THE BIOMETRIC TIME AND ATTENDANCE SYSTEMS

A.PALANIAMMAL,
HEAD.DEPT.OF BCA,
SREE ARUMUGHAM ARTS AND ACIENCE COLLEGE,
TOLUDUR, TAMILNADU, INDIA.

Abstract:

The Biometric time and attendance systems use the fingerprints of employees to verify who is actually clocking in and clocking out of work each day. The system scans the finger of the employee, coordinates are determined and then the system maps the endpoints and intersections of the fingerprint.The every Organization, Businesses & Enterprise, managing and maintaining the workforce attendance is critical. Mantra biometric time and attendance system renders an accurate clock-in and clock-out time of personnel in any firm to achieve functional excellence. A biometric attendance system presents a cost-effective solution for controlling the employees' attendance and collecting the data.

Keywords: Biometric, ACTIVITY OF BIO SYSTEMS, TYPES OF BIOMETRIC.

1. INTRODUCTION

Our biometric time and attendance system not only enhances security amongst the workers but safeguards the working environment along with protecting a company's valuable data. Moreover, our attendance management system renders secured access control and authorization by tracking & maintaining the entries & exits of every employee.Mantra's unique time and attendance system presents a boundless attendance solution to businesses or enterprise, broadly applicable and accessible at diverse locations. Our biometric machine acknowledges an individual's physiological features like fingerprint, iris and face detection to register the attendance, thus eliminating any manipulation via proxy attendance at the workplace.

1.1 The state-of-the-art biometric attendance system renders

- Faultless payroll calculation with just one tap
- Biometric machine eliminates employee proxy
- Reduces the cost and manpower
- Offers real-time information
- Restricts unauthorized access
- Boost employee efficiency
- Managing leaves and holidays efficiently
- Gathers data from multiple locations at one place
- Complete reporting of the employee details

1.2 Biometric Time and Attendance System supports

Star Link Communication Pvt Ltd is one of the leading INDIAN manufacturer of *Biometric Attendance System* and *Access Control System*. We are restless in pursuit to implement latest technologies into our products and provide the excellent solution to our customers and users. In order to achieve this, we have set up a team of some highly qualified professionals,

- Cloud Based Platform to access the data anytime anywhere
- Report generation on employee attendance
- Live Attendance Tracking
- Centralized Data Collection of multiple locations
- Personnel-wise attendance tracking and monitoring
- Report Scheduling
- Time-Attendance Management for different shifts

1.3 Biometric Systems are Safe

Many people worry that biometric systems can be hacked or logged into by outside entities, such as law enforcement agencies. This is not the case. A biometric absence tracker is completely safe and secure. It can only be used, and data accessed, by the company that uses the system. These systems can typically only be used for tracking time and attendance and providing access to employees to certain areas of the building.There is no personal information used in the biometric system except for the employee's fingerprint and his or her employee ID number. The employee's social security number and other personal information, such as birthdate, are not used by the biometric system. This is what makes the system so secure. Even if it is hacked, which is highly unlikely, there is no personal information worth stealing.

1.4 Fingerprints are Deleted from the System

To make a biometric system even more secure, the system deletes fingerprints from the system. When a new employee is entered into the system, the software scans the fingerprint to create a group of coordinates. The fingerprint itself is

then deleted to protect the security and identity of the employee. The next time the employee uses the touchscreen on the biometric system to clock in or out, the coordinates on file are matched with the fingerprint on the screen to verify the employee's identity.

1.5 Restrict Employee and Non-employee Access

Another major benefit of using time & attendance systems is that they restrict employee and non-employee access to certain areas of your organization. For example, if a group of employees are not supposed to access a certain area of your building, their fingerprints will be flagged in the system so they cannot enter.This makes the building more secure from intruders or visitors who simply want to wander around the campus. They will not be able to access the restricted areas even if they attempt to use their fingerprint to gain access. Management will be able to assign and revoke access to individual employees using the software, much like using a keycard or keyfob.

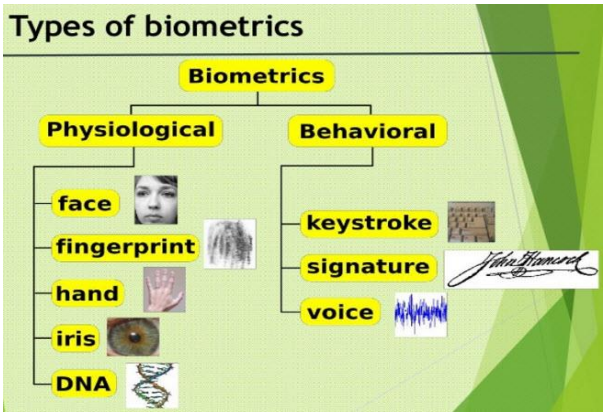
2. METHODOLOGIES:

Two Technology Types Used
Biometric absence management software uses two types of technology;

i) Image-based :
Image-based technology is when the software takes a picture of the fingerprint using a scanner to create the biometric template for each employee.

Capacitive:

ii) Capacitive technology is when the software uses electronic pulses on a touchscreen to feel the ridges on the fingerprints to make the template of endpoints and merge points



3.1 DNA Matching

The identification of an individual using the analysis of segments from DNA.

Chemical

3.2 Ear

The identification of an individual using the shape of the ear.

Visual

3.3 Eyes - Iris Recognition

The use of the features found in the iris to identify an individual.

Visual

3.4 Eyes - Retina Recognition

The use of patterns of veins in the back of the eye to accomplish recognition.

Visual

3.5 Face Recognition

The analysis of facial features or patterns for the authentication or recognition of an individuals identity. Most face recognition systems either use eigenfaces or local feature analysis.

Visual

3.6 Fingerprint Recognition

The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

Visual

3.7 Finger Geometry Recognition

The use of 3D geometry of the finger to determine identity.

Visual/Spatial

3.8 Gait

The use of an individuals walking style or gait to determine identity.

Behavioural

3.9 Hand Geometry Recognition

The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

Visual/Spatial

3.10 Odour

The use of an individuals odor to determine identity.

Olfactory

3.11 Typing Recognition

The use of the unique characteristics of a persons typing for establishing identity.

Behavioural

3.12 Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.

Vein

3.13 Voice - Speaker Identification

Identification is the task of determining an unknown speaker's identity. Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc. For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match(es). In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of

verification processes to determine a conclusive match.

Auditory

3.14 Voice - Speaker Verification/Authentication

The use of the voice as a method of determining the identity of a speaker for access control. If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation. For example, presenting a person's passport at border control is a verification process - the agent compares the person's face to the picture in the document.

Auditory

3.15 Signature Recognition

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilised in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

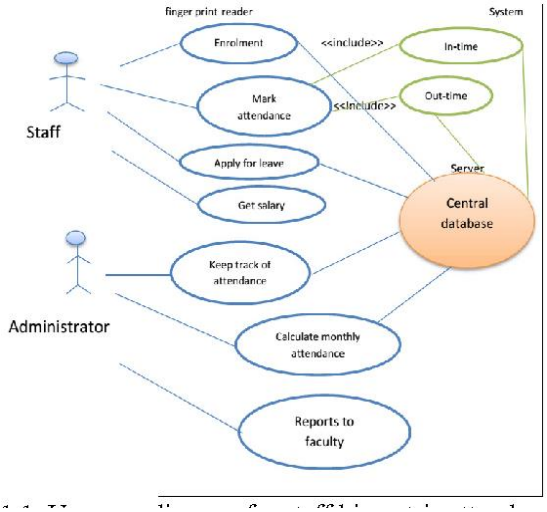
Visual/Behavioural

Note: There is a difference between speaker recognition (recognising who is speaking) and speech recognition (recognising what is being said). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.

Application Scenario

It is suitable for thousands of people's office areas, hotels, access gates, office buildings, schools, shopping malls, shops, communities, public services and management projects that require face access control.

3. PERFORMANCE ANALYSIS:



4. CONCLUSION:

The developed system is an embedded system that is part of a fingerprint recognition/authentication system based on minutiae points. ... Therefore, Fingerprint Recognition using Minutia Score Matching method was used for matching the minutia points before attendance is recorded.

REFERENCES:

1.Jain A.K . Bolle R. and Pankanti S. eds. Kluwer Academic, (1999), Biometrics: Personal Identification inNetworked Society,.

2.Zhang.D. Kluwer Academic (2000) Automated Biometrics: Technologies & Systems..

3.Jain A.K., Hong L. Pankanti S, and Bolle R., (1365-1388, 1997) "An Identity Authentication System Using Fingerprints," Proc. IEEE, vol. 85, no. 9, pp..

4.JainL.C., Halici U. Hayashi I, and Lee, eds S.B. CRC Press, (1999) intelligent Biometric Techniques in Fingerprint and Face Recognition.

5.Jain A.K., Ross A, and Pankanti S. (Mar. 1999) "A Prototype Hand Geometry-Based Verification System," Proc. Second Int'l Conf. Audio-and Video-Based Biometric Person Authentication, pp. 166-171,.

6.Shu W. and Zhang D., (Aug. 1998) "Automated Personal Identification by Palmprint," Optical Eng., vol. 37, no. 8, pp. 2359-2362,.

7.Zhang D. and Shu W. (1999) "Two Novel Characteristics in Palmprint Verification: Datum Point Invariance and Line Feature Matching," Pattern Recognition, vol. 32, no. 4, pp. 691-702.

8.Wildes R.P. (2000), "Iris Recognition: An Emerging Biometric Technology," Automated Biometrics: Technologies & Systems, pp. 1348-1363.246

9.M. Negin M. Chmielewski Jr T.A.., Salganicoff M., Camus T.A, U.M. Cahn von Seelen U.M, Venetianer P.L, and Zhang G.G., (Feb. 2000)"An Iris Biometric System for Public and Personal Use," Computer, vol. 33, no. 2, pp. 70-75.

10.Hill R., (1999) "Retina Identification," Biometrics: Personal Identification in Networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic, pp. 123-141.

11.Burge M. and Burger W., (1999) "Ear Biometrics," Biometrics: Personal Identification in Networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds., Kluwer Academic, pp. 273-286.

12.Campbell J.P. (2000), Kluwer Academic "Speaker Recognition: A Tutorial," Automated Biometrics: Technologies&Systems, pp. 437-1462.

13.Lynne Coventry, Antonella De Angeli, Graham JohnsonNew York, NY, USA (2003) Usability and

biometric verification at the ATM interface CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems pp. 153—160.

14.John D. Woodward, Jr. (2003), Searching the FBI's Civil Files: Public Safety v.Civil Liberty, in Biometrics 307, 324.

15.Yagiz Sutcu, Husrev Taha Sencar and Nasir Memon A (2005) Secure Biometric Authentication Scheme Based on Robust Hashing, MM-SEC'05.

16.Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, (Jun. 2003) "Personal Verification using Palmprint and Hand Geometry Biometric", In Proc. of 4th International Conference on Audio-and Video-based Biometric Person Authentication, Guildford, UK, pp. 668 -678.

17.Anderson, R.J. (2001). Security engineering: A guide to building dependable distributed systems. New York: John Wiley & Sons.

18."Banking on biometrics." (2004, April). Security, 41(4), 39.24719."Beyond doors: Securing records with finger flick." (2002). Security, 39(7), 57.

20.Bringing biometrics to e-commerce: James Uberti speaks out on new solutions." (2003, July 21). Electronic Commerce News, 1.

21.Chirillo, J. & Blaul, S. (2003). Implementing biometric security. Indianapolis, IN: Wiley.

22.E. Kukula, S. Elliott, "Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance", In Proc. of 35th Annual International Carnahan Conference on Security Technology, UK, Oct. 2001, pp. 83 –88.

23.Groves, E. & Aston, A. (2004, April 12). To make a quick I.D., play it by ear. Business Week, 92.

24.Hannah, G. (2005, January). Is it time to change your company's time and attendance system? IOMA's Payroll Manager's Report, 5(1), 5-7.