BIOINFO Security Informatics
Volume 1, Issue 1, 2011, pp-06-10
Available online at: http://www.bioinfo.in/contents.php?id=344

Biometrics Authentication Techniques in ATM

[1]Sandeep S. Majge and [2]Hanmant W. Kulkarni
[1]*Department of Computer Science, M.U. College, Udgir, (MS), India*
[2]*Department of Commerce, Shivaji College, Udgir, India*
e-mail: s_ssm@rediffmail.com

Abstract—This paper presents the different biometric authentication techniques in ATM. The biometrics authentication technique consists of two types as basic and developing. Problems and issues as well as current applications of biometrics will also be discussed.

Keywords: Internet protocol, ATM, Biometrics, Authentication

I. INTRODUCTION

Biometrics is the statistical analysis and measurement of human traits or characteristics. Once these measurements have been taken, they may then be used to authenticate an individual or user. It is also the measurement of life for statistical or actuarial purposes. In this case we are just talking about a combination of machinery and physical characteristics of a human being that together form an authentication system. An authentication system is a method for a computer to decide whether you are whom you say you are, and thus a method to let you into a certain system or deny you access to it. (In this case one should not merely think of one's own computer but also of e-commerce for example, credit card use, etc.)Most of the time, authentication is done by the use of a password and username combination. (Sometimes by trusted ip-addresses or other things.) The most obvious of these systems are, like the fingerprint- or iris-scan systems. Hence biometrics is viewed as an emerging technology, in reality, their use has been documented throughout the history of mankind[1].

II. BIOMETRIC PROCESS

There are many differences between the different biometrical authentication systems, but all systems basically work by the same principle. To be able to recognize if a person is who he claims to be, the system will need to compare a sample of the physical structure of a person with a sample that was taken earlier. To make sure the system can make a comparison one first has to "signup" with the system. This process is called enrollment. A biometric sample is taken of the user, which then can later on be used to compare with, when a user requests to be authenticated. The sample (which is called "biometric template") that is taken during enrollment is saved into the system and after that the system has something to compare a user with when he tries to authenticate. When the given biometric sample matches the one in the system, you are authenticated and get access and when there isn't a match; you don't. The whole process of authentication can also be monitored. In this case, the process of trying to be authenticated is send to an outside network, another computer, etc. For the authentication process the different biometric techniques are used which are discussed below.

III. BIOMETRIC TECHNIQUES

The different biometric techniques are categorized as basic and developing which are as follows.

A. Basic Biometric Techniques

1. Fingerprint verification

Basically this is a technology, where you use an apparatus connected to your computer that scans your finger and so recognizes that you are you. If it recognizes you, you are granted access, if not you are not. Fingerprints have certain natural traits that make them ideal for use in biometric systems. Fingerprints are developed between the first and second trimester and remain unchanged (barring any damage or scarring) until death. Fingerprints are unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used by law enforcement agencies for many years. But this type of one-to-many match is seldom used for commercial purposes. Most fingerprint systems operate in authentication, rather than identification, mode. Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method). Others analyze the distance between ridge endings and ridge burifications on the finger. The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three-dimensional surface shape) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader. The amount of bytes used to save a finger-scan is about 250 up to a thousand bytes, whereas an exact copy of the fingerprint uses 250 kilobytes. So in fingerprinting an exact copy is made for getting meaningful information.

2. Hand-scan

Hand geometry involves the analysis and measuring of the hand and fingers. The user places their hand on the

reader with their fingers in designated positions. It uses a 32 thousand pixel digital camera to measure the width, length and thickness of the hand and the fingers. Over 90 different measurements are taken and all this is saved in a 20 bytes template. There are already many hand-scan devices on the market, many of which can be used with your normal home-pc.

3. Voice-scan

The voice-scan technology makes use of the fact that no voice is like any other. Microphone-recording device records the voice of a user and is able to recognize this voice on a later day, because of the specific characteristics of a human voice. It's important that for both the first voice recording and later recognition, the same equipment is used under basically the same circumstances, because things like sound-/recording-equipment quality, echo's, background noise, etc. influence the recognition system. One of the advantages of voice-scan technology over other biometric authentications systems is that it requires no expensive equipment. It can be used with a normal computer and soundcard.

4. Iris-scan

Another well known biometric authentication system is the iris-scan The idea is comparable to the finger-scan. The eye contains a certain structure which is different for all human beings and thus can be used to authenticate a person. Iris contains a very complex pattern and large number of measurable characteristics that make it practically impossible to replicate. Even a person's right and left iris patterns are different. For iris scanning, a camera is used to record a digital image of the user's iris. Contact lenses and glasses do not interfere with the scan.

With the use of normal or ultra-violet light, it's possible to distinguish patterns in the "trabecular meshwork", a tissue that divides the iris in a radial fashion. Not only this, but also other recognizable things like freckles, rings and other specific characteristics are encoded into a 512 byte Iris code which is the iris-scan's equivalent of the fingerprint. Although in basics the iris-scan has always been a bigger and more expensive system, it has proven to be very accurate. It has been used so far in high-security facilities like ATM machines, airports.

5. Facial-scan

The facial-scan technique makes uses of specific characteristics of the human face. A camera of some sort (digital, video or thermal) is used to capture the features. It compares data from certain parts of the face with your face during a scan. Only certain parts of the face are used in this technique (the upper outlines of the eye sockets, the areas around the heek bones, and the sides of the mouth) because these parts are hard to change with plastic surgery. And so, in this case it wouldn't matter if you would lose some weight, become a bit thin or change your hairdo. The facial-scan technology works fine at a 320x240 resolution and 3, 5 frames per second, which means it can be used with normal pc video equipment

6. Signature verification

Signature verification involves the use of a special pen, tablet, or both to capture the way a person signs their name. Although the final appearance of the signature is important, a number of other attributes are captured as well. These include speed, velocity, pressure, angle of the pen as well as the number of times the pen is lifted from the pad. Signature verification is considered to be very accurate. Additionally, most users will not object to providing their signature for verification, as they are use to identifying themselves by signature all the time (i.e. credit card slips, checks, etc.).

7. *Hand geometry*

Hand geometry involves the analysis and measuring of the hand and fingers. The user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established uses of biometrics today. It is accurate and fast.

B. Developing Biometrics

1. Palm print

Similar to fingerprinting, palm print biometrics is a system that measures the physical characteristics of an individual's palm. The specified palm is placed on a reader where the measurements are taken. Not enough data has been collected yet to determine if palm prints are as unique as fingerprints.

2. Vein pattern

Vein pattern matching involves scanning the vein patterns on the back of a user's hand. The user places their hand into a reader. Inside a small black and white camera and LED array are used to capture the digital image. The LED array, combined with filters also inside the reader, is used to magnify the contrast of the veins under the skin. This results in a vein distribution pattern that may be used for authentication. Certain vein aspects or points, as well as the whole distribution, are used for verification. Like finger and palm prints, vein distributions are unique, making them an attractive

BIOINFO Security Informatics
Volume 1, Issue 1, 2011, pp-06-10
Available online at: http://www.bioinfo.in/contents.php?id=344

biometric for use. The right and left hand of an individual do not exhibit the same vein distribution pattern. They can also be expensive to implement and are not as convenient as fingerprint readers. There is also the question of how vein patterns change over time. It is unknown whether there is significant change in the vein pattern over long periods of time and how this could possibly affect authentication.

3. Ear shape, body odor and gait analysis

Ear shape is a physical biometric that measures the shape of the outer ear, lobes and bone structure. Done much in the same manner as facial recognition, a two or three-dimensional picture may be taken. Body odor is a system that analyzed the natural body odor given off by an individual. Electronic sensors are used to gather the odor, usually from the least intrusive area as possible, such as the back of the hand. Gait analysis is the analysis of the way an individual walks. This usually includes some sort of mat with sensors that an individual will then walk across. Measurements of the speed, pressure applied by the foot, manner in which steps are taken as well as the number of steps required are taken and used for verification [2].

IV. BIOMETRICS APPLICATIONS

As stated previously, the use of biometrics is an emerging technology. Because of this, it is likely that most of us have not worked with security systems that utilize them. There are a relatively few number of vendors that manufacture these specialized products and costs at times have been prohibitive. But like most technologies, costs will decline as manufacturing and research processes improve. And as user acceptance increases, it is more likely that biometrics authentication will become a part of our everyday lives. Since the purpose of any authentication system is to prove the identity of the user, biometrics can be incorporated into any number of situations where this security requirement exists. The sky really is the limit for biometrics use. Following are some examples of how biometrics are being utilized at this time.

A. Financial Transactions

Almost all financial institutions have researched using biometrics at one point or another. The benefits are obvious. One of the greatest advantages would be the ability to replace a PIN number with a secure biometric. This would greatly reduce the chance that an ATM card could be used maliciously. The implementation of a biometric with the use of checks and credit cards would also have a huge impact on identity theft, a growing problem of concern. Loyalty and rewards programs could be setup to require a biometric any time a transaction is processed. They could also be set up to control access to safety deposit boxes and vaults.

1. Access control

Biometrics can also be utilized any time that access control is a requirement. This could be general physical access to a building as well as access to a workstation, computer system or network. Theoretically a biometric could be used to delineate access control to the lowest levels such as access to a particular file or computer application. Building security systems, especially in areas where confidential or classified information needs to be stored. Such would be the case in many government buildings.

2. Identity verification

Again, at the simplest level, biometrics is about identity authentication. This opens up a wide area of suitable applications for the technology. Any time you are looking for a convenient, accurate and quick method of identifying or verifying an individual, a biometric solution could be a good choice. Some common uses throughout the world include such things as time card or attendance systems. Employees can be required to quickly check in and out of work with the scan of a finger or the eye. This helps keep an accurate record of hours worked and makes it impossible to forget to "punch" in. Public welfare programs utilize biometrics to make sure benefits are received, as well as used, by the correct individuals. Biometrics are used for patient management in hospitals and clinics to keep track of individuals for billing purposes as well as medical charts and to make sure that patients receive the correct medications.

3. Law enforcement

Although biometrics have been used by police agencies for some time on a limited basis fingerprinting, etc.) the tragedy of 9/11 helped bring to light the many hypothetical benefits of biometric systems to law enforcement areas. The ability to do such things as facial recognition scans to look for potential terrorists or criminals in airports or other high profile public places can be a great benefit to security personnel and systems. Unfortunately, in reality many of these systems have not been able to live up to the standards they claim to accomplish. False identifications (i.e. false rejections) occur frequently and slow down check in times, angering customers. However, as technologies progress these will be very viable uses. In addition, biometric systems are currently used with great success in such areas as immigration checks and individual movement control. They have been implemented to help move law enforcement criminal records into the digital age. Digital fingerprint scans have replaced the traditional ink system [3].

V. PROBLEMS AND ISSUES

The benefits of a biometric system are fairly obvious and straightforward. Since they are an intrinsic part of

the user, they do not require the user to remember a password or pin. At first glance, they are very secure. An impostor will not have much success randomly generating a fingerprint to gain access. But because they are an intrinsic part of the user, they pose some interesting problems that other systems do not have. Also, since most biometric systems are not completely isolated, they are exposed to the same risks that the rest of the network or other applications are. Following are some of the main problems and issues surrounding biometric systems.

A. User Acceptability

This was mentioned earlier under considerations but is important enough to be mentioned again. User acceptability may be the biggest issue facing biometrics for a number of reasons. First and foremost, users are concerned about their privacy. Many view the use of biometrics as an intrusion into their personal life. They are unsure how this information might be used in the future. Is it possible that the government could get a hold of such information and use it to keep track of what someone does without his or her consent? Will banks and retailers be able to sell such information much like e-mail addresses? It sounds like a conspiracy theory, but it really is possible. There is also the issue of being able to possibly gather medical information from some biometric templates. Scans of the iris and retina may possibly indicate drug use or even medical conditions and diseases as blood vessel patterns may change due to health related events. Does this violate HIPPA laws and statutes? It is most certainly not the purpose of any system to be detecting such things at this time, but what if the information falls into the wrong hands or is used improperly. Most people would not want their management or employer having this information without their consent. Finally, many users also fear that use of a biometric system may result in some harm to them. This may be as simple as fearing that the light shown into their eyes during a retinal scan could cause damage to their vision. This is not the case, but it is easy to see where this fear comes from. There is also the issue of possibly spreading contagious diseases through the use of scanners by many individuals. Many contagious diseases can be spread by simple contact so this is a possibility. With all of this being said, user acceptability has actually started to increase. Education of the user base has been the main reason for this. Users are beginning to understand the potentially devastating financial problems caused by such things as identity theft. And the tragedy of 9/11 has proven that there is a need for enhanced security which biometrics can help provide. A recent survey conducted by Privacy & American Business (P&AB) and funded by the US Bureau of Justice Statistics showed that many American consumers felt that it was appropriate for the private sector to require biometrics for certain transactions. This included such things as:

- Verifying the identity of a gun purchaser against a database of convicted felons (91% agreed)
- Verifying the identity of credit card purchasers (85%)
- Withdrawing funds form an ATM (78%)
- Accessing medical or financial records (77%)
- Conducting background checks (76%) (16)

1. Technical problems

System cost and accuracy are two of the biggest technical problems associated with biometrics. In most cases, new hardware and software will be required to implement a biometric solution. Depending on the type of system used, for example iris scanning, the cost may become prohibitive to install scanners at all desired locations. Fingerprint scanners, on the other hand, have become more affordable. As time goes on, most systems will become cheaper and more efficient. Accuracy may pose a problem if false acceptance and rejection rates are not acceptable for an organization. As mentioned earlier, these usually may be fine tuned, but in some instances biometrics may still not be able to offer the same false acceptance and rejection rates as a cryptographic token solution. As mentioned above, most biometric systems are part of a bigger security or technical infrastructure. They often rely heavily on other parts of that infrastructure to perform effectively. A good example would be the storage of templates. If these are stored on a central database or server you have another possible point of entry for an intruder. Typical precautions would need to be taken to make sure that your network was secure. Although an impostor may not be able to easily replicate a fingerprint, you need to remember that a fingerprint is translated by an algorithm into a mathematical code or string of bits. If an intruder is able to hack into the network and retrieve and decipher that code, they may be able to circumvent the system and use the digital fingerprint. The physical security of the biometric device needs to be considered as well. If an intruder had access to the wiring of a voice recognition system, it may be possible for them alter the wiring and play a recorded voice into the microphone. This may seem far-fetched, but it should be considered a possibility. An organization can evaluate how likely, or unlikely, such events are and plan accordingly.

2. Intrinsic problems

As mentioned previously, biometrics have the advantage that they are an inherent biological trait, and as such, cannot be lost. But this also poses an interesting dilemma at times. What can you do if your trait happens to be stolen? Fingerprints, for example, are unique but they are not secrets. We leave them everywhere with everything we touch. Voices may be

BIOINFO Security Informatics
Volume 1, Issue 1, 2011, pp-06-10
Available online at: http://www.bioinfo.in/contents.php?id=344

recorded and replayed at any time. Once your biometric is stolen, you have some serious issues. Reenrollment is not possible. Unlike resetting or changing your password you cannot simple reset your fingerprint. There is no simple or correct solution for this problem. The use of multifactor authentication can help insure the security of the system if a biometric is stolen but will not resolve the problem completely. Multifactor authentication is the use of two or more authentication techniques such as requiring a PIN or password to be used with a fingerprint scan. An impostor would not only need to steal the fingerprint, but would have to know the password as well. It is possible to combine as many authentication techniques as desired. For highly classified systems, for example, it would be possible to require a PIN, a smart card, a fingerprint scan and an iris scan. Of course most organizations, besides governmental agencies, would be unable to afford such a system. In any event, special consideration should be given to how a stolen biometric would be handled if it did occur.

VI. CONCLUSION

Biometric systems have made leaps and bounds in the last few years since their inception. While there are obvious advantages to these systems, there are also certain considerations that organizations need to think about when deciding whether or not to implement a biometric solution. They are not for everyone. Further testing is needed to make sure that they are as secure as they claim to be. But in the coming years, it will be hard to deny the advantages that they offer. In the future, biometrics will become a basic fundamental of everyday life.

REFERENCES

[1] http://www.ffiec.gov
[2] http://www.informit.com
[3] Ashbourn and Julian. “The Biometric Whitepaper.”, Oct.2003.