ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Smart Access Technique in Corporate Sector Using Biometric Aspect

Sathish.Y[1], Surabhi.S[2], Sanila.S[3]

Student, Department of CSE, Angel College of Engineering and Technology, Tirupur, India[1,2,3]

Abstract: Access control is vital to provide a safe and secure environment. The process of designing an access control system that meets your needs involves amalgamation of appropriate technology which facilitates management and existing construction environment. In Information Technology, biometrics is expertise in measuring and analyzing human body characteristics, such as fingerprint, irises etc., for authentication purposes. In many organizations Swiping or Scanning the ID cards are used for registered entry of the employee that can be misused by any person which is highly insecure. To attain high security, we proposed a new Apps "MOVE ON" which incorporates entry to an organization provided by using a combination of Biometrics and Bluetooth 4.0 technologies in mobility which is trustworthy. The entry can be successfully computed even at a distance of 60m. This Apps provides an authentication with a strong degree of confidence.

Keywords: Access Control, biometrics, MOVE ON Apps, authentication.

I. INTRODUCTION

Multiple factors of authentication, including biometrics, can increase the probability that a person presenting a card to a reader is the same person who was initially issued the card. Biometrics authenticates identity by measuring and verifying an individual's unique physical characteristics, such as fingerprints, hand and face geometry, or patterns found in the eye's iris.

Since these identifiers can't be borrowed or stolen, several trends are driving the adoption of physical and logical access control on smart phones and other mobile devices. "MOVE ON" Apps. is an easy to use *biometric time and attendance* and *access control system*. With an intuitive and user-friendly interface, it makes managing your employees and physical security easy to do.

This Application ensures that the most high value asset of the company, employee work time, is used effectively. It is ideal for businesses of any size. Small and medium-sized businesses will benefit from the efficiency, ease of installation and operation.

While large businesses and other enterprises can centrally manage attendance information from widely-dispersed offices and branches.

II. EXISTING SYSTEM

An identification system can help you run your growing business more efficiently. If you have an existing employee attendance and time system and a separate building access system, issuing your own customized employee ID cards with your own.

You can even keep detailed logs of who enters and exits your facility at what time. The existing system can be a Swipe cards and Scanning the ID cards.

These two techniques are most widely used in many Organizations and Educational Institutions.

Fig.1 Swipe Card System

Fig.2 Scanning the ID Card System

III. POSSIBLE DISADVANTAGES OF EXISTING SYSTEM

In both the existing system, there are similar disadvantages

A. Easily Lost

Swipe card is small and lightweight and can be easily lost if the person is irresponsible. swipe cards can have multiple uses and so the loss may be much more inconvenient. If you lose a card , you could be severely inconvenienced for a number of days BECAUSE it can be used as key to the office.

B. Security

A second disadvantage of the using swipe cards is their insecurity. However, they are not as secure as some in the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

general public would believe. This creates a false sense of security and someone might not be as diligent as protecting their card and the details it holds.

C. Possible Risk of Identify Theft

When used correctly for identification purposes, they make the jobs of law enforcement and healthcare professionals easier. However, for criminals seeking a new identity, they are like gold, based on the amount of information it can contain on an individual.

D. Multiple Users

In an office, one employee's swipe card can be used by the another person for their entry into the office, which is highly in-securable.

IV. PROPOSED SYSTEM

Secure entry system is mandatory in every organization. There are many ways in which it is being misused. Any of the employees in an organization can make use of the swipe card of another employee in the same organization, which is insecure. Our proposed system will overcome these grievances by the new application "MOVE ON".

Apps "MOVE ON"

If an employee wants to enter into his/her organization he can access the door while he is 60m apart by using Bluetooth 4.0. In an smart phone, this application can be initiated by giving the user ID and password. The password we are supposed to give is the finger print which is a biometric aspect. The sensor senses the password and sends an input to the preprocessor, the processor process this input and produces the output which is an input for the feature extractor. The feature extractor extracts the necessary features and the convert it into the templates with the help of template generator. These templates are send via., "Bluetooth4.0" to the matcher. These templates can be compared with the existing templates by using matcher.

Matches: It will send a welcoming note
"Welcome Mr. XXX"
"JUST MOVE ON"
If Not: Access Denied

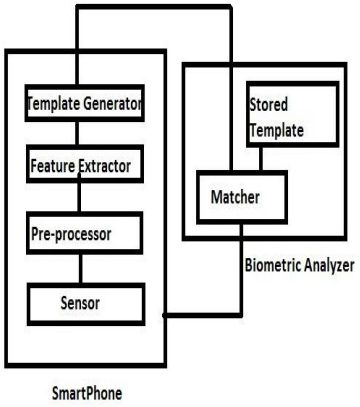

Fig.3 Block Diagram of MOVE ON Apps

The above block diagram designates the complete process of "MOVE ON" Apps.

V. ALGORITHM USED FOR FINGERPRINT IDENTIFICATION AND VERIFICATION

Fingerprints are the most used biometrics technique for personal identification. There are two main applications involving fingerprints: fingerprint verification and fingerprint identification. While the purpose of fingerprint verification is to verify the identity of a person, the goal of fingerprint identification is to establish the identity of a person. In the past three decades, automatic fingerprint verification is being more widely than other techniques of biometrics such as face identification and signature identification. Usually associated with criminal identification, now has become more popular in civilian applications, such as financial security or access control.

Many fingerprint identification methods have appeared in literature over the years [1, 5, 7]. The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae. In general, the two most prominent used features are ridge ending and ridge bifurcation (Fig. 1).More complex fingerprint features can be expressed as a combination of these two basic features. Minutiae matching essentially consist of finding the best alignment between the template (set of minutiae in the database) and a subset of minutiae in the input fingerprint, through a geometric transformation

A. Minutiae Extraction

Typically each detected minutiae m_i is described by four parameters:

$$m_i = (xi, y_i, \Theta_i, t_i)$$

Where,

$x_i y_i$- are co-ordinates of the minutiae point.

Θ_i- is minutiae direction typically obtained freom local ridge orientation.

t_i- is type of the minutiae point (ridge ending or ridge bifurcation).

The position of the minutiae point is at the tip of the ridge or the valley and the direction is computed to the x axis.

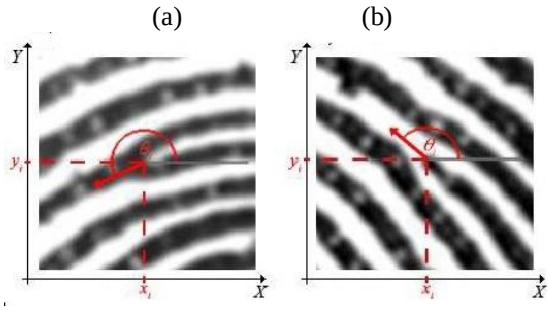

Fig.4 Parameters of minutiae
a)bifurcation and b) ridge ending type.

B. Matching Algorithm

For matching regular sized fingerprint images, a brute-force matching, which examines all the possible solutions, is not feasible since the number of possible solutions increases exponentially with the number of feature points on the prints. Transformation of input minutiae set, is the most important step, in order to maximize the value of similarity score.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Let *map* be transformation function that maps the minutia set from I to I' according to given geometrical transformation. Then, matching problem can be formulated as:

$S(T,I)=\max[¥_m \Sigma^n_{i=0}\ md(m_i, map_m(m_i'))]$
$md(m_i,m_j)=sd(m_i,m_j).dd(m_i,m_j)$

Where:
n- is the number of minutiae points in I input.
m- is the number of transformation equal set to the number of minutiae in T template set.

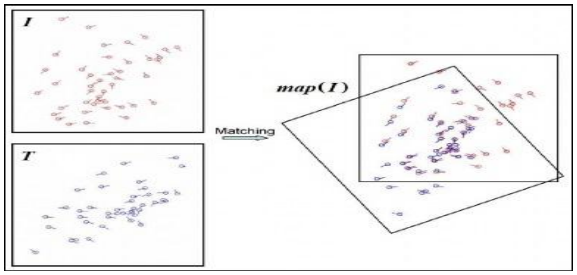

Fig.5 Minutiae based matching

VI. ADVANTAGES OF PROPOSED SYSTEM

A. *Increase security* - Provide a convenient and low-cost additional tier of security.

B. Reduce fraud by employing hard-to-forge technologies and materials. For e.g. minimize the opportunity for ID fraud, buddy punching.

C. Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.

D. Reduce password administration costs.

E. Replace hard-to-remember passwords which may be shared or observed.

F. Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access

G. Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!

H. Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.

I. Unequivocally link an individual to a transaction or event.

J. Less Time Consumption.

K. Uniqueness.

VII. CONCLUSION

Outmoded methods for identifying employees using cards and handwritten journals cannot ensure the proper level of effectiveness, after all physical media can easily be transferred, and one can forge a record in a journal. But fingerprints are unique for every person on earth. When using them to clock in and clock out, you can be confident that the recordkeeping is accurate. Definitely this new proposal of Application will make tremendous change in the authentication field and increase the security level.

REFERENCES

[1] Guide to Biometric Reference Systems and Performance Evaluation by Petrovska-Delacrétaz, Dijana; Chollet, Gérard; Dorizzi, Bernadette (Eds.)2009.
[2] Minutiae based fingerprint verification through multiple references and score normalization techniques by D.Simon-Zortia, J.Ortega-Garcia, M.Sanchez-Asenjo, J.Gonzalez-Rodriyaer.
[3] Biomerics Technology-Wikipedia free encyclopedia
[4] A Minute-based matching algorithm in finger print recognition System.