Comparison on Fingerprint Biometrics , Traditional PIN based Security and Iris Biometrics on the grounds of commercial and industrial use

Preeja Priji[1], Pranav J.I[2]
Department of Computer Science and Engineering
[1] Mohandas College of Engineering and Technology Trivandrum, Kerala ,India
[2] Heera College of Engineering and Technology Trivandrum, Kerala ,India

Abstract- *Authentication has been a major concern for centuries now. The modern technology and equipment relies greatly on safety and security. A number of security and authentication techniques are available today. The only problem is choosing which and where. Like everything in this world each technique has their own advantages and disadvantages. The choice of authentication varies with environment, sensitivity of information protected and number of users. In this paper three methods of authentication which are Fingerprint biometrics, password based security ,smartcard based security and Iris biometrics are compared on the basis of commercial and industrial usage.*

Keywords- fingerprint; PIN based security; Iris biometics; commercial authenthication ;industrial authenthication; comparison

I. INTRODUCTION

Since the time of Caesar authentication has been practiced. It is termed as Caesar cipher which is said to be the first type of encryption. Authentication involves identification of the individual(s) or restricting the usage of the protected element from anyone other than the intended individual(s). The protected element can be data, machines, safe, commutation, messages, equipment, weapons, etc. Different applications implement different authentications. The type of authentication technique used relies on three factors. Sensitivity of the secured element, environment and number of users. According to these criteria the techniques can be classified into commercial user friendly and industrial user friendly. In this paper. we are going to compare three major authentication techniques which are finger print recognition, iris biometrics and traditional personal identification number based techniques and find out which is more suitable for commercial use and industrial use on the basis of sensitivity, environment and number of users.[1]

The paper is divided into X chapters. The chapter II deals with a brief on fingerprint recognition and its applications, the chapter III deals with traditional password based security and its features. Chapter IV deals with smart card based security and Chapter V deals with brief on Iris biometrics and its uses.

Chapter VI deals with advantages and disadvantages of Fingerprint recognition in commercial and industrial security.

Chapter VII deals with advantages and disadvantages of Password Security in commercial and industrial use and chapter VIII deals with advantages and disadvantages in of Smartcard in the commercial and industrial application. Chapter IX deals with use of iris/retina recognition and Chapter X deals with verdict which shows which to use where. Chapter XI concludes the paper.

II. FINGERPRINT RECOGONITION TECHNIQUE

Fingerprint is unique for all human beings. Fingerprint analysis has been around for some time now. Before digital era Fingerprints were used in the field of forensics and document proofing. Fingerprint is God’s way of distinguishing humans. No two different people’s fingerprints are never exactly the same [2]. Fingerprint consists of different parts.

Figure 2.1 shows the main regions of a fingerprint. Fingerprint also differ in its type.

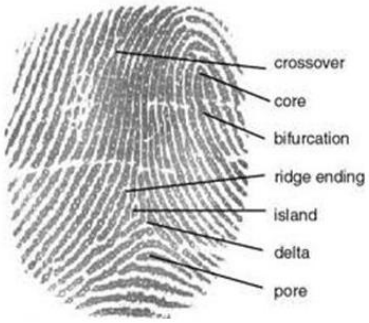

Figure 2.1 Regions of Fingerprint

Figure 2.2 shows given are the patterns of different fingerprints. The distinguishing of individuals is done by utilizing these differences.

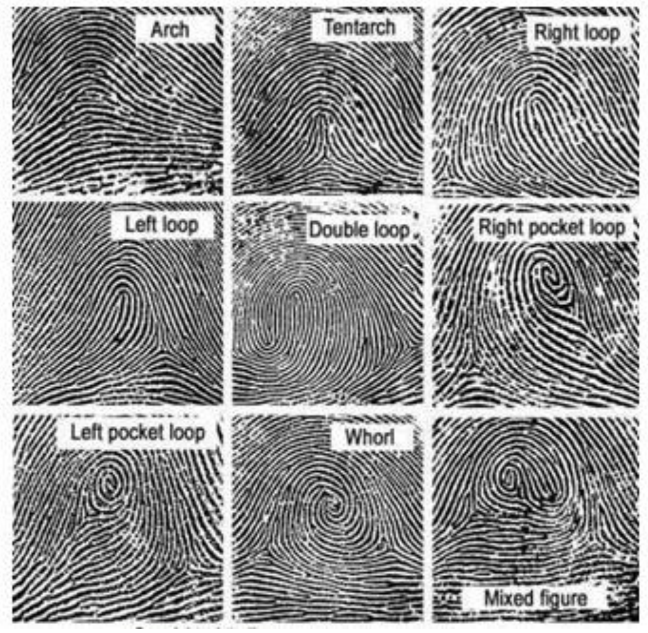

Figure 2.2 Types of Fingerprints

Using the fingerprint regions and types fingerprints can be easily distinguished. In modern age the fingerprint is digitally processed by computers with the help of digital image processing (DIP). Fingerprint recognition has become the main method of authentication. Its application ranges from locker safe to mobile phones. Most of the new commercial devices use finger print instead of password. (Examples are HP notebooks, iPhone, Samsung Galaxy S6).

In digital fingerprint processing not all of the features of fingerprint are used for recognition. Different methods use different regions for recognition. According to the methods of matching the fingerprint recognition can be classified into three.

1. Correlation Based
2. Minutiae Based
3. Pattern Based

The correlation based methods, relate fingerprint images in frequency and spatial domains to compute the similarity between them, and generates a typical correlation values of each fingerprint image and then compute their similarity. Always the fingerprints has to be aligned.

In minutia based approaches, minutiae (i.e. endings and bifurcations of fingerprint ridges) are extracted and matched to measure the similarity between fingerprints. These minutia-based is now used widely since it can detect fingerprints in different angle yet it cannot identify low quality fingerprints.

In Pattern based a previously stored template and a candidate fingerprint is compared on the grounds of type of fingerprint. This requires that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

III TRADTIONAL PASSWORD BASED AUTHENTHICATION TECHNIQUE

Password is the simplest and commonly used authentication technique in digital computer. Password is a sequence of characters that is memorized or written down in a secure document which can be used to access the secured element. Passwords are of different types. PIN, OTP, encryption code, etc.

A common password is usually easy to memorize strings of alphanumeric character, sometimes special character which is in the length of 4 to 16 characters. It is known only to the user. Often used in internet applications, email security or computer based security.

A PIN or personal identification number is a sequence of 4 to 8 digits which is used in facilities with number pad like ATM, Telephone DTMF services, etc.

An encryption code is usually a 16 to 20 character long alphanumeric string that is used for decrypting data. Usually used for product activation or military application.

The main problem of password is in long term. The user tends to forget after a long period of un usage. Also writing down may cause it to get stolen. More over passwords are more prone to be hacked by brute force attack.

IV. SMART CARD BASED SECURITY

Smart cards are physical cards that is tamper proof. A smart card contains a chip which contains some encrypted data. Smart cards are often used for digital wallet, secured military access, ATM etc.

Smartcard data are protected by encryption algorithm, still its prone to forging.

The advantage of smartcard is that a large size of information can be programmed and stored to a smart card.A smart card can be used to store many banking credentials, medical details, driver's licenses, loyalty points and so on. Multi-factor and proximity authentication is embedded to smart cards to increase the security.

Smart card provides more security . A Smart card is flexible and have many function. Like it can be used as a credit, debit or cash card. A PIN provided more security to smart card. If card detects any attempt of fraud it will be blocked for security.

Another advantage Smart cards can give user access to information without online connections. Encryption devices can encrypt and decrypt information to avoid unauthorized use. Smart card is flexible in providing secured access at different level. [2]

Other general benefits of smart cards are:

- Portability
- Increasing data storage capacity
- Reliability that is virtually unaffected by electrical and magnetic fields.

Smart cards are generally subjected to forgery and security breaches since the chip can be directly accessed. Also losing a smart card puts the user at risk of exposing his sensitive data.[3] So smart cards are not used without an OTP or PIN

V. IRIS/RETINA RECOGNITION.

Iris pattern recognition is an approach to reliable visual recognition of an individual. It uses unique patters of iris to recognize a person. Iris is actually a muscle that regulates the size of eyes for light to enter.[4] Iris recognition is relatively a new field. While iris recognition examines the iris, retina recognition use patterns of blood vessels that create retina.

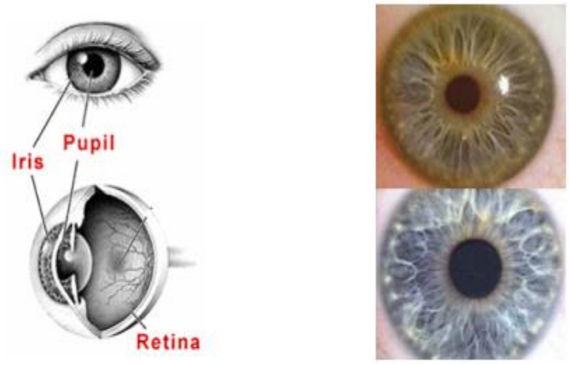

Figure 5.1 Iris and Pupil

VI. ADVANTAGES AND DISADVANTAGES OF FINGERPRINT RECOGNITION IN COMMERCIAL AND INDUSTRIAL SECURITY

Fingerprint recognition is a widely used techniques now a day both commercial and industrial authentication. Although it has many disadvantages too.

Fingerprint recognition is not idea for extreme cold conditions since there may be chances of misread of fingerprint. Also it is difficult to remove warm gloves each and every time the user has to login.

In commercial applications like mobile phone, computer login, etc. fingerprint is very useful and hassle free but industrially fingerprint recognition is not recommended since the workers may use gloves or will have foreign materials like oil and coals that may affect fingerprint image. [5]

The only disadvantage in commercial use known is losing of finger print by accident.

VII. ADVANTAGES AND DISADVANTAGES OF PASSWORD SECURITY IN COMMERCIAL AND INDUSTRIAL SECURITY

It can be said that password security is ideal for both Industrial and commercial uses, yet like everything else it also has its own pros and cons.

Commercially speaking a password is good if it is used daily, but if it is used rarely there is a risk of forgetting the password. Password cannot be written down since it voids the use of password. But the advantages are that it doesn't require any special hardware like fingerprint scanner.

Industrially speaking a password is perfect since there may be a chance of change of authorization frequently. So passwords can be changed and user has to be informed the new password. But if the protected element is highly sensitive a OTP is recommended.

VII. ADVANTAGES AND DISADVANTAGES OF SMARTCARD IN COMMERCIAL AND INDUSTRIAL SECURITY

Smart card is more intended for commercial user. It stores large amount of data that are sensitive. Yet a smart cart is not recommended for industrial user since the card grants unauthorized access to anyone who bears the card also there is a high chance of loosing and damaging the card in rough environment. [6],[7].

VIII. ADVANTAGES AND DISADVANTAGES OF IRIS/RETINA SCAN IN COMMERCIAL AND INDUSTRIAL SECURITY

Iris and Retina scan is used if the secured element is highly sensitive. There is a high risk in using retina scans for regular authentication. Long term scan may cause damage of the retina or iris. It is not commercially recommended since the hardware is expensive and also it is difficult to scan each and every time. Although it is perfect for highly secure military and industrial authentication. Commercially Retina and iris scan are not recommended due to its increased cost. [8],[9]

IX. FINAL VERDICT

Brief Comparison tables showing the pros and cons of various techniques are shown in the tables 9.1,9.2,9.3 and 9.4.

Password Security
Pros
Recommended for commercial daily use and Industrial use. Also recommended for One-time sensitive data security
Cons
Not Recommended for rare use since there may be a chance of forgetting. Also hacking is easier

Table 9.1 Pros and Cons of Password Security

Smart Card Security
Pros
Recommended for Commercial use
Cons
Chance of Forgery, damaging and loosing card is higher. So not recommended for industrial use

Table 9.2 Pros and Cons of Password Security

Iris/Retina Security
Pros
Recommended for military security and protection of highly secure data in industries
Cons
Not Recommended for daily use or commercial use.

Table 9.3 Pros and Cons of Password Security

Fingerprint Recognition
Pros
Recommended for Normal Commercial Conditions
Cons
Not Recommended for cold and Industrial Rough Conditions as gloves or dirty hands make detection impossible

Table 9.4 Pros and Cons of Password Security

X. CONCLUSION

In conclusion, each method has its own advantages and disadvantages. Fingerprint, password, smartcard and iris and retina authentication techniques were analyzed and a verdict is shown as tables. The tables conclude that of these analyses technique fingerprint is more useful in daily life.

REFERENCES

[1] Fingerprint Matching Using Correlation (In Frequency Domain) Kalyani Mali1 , Samayita BhattacharyaInternational Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2014.

[2] http://en.infosoc.gr/content/downloads/biomet.pdf.

[3] Anil, J., L. Hong, S. Pankanti, and R. Bolle. 1997. An Identity Authentication System Using Fingerprints, IBM T. J. Watson Research Center.

[4] Wasserman, Philip (2005-12-26). "Solid-State Fingerprint Scanners - A Survey of Technologies"

[5] How Iris Recognition Works John Daugman, PhD, OBE University of Cambridge, The Computer Laboratory, Cambridge CB2 3QG, U.K. www.CL.cam.ac.uk/users/jgd1000/

[6] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/iris-recognition.pdf

[7] https://en.wikipedia.org/wiki/Iris_recognition

[8] Retina identification based on the pattern of blood vessels using fuzzy logic Wafa Barkhoda, Fardin Akhlaqian , Mehran Deljavan Amiri and Mohammad Sadeq Nouroozzadeh

[9] Pin based authentication by Rob Singh. September 4 2015

[10] https://success.mocana.com/hc/en-us/articles/208483578-PIN-Based-Authentication