a look at the future software security methods that aim to ensure safety of user's data.

Keyword: Biometric security system, facial recognition, fingerprint reader, voice recognition, iris and retinal recognition, vein recognition, DNA recognition, privacy, safety.

1. Introduction

Biometric system includes any details of the human body which differs from one human to other to be used uniquely as a person's unique identification like: finger/ palm print, retinal/ iris scan and DNA testing. Biometric systems are developed to collect and store data in order to use it for verifying personal identity of any person. The biometric security system is just like a lock and key mechanism to control access to specific data where biometrics security system is the lock and biometrics is the key to open that lock [1]. There are five most basic criteria for biometric security system namely [2]:

- **Uniqueness:** It indicates how uniquely the biometric system recognizes users. For instance, DNA of each person is unique and it is impossible to be replicated.
- **Universality:** It indicates unique characteristics of each person which cannot be replicated. For example, characteristics of retinal and iris scan.
- **Collectability:** It requires the collection of each characteristic / trait of system in order to verify their identification.
- **Performance:** It outlines how well the security system works.
- **Accuracy & Robustness:** It validates that a system is accurate and robust.

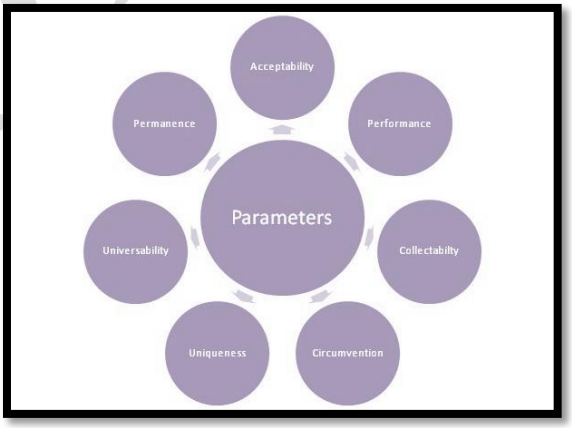

Figure 1: Parameters of Data Security

2. How biometric identification system works?

The technology which works based on pattern recognition is known as biometric technology. Biometrics provides highest level of security. It utilizes following characteristics in order to authenticate or identify the

valid user like: fingerprints, voiceprints, facial features, writing patterns, iris patterns, hand Geometry and so on. Biometric system consists of following modules:

• **Data Collection:** The main component is sensor which captures the image of the pattern. This image is compressed.

• **Transmission:** The compressed image of the pattern is transmitted and stored.

• **Signal Processing:** The live pattern sample is collected and unique features are extracted using signal processing algorithms. This is compared with the unique features of the image initially stored at the time of enrollment.

• **Data Storage:** The place of storage for the image samples of many people. This can be hard disk or any other memory types.

• **Decision:** This is kind of software or hardware or combination of both which compares the live data with the one stored in the database for authentication and verification purpose.

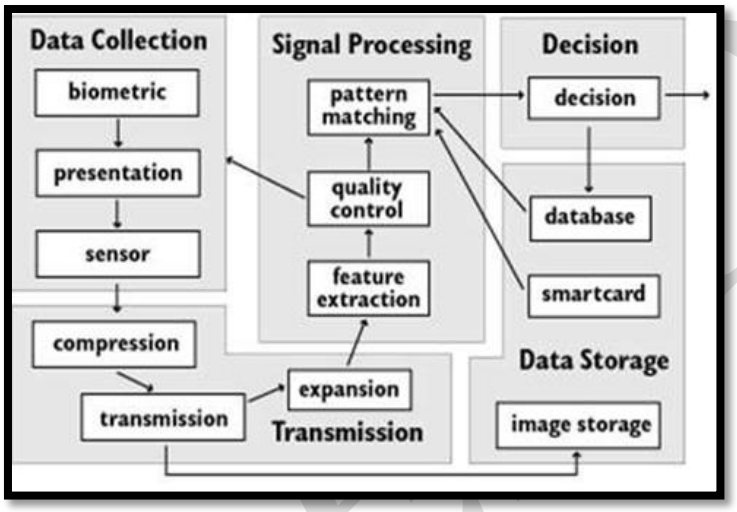

Figure 2: Block Diagram of Biometric System

3. Biometric Personal Data Security Systems

Today, a number of biometric data security systems are part of our daily lives, namely:

1. Fingerprint Authentication System
2. Voice Recognition System
3. Facial Recognition Detector System
4. Retina or Iris scanner and Recognition System
5. Veins Recognition System
6. DNA Biometrics System

Now let's start evaluating each biometric security system along with its safety aspects.

1. Fingerprint Authentication System

The Concept:

Our fingerprint is having a number of ridges and valley on the inner side of finger/thumb that is unique to each human. Ridges are the upper skin layer segments of the finger and valleys are the lower segments [3]. One of the most popularly used techniques of biometric authentication is fingerprint scanning. While high security professionals have been using biometric identification for years, it has gained its widespread use with the release of concept of Touch ID. In order to save our fingerprint to file, users must go into their device's settings and enable Touch ID; then place their finger on the home button. The user then lifts their finger off the home button, and places it back on a number of times so a full scan can be performed. While Touch ID was originally used only to unlock the device, application developers have started to make it usable as a way for users to sign into their device's mobile apps.

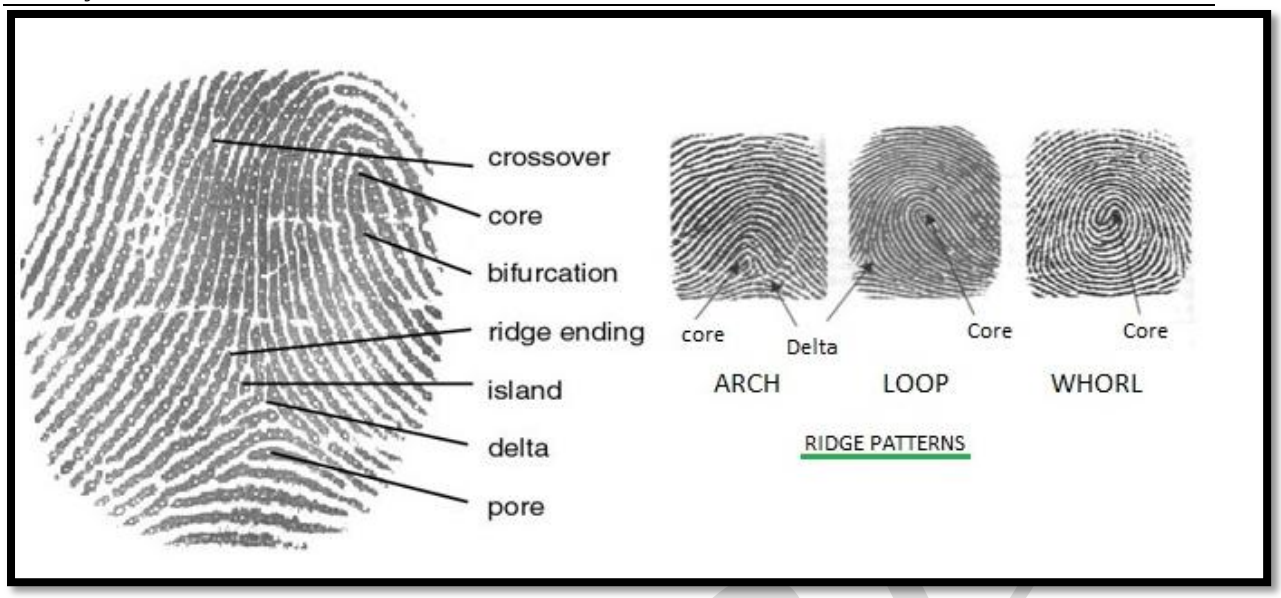

Figure 3: Segments and Patterns in Fingerprints

In the last two years, banking institutions like HSBC, Bank of America, and U.S. Bank have all allowed their mobile banking customers to use Touch ID instead of entering a username and password to gain access to their mobile app.

Is it Secure?

There are several benefits of using fingerprint recognition systems as it is easy to use, cheaper to install and has low power consumption for its equipments. Fingerprint authentication is secure as the fingerprint is a unique ID of a person and thus one of the best passwords available globally as it's always with you. For simple hackers who attempt to crack passwords using password generators or by guessing passwords, they would find themselves unable to replicate the fingerprint. However, there are some disadvantages in this system. If the finger gets damaged and/or has one or more cuts on it, identification becomes increasingly hard or impossible. However, hackers have a habit of keeping ahead of the latest security technology. Not long after Touch ID started gaining widespread acceptance, security experts began warning users of potential issues. Recently, hackers have been found making use of high-resolution pictures of people and then lift their fingerprint from the picture. So, while it's convenient that we have fingerprints always with us, the negative aspect is that they are also left on everything we touch. Experienced hackers will have the ability to lift prints from pieces of paper or computer keyboards. Companies have started to work on increasing level of security with the second stage of fingerprint authentication. For example, Samsung and Apple have started to release products with double locks in software that require both a fingerprint and a pass code in order to use the device.

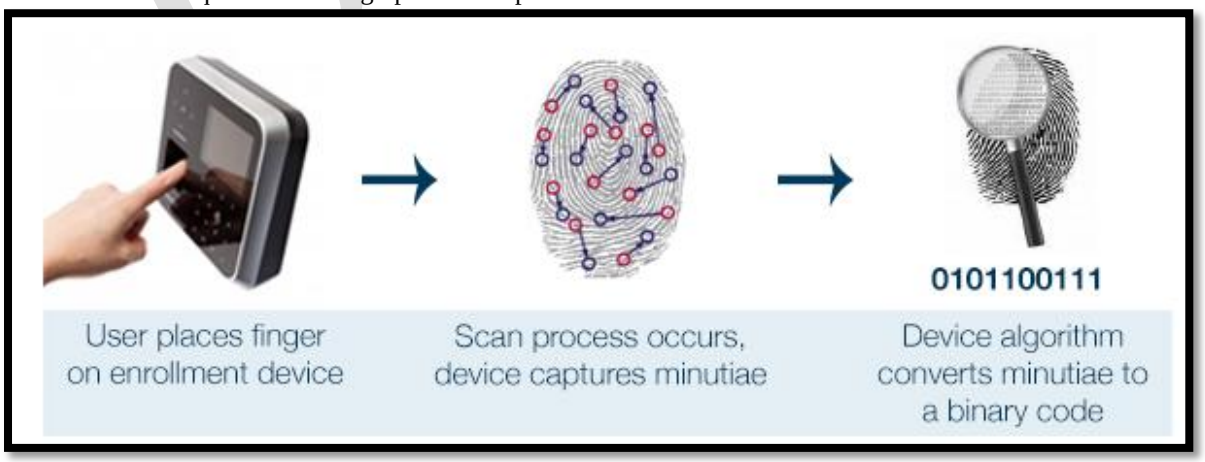

Figure 4: Fingerprint Authentication Process

We have to just remember numbers of the pass code but hackers are after all behind you, as we are leaving our fingerprint on the pass code buttons.

2. Voice Recognition System

The Concept:

In voice recognition, there are two main factors which make a person's voice unique: voice tract and voice accent. By taking advantages of these two characteristics, biometrics technology has created voice recognition systems in order to verify each person's identification using only their voice.

Figure 5: Voice Recognition Devices

Voice recognition systems are easy to install and it requires a minimal amount of equipment like microphones, telephone and/or even PC microphones. Along with the other biometric methods mentioned in this technical paper, a user's voice is also proving to be an excellent security option as it is unique and it's always with the user. While it's easy to think that a father and son / siblings sound "just like" each other, an individual's voice is unique due to the shape of their vocal cord, and the way they move their mouth when speaking and pressure they exert on voice tract. Voice recognition is not as widespread in use and accepted as compared to fingerprint authentication but is now gaining demand in the software security world. For example, banks in general have started recognizing that passwords have become the weak point of their security infrastructure, and are looking to move towards either biometrics or specifically voice recognition in the coming years. For example, banks like HSBC have already rolled out their Touch ID authentication and replaced it with voice enabled recognition to authenticate their bank account. Various software development firms like Micro strategy have made an app called Usher that allows its employees to sign in with their voice.

Is it secure?

The weak point for voice recognition seems obvious; one can just record a person's voice either forcefully or even as a fraud attempt and then play it back when a password is requested. To prevent the risk of unauthorized access via recording devices, voice recognition systems will ask users to repeat random phases which are provided by the system during verification state [4]. Another problem is that often, there are no stored files in a database anywhere and the user attempting to be authenticated for the first time will often repeat a few phrases so the software can recognize how the phrases are stated, rather than recognizing the phrases themselves. When asked for authentication, a user will be asked to repeat a random phrase, and will have a limited time to do so. Unless a hacker has a number of random recorded phrases ready and can play them with perfect clarity in the time allotted, they would be denied access.

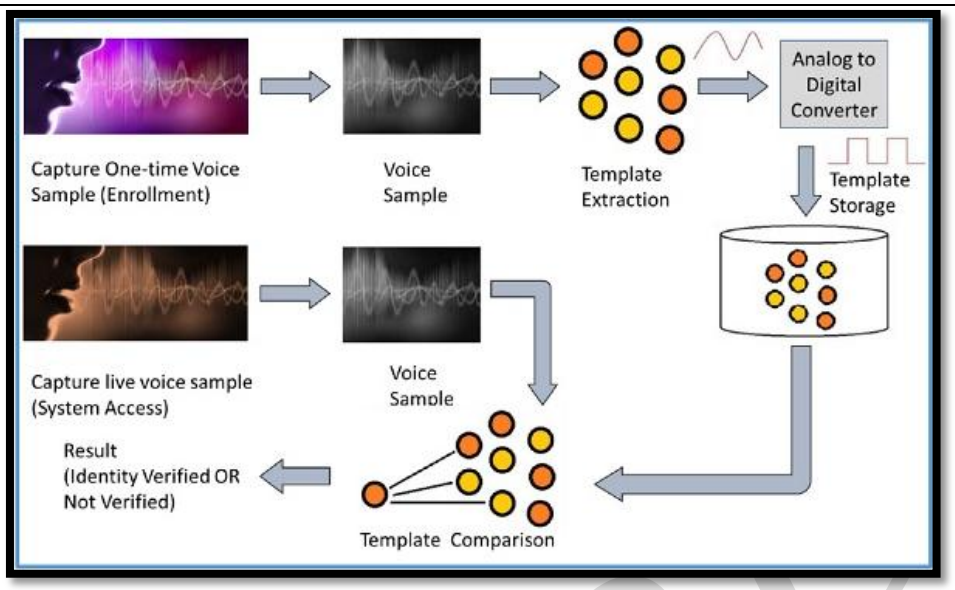

Figure 6: Process of Voice Recognition

The biggest current threats to voice recognition technology come in the form of loopholes in the software's functionality. Siri, for example, was hacked through the headphone port and a fraud hacker could send radio waves through the microphone port that would activate the home button, and thus, allow them to install apps and perform financial transactions. Example of hacked programs include: Google Now app, which was hacked when researchers at AVG created an Android game with access to voice commands. Those commands were then used to access Google Now, granting hacker's access to the phone's messaging service. However, these Apple and Android hacks are the tasks of high level hackers and couldn't be done by a standard hacker. In present era, we can conclude that voice recognition technology is extremely secure and it would be greatly helpful to end users if software developers begin to implement these precautions.

3. Facial Recognition Detector

The Concept:

Facial recognition technology is very popularly used widely as it does not require any kind of physical contact between the device and/or users. Cameras scan the face of user and then match it to the database for verification. It will measure the overall structure, shape and size of facial features such as the distance between both eyes, size of nose, position of mouth, size of ears, shape and size of jaw, size of eyes, shape of mouth and many other expressions.

Figure 7: Facial Recognition Device

Used by far fewer people than either fingerprint authentication or voice recognition, facial recognition promises to provide secure logins for its users.

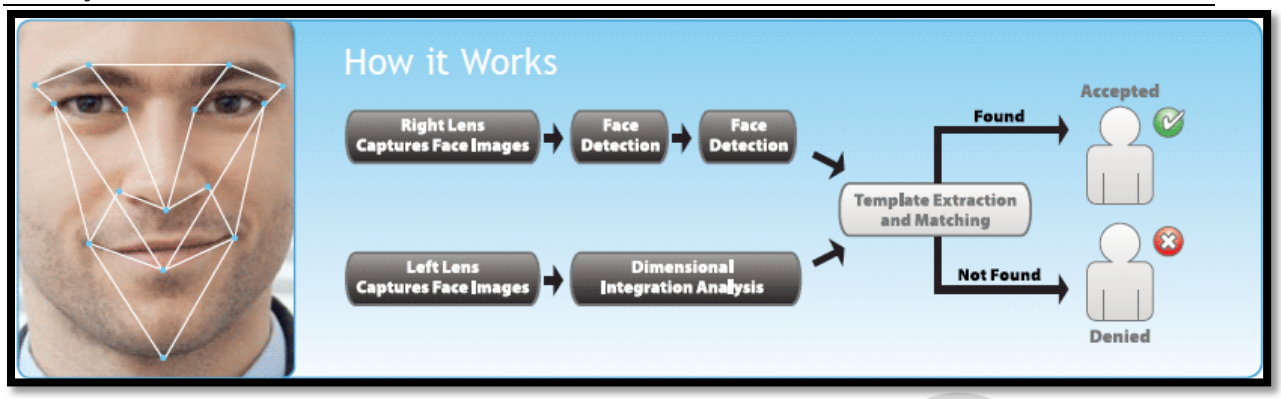

Figure 8: Facial Recognition :How it Works?

With the ability to recognize the main points on a human face (each human face has about 80 of these points), software like Identix is able to find a user's face i.e. through 3D facial recognition, it finds features such as the shape of someone's eyes, nose, or chin.

Is it secure?

It is easy to install with no need of costly hardware. In it's current commercially available state, facial recognition is quite usable. Many initial procedures require the user to turn their head and (or) blink to confirm their identity. As with everything else, though, this can be bypassed too. Time is the most negative affective factor with face recognition technology because as the user ages will change over time [3].

4. Retina or Iris scanner and Recognition System

The Concept:

Iris recognition systems will scan the iris through different characteristics like size of pupil, iris color, patterns of iris etc. Iris recognition security systems are considered as one of the most accurate security system nowadays. It is a unique and easy mechanism to identify a user and is still the easiest and fastest method to identify a user.

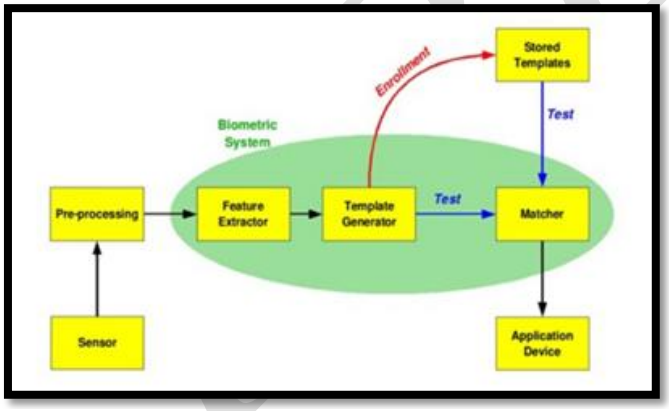

Figure 9: Process of Iris and retina Scanning

Figure 10: Retina Scan Apparatus

Is it secure?

Retinal scanning spreads a beam of light into the users eye that traces the path of the retina and in Iris scanning, users have a picture taken of their eye from a further distance. Both techniques are extremely secure as no two people have the same iris or retinal pattern. E.g. ZTE's Grand S3 smartphone allows users to unlock their phone with this technology.

Iris scans are estimated to be up to ten times more accurate than a fingerprint scan and are very hard to spoof. The biggest threat to this method may be health concerns. Having a light shined into your eye might affects our vision on a long-term basis. With this in mind, the biggest hurdle for retina and iris scanning may not be how secure it is, but how willing users would be to adopt it.

5. Veins Recognition System

The Concept:

Vein recognition system is one of the recent inventions in biometric technologies. Veins are the blood vessels carrying blood to the heart and these veins have unique behavioral traits in each person. So, taking advantage of this feature, biometrics uses veins as a method to identify a user. The vein recognition system captures images of the vein patterns inside a users' fingers by applying light transmission to each finger.

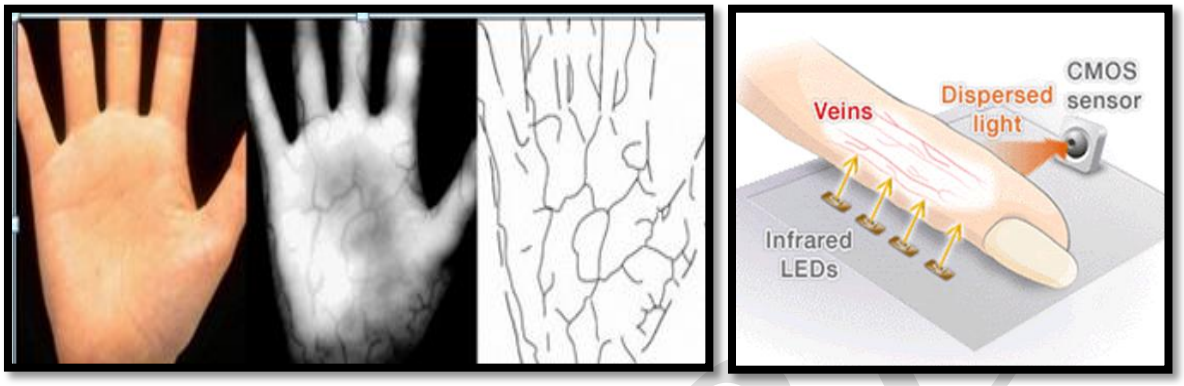

Figure 11: Vein Recognition System

Is it Secure?

Vein recognition systems are getting more attention from experts because it has a higher level of: security, accuracy, reliability, and have a shorter time for verification process with a low cost on installation and hardware.

6. DNA Biometrics System

The Concept:

One of biometrics technology that is used recently in security systems is DNA biometrics. It is impossible to fake this characteristic of a user because each person's DNA is unique. Each person's DNA contains some trait from his/her parents. Each and every cell in the human body contains a copy of this DNA and sample can be taken to verify it easily. DNA profiling will decide the amount of VNTR (variable number tandem repeat) which repeats at a number of distinctive loci and these amounts of VNTR will make up an individual's DNA profile [3].

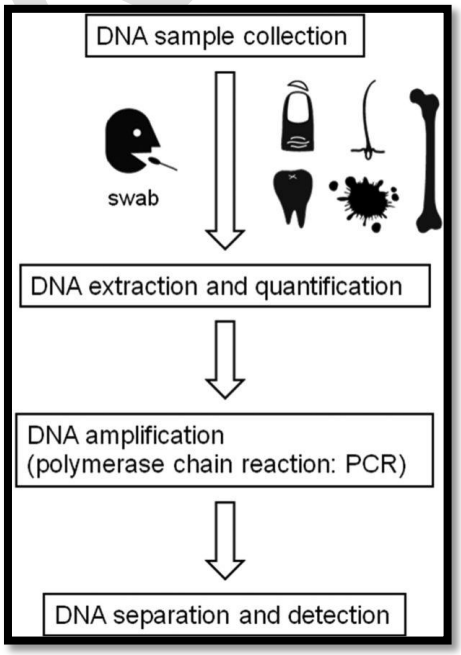

Figure 12: Process of DNA Biometric System

Is it secure?

The major drawback of DNA biometrics is that it is time consuming and lengthy process of verification.Moreover, it also requires expensive equipment in order to match/ check the DNA successfully.

Advantages of Biometrics Security System

In this section, we'll enumerate the advantages of using biometric security systems [5]:

1. *Uniqueness:* With uniqueness of biometrics technology, each individual's identification will be single most effective identification for that user. A chance of two users having the same identification in the biometrics security technology system is nearly zero.
2. *Highly Secure:* The highly secure way of identifying users makes this technology less prone for users to share access to highly sensitive data. For example, users can share their fingerprints, iris and so forth allowing other users access to secure information. This makes it ever more secure allowing user information and data to be kept highly secure from unauthorized users.
3. *No fear of Theft:* The identification of users though biometrics cannot be lost, stolen or forgotten. This aspect of biometrics technology allows it to become more popular in its use. This method of identifying and giving access to user makes user identification a lot easier.
4. *Easy to install:* Most biometrics security systems are easy to install and it requires small amount of funding for equipment.

Disadvantages of Biometrics Security System [6]

Even though, there are many advantages of biometrics security system, it still has many flaws in its system. Each biometrics application method has weaknesses which can cause problems for its users. For example, if the biometrics security system uses fingerprints to identify its users and an accident causes a user to lose his/her finger then it can be a problem during the verification
process. For voice recognition methods, illnesses such as strep throat can make it hard for authorized users to get access to their information. Another factor that can influence voice and fingerprint recognition systems is the continuous aging of its users. For iris or retinal scanning applications, users may find it very intrusive. Users may also have the concern for the safety of their eyes during the iris or retinal scan. Furthermore, databases used to store user identification data will be very large which might form a potential threat. For scanning retinal/iris characteristics and storing large amount of database, biometrics system requires new and modern technology. Moreover, the cost for equipment is also expensive.

Conclusion

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it. In conclusion, biometrics technology is a new technology for most of us because it has only been implemented in short period of time. There are many applications and solutions of biometrics technology used in security systems. It has many advantages which can improve our lives such as: improved security and effectiveness, reduced fraud and password administrator costs, ease of use and makes live more comfortable. Even though the biometrics security system still has many concerns such as information privacy, physical privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

References

[1]. Jain, A.K.; Ross, A.; Pankanti, S., "Biometrics: a tool for information security" Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125 – 143
[2]. Michael E. Schuckers, "Some Statistical Aspects of Biometric Identification Device Performance", 2001
[3]. "Biometrics new portal" UK 2011http://www.biometricnewsportal.com/
[4]. Peter O'Neill; Anne O'Neill; Shaun Winters; Lucy Kwiaton "Biometrics security system", 2011 http://www.findbiometrics.com A Survey of Biometrics Security Systems http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/index.html
[5]. Massimo Tistarelli and Marks Nixon, "Advances In Biometrics", Springer-Verlag Berlin Heidelberg 2009,ISBN 03029743
[6]. PBworks, "Advantages and Disadvantages of technologies", 2006 http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies