International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP25-30

Multimodal Biometrics Based Integrated Authentication and Security System

Mr.Rajput Nirajsing[1], Ms. Rajgire Mayuri,[2] Mr. Shaikh Moinuddin [3], Ms.Nakhawa Priyanka[4]

[1 2 3 4]*(Comp Dept &*DYPCOE,,Talegaon, *Pune University,India,)*

Abstract—Main goal of this project to increase acceptance rate and reduce failure rate (by reducing FAR and FRR). The basic functionality of single or simply biometric modal is to identify person. But we examine that single modal biometric gives low acceptance rate or low hit ratio. Multimodal biometric identification systems aim to accept two or more physical or behavioural traits to provide optimalFalse Acceptance Rate and False Rejection Rate, thus improving system accuracy. In this paper, a different multimodal biometric identification system based on RFID, fingerprint and voice recognition traits is proposed. This multimodal Biometric System integrated with payroll system and security system in order to provide up level security. In this system payroll system take output of multimodal biometric as an input, generate OTP in critical situations.

Keywords— Biometric **,** Fingerprint, Multimodal, RFID, security, voice recognition.

I. INTRODUCTION

Multimodal biometric: Person identification is also easily done with single or uni-modal biometric system. But there is high probability of higher false acceptance rate (FAR) and false rejection rate (FRR). This disadvantage will be covered with the help of Multimodal biometric system. Multimodal biometric system is fusion of two or more biometric parameter in order to improve acceptance rate and robustness of biometric system.

To increase hit ratio (acceptance rate) in identification of different person to get access to logical or and physical areas and to design high secure and more accuracy in person identification is always important issue, this issue can be solve using multimodal biometric system.

Multimodal: We can implement multimodal of biometric using different biometric feature that is Face, Fingerprints, Ear, Retina, Iris, RFID, Palm print, Voice, typing speed etc. Out of these parameter Fingerprint, voice and RFID [1] use in proposal project. By using these Biometric parameter the False Acceptance Rate (FAR) and False Reject Rate (FRR) are compressed. We use this multimodal biometric verification and identification for large scale company's security purpose and use this modal for identify person and his employment position in company. The main goal of the proposed system is to increase hit rate and reduce rate of failure.

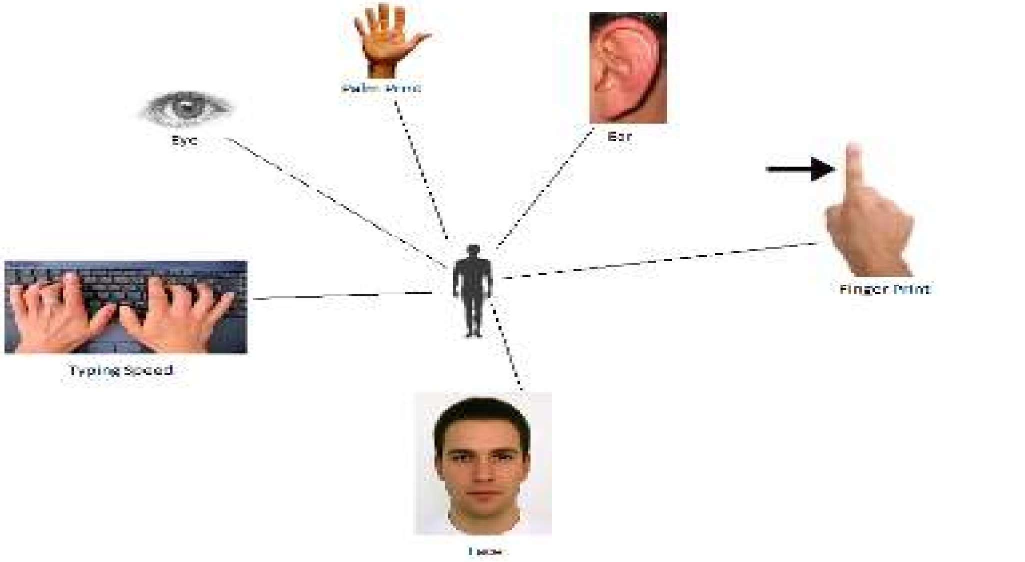

Fig 1. Human Biometric Parameters

TABLE 1. Comparison of different Biometric Parameter.

Characteristics	**Fingerprint**	**Hand Geometric**	**Iris**	**Voice**
Ease of use	High	High	Low	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Noise, cold whether
Cost	Medium	Medium	High	Medium
Accuracy	High	High	Very High	High
User Acceptance	Medium	Medium	Medium	High
Required security level	High	Medium	Very high	Medium

Working of current system:

In real world application most of the systems are based uni-modal biometric, they depend on one source of information for identification and authentication. Current payroll system work on uni-modal or single modal biometric, in this system there are high probability of higher FAR and FRR. For example suppose any organizations system work with only Fingerprint then, Employees IN-Time ,Out-Time, Overtime measured through that Single level Biometric system. This work efficiently but there are some limitation such as low level security, low acceptance rate, etc.

II. RELATED WORK

We use Multimodal Biometrics concept in access control and payroll system with higher security which is highly needed for different business, transport, government sectors, national boundaries, communication system etc.

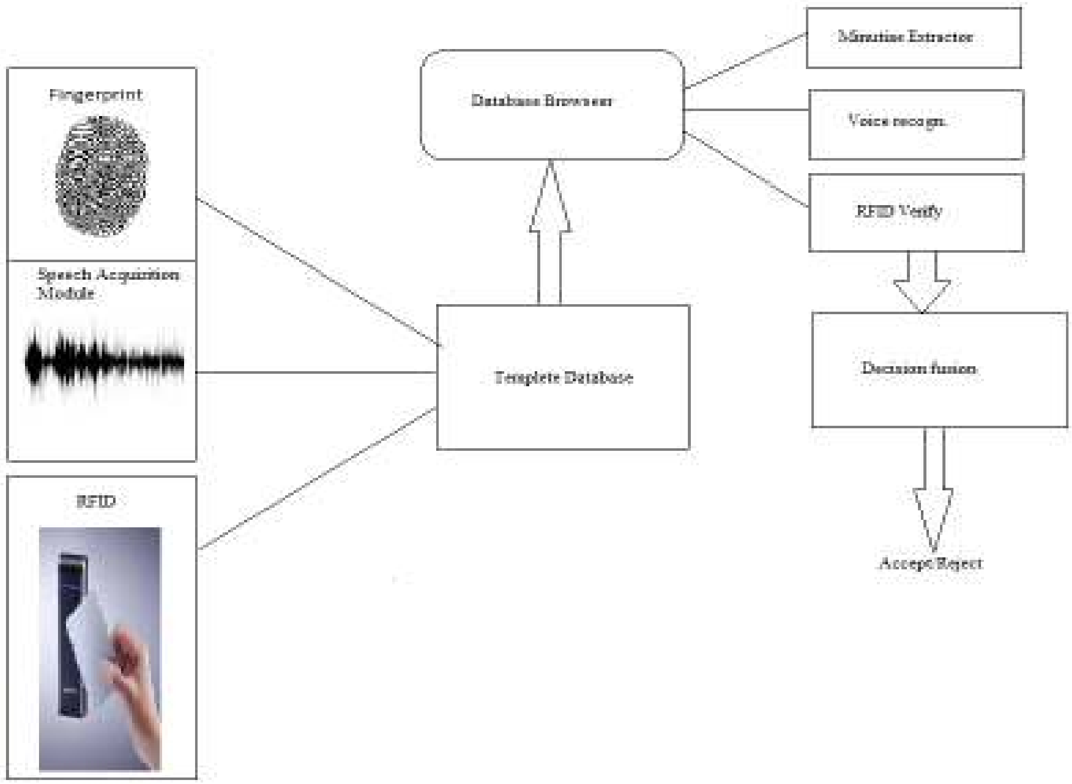

FIG 2. Identification and Verification using multimodal biometric

1. Role of Multimodal Biometrics in Payroll and Security:

We integrate Multimodal Biometrics with payroll system for identification and verification of employees in large organization and provide access control for physical and virtual areas of the organization and also provide privatization for employees of that organization using OTP.

In current system Uni-modal Biometric is used, in this case employee can easily place their finger on biometric scanner which read their finger print, but using single modal biometric employee faces many problems with high probability for example,

1. False acceptance: False acceptance means system falsely hit for unauthorized person therefore called as False Acceptance Rate (FAR) [2].
2. False Rejection Rate: False rejection means system may be falsely reject authorized person, therefore called as False Rejection Rate (FRR) [2].

Input to payroll:

i. Get employee ID through RFID:

RFID is generic method use to store data on small chips and communicate through radio transmission. RFID consist of three basic component, first is RFID tags in which antenna connected to a chip, second is RFID reader and third is database infrastructure which consist hardware as well as software.

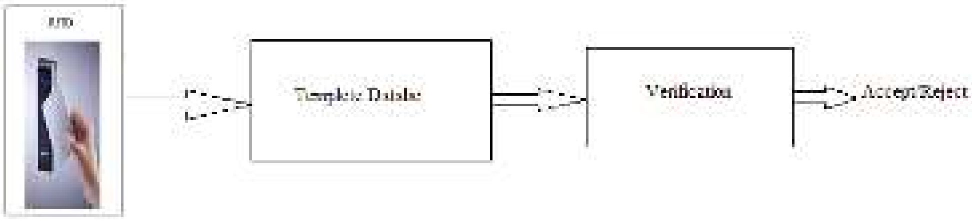

FIG. 3. Working of RFID.

After getting unique identity, System cross check in order to check whether the person is authorised user of this RFID card by verifying Biometric identity.

ii. Getting Biometric identification Details Through Multimodal biometrics System:

a. Calculation of biometric Parameter: Let β denotes to biometrics system, and let α 1, α 2,..,α n denote to template of users stored in template database of β and each user has only one template for each type of parameter in template database. So the template for ith user is αi = {α1, α2, α3}, three component for fingerprint, voice and RFID respectively. Let consider αC is identity claimed by user, so again for αC there are three component αC= {α1, α2, α3} for three different biometric parameter Fingerprint, voice and RFID. The resultant user claimed identity either in two categories first is T that indicates the claimed identity is true or accepted and another is F that indicate the claimed identity is false and rejected. The multimodal biometric checks αC to determine αC falls in which category of result either T or F.

b. Fingerprint Biometric: A Fingerprint is collection of ridges and repeated designs on the surface of fingertip. Each person has unique local ridges characteristics and spatial relation, so uniqueness can be easily determined. There are some important characteristics,

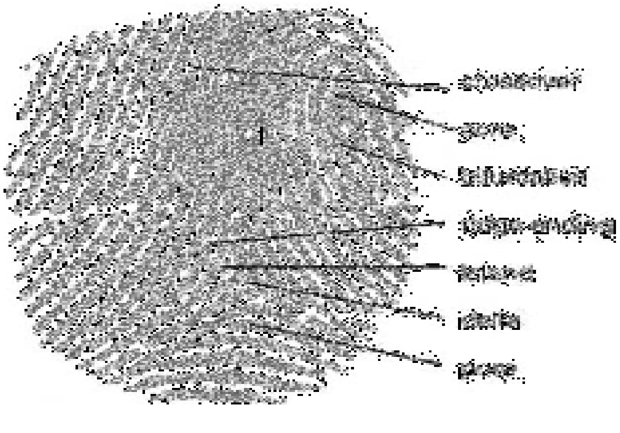

FIG.4 Sample of fingerprint (Thumb Impression).

i. Ridge ending
ii. Ridge bifurcation
iii. Core
iv. Delta

Core and delta extraction: Different-point detection is performed by checking the Poincare indexes associated with the fingerprint direction matrix. As pointed out before, the singularity points with a Poincare index identical to 180◦,

−180◦, 360◦ are associated with the core, delta, and double core, respectively. The process of fingerprint matching is divided into two parts namely [5],

i. Minutiae Extraction
ii. Minutiae matching

The extraction module extract minutiae from input print of finger and matching module match two minutiae patterns. There are several advantages of use of fingerprints such as ease of use, accuracy, device cost is also less as compare to Iris scanner, user acceptance rate is also high, etc.

Voice recognition:Voice biometric identification [3] is a process of identify and verify the person who is speaking. Voice biometric authenticate individual person through natural voice pattern. This technology is used for several of applications, like security access control for smart phone, for ATM, Automobile manufacturers

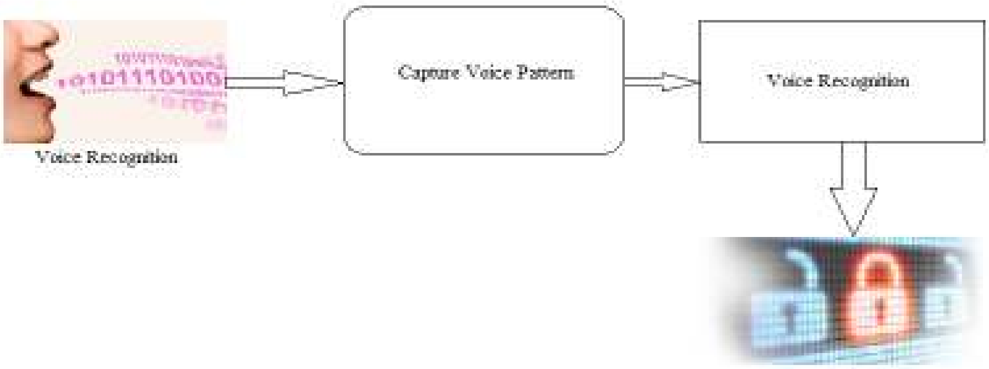

FIG. 5. Voice Pattern Matching

III PROPOSAL SYSTEM

A. How work proposal system:

Main aim of this project is to increase acceptance rate of biometric system and provide security by reducing false acceptance Rate (FAR) and false rejection Rate (FRR).

i. Authenticate employee using multimodal biometric:

This is first phase of this project; in this phase multimodal biometric system is used to authenticate person and granting access to physical as well as logical areas of the organization. Finger print biometric: First of all fingerprint biometric check for authenticate person, this phase gives two results, first is authenticate person successfully and grant access and second is authentication failed. If authentication done successfully system grant person to enter in organization and record his both the in time and out time and store in database. If fail to authenticate then person will claim for another biometric identity that is voice biometric, this part of biometric identification gives two results pass and fail. If authenticate successfully then next procedure same as above, and if fail he will claim to third biometric parameter which is RFID card. He needs to swap his RFID card to gain access in organization.

ii. If match not found in database then inform to security team:

Whenever unauthorized parson wants to access the system, system will automatically inform to security team. Suppose any person wants to enter in organization, first of all system get **fingerprint** of that parson, if fingerprint is not matched, then system will ask for another biometric that is **voice pattern,** if this biometric identification fails to identify that person, then again system will ask for **RFID card,** if RFID number will not match (All three biometric identification methods are fails) then system will automatically inform to the security team of the organization.

Note that if and only if all of the above biometric identification fails to identify employee, then system will automatically inform to security team of organization.

iii. Privilege distribution and information access system:

once employee has identified by biometric system then as per his privilege (CEO, MD, Project manager, etc) he will get access to the logical areas of the organization for example CEO has highest privilege than other employees, so CEO will get access to any physical or logical area and other employee will be restricted to certain physical or logical areas of the organization such as **Server rooms.**

iv. Access for guest or client visits:

In this phase, if any client or any guest wants to enter in organization then he needs to temporary access. This temporary access is done with temporary RFID card that's valid for certain time period, after time limit over, RFID number automatically discarded from database (also called as run time database). This card issued by authorized person of organization or need to get permission from authorized person to issue any temporary RFIDs.

v. OTP generate for verify authorized holder of RFID card:

Whenever any employee wants to get his personal details like salary detail, (employee ID, date of joining, department, designation, basic salary, overtime, dearness allowance, medical allowance, house rent allowance, provident fund, service tax, total earning, total deduction) then he needs to swap his RIFD card after swapping if match will found then system will automatically generate OTP [4] and send to the authorized user of that card. After that if user enters correct OTP then system gives detail his/her, otherwise system denied access.

OTP for up level security: If Employee wants to access any confidential information this system will generate OTP, user needs to enter OTP [4]. If and only if OTP matches user will get access to particular areas of the organization.OTP authenticator generate highly secure OTP and only authenticated person will gain access to the critical areas or data.

IV. CONCLUSION

Biometric system provides high level physical security. Today's most of the highly secure environments have used biometric system for access control; primary use of biometric system is in physical level security. By using biometric system we can easily control the access in critical areas such as server rooms of organization. There are some disadvantages of uni-modal biometric system, which is overcome by using multimodal biometric system. Multimodal biometrics: biometric system which takes input in the form of two or more biometric parameter is called as multimodal biometric. This paper highlights robustness of biometric and organizational need in terms of security.

V. REFFERENCES

[1] Angell, I., Kietzmann, J. (2006). "RFID And The End Of Cash" (PDF). Communications Of The ACM49 (12): 90–96. Doi:10.1145/1183236.1183237. Retrieved 9 November 2013.

[2] Martin, A. F. Et Al., "The DET Curve In Assessment Of Detection Task Performance", Proc. Eurospeech '97, Rhodes, Greece, September 1997, Vol. 4, Pp. 1899–1903.

[3] Elisabeth Zetterholm (2003), Voice Imitation. A Phonetic Study Of Perceptual Illusions And Acoustic Success, PhD Thesis, Lund University.

[4] Nohl, Karsten; Chris Paget (2009-12-27). "GSM: SRSLY". 26th Chaos Communication Congress (26C3): Retrieved 2009-12-30.