ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

IoT based Biometric Access Control System

Divil Jain [1], Dr. P.S. Ramkumar[2], Dr. K.V.S.S.S.S Sairam[3]

M.Tech Student, Department of Electronics and Communication, NMAMIT, Nitte, Udupi District, Karnataka, India[1]

Director, Applied Cognition Systems Pvt. Ltd., Bangalore, Karnataka, India [2]

Professor, Department of Electronics and Communication, NMAMIT, Nitte, Udupi District, Karnataka, India [3]

ABSTRACT: In this paper, a Biometric Access control system based on IoT is designed and implemented. These systems can be used for security of an environment so that only the authorized persons are allowed to pass or also for attendance measuring purposes. Biometric authentication is the best among security systems because it's unique and personal. These systems are comprised of biometrics such as fingerprint, iris, etc. Fingerprint based biometric system is a good combination of low cost and high accuracy. Evaluation of person's authentication is done by updating time, attendance and all related information to a Web server.

KEYWORDS: Fingerprint, IoT, Wi-Fi, Biometrics

I. INTRODUCTION

Human beings are gifted with some eccentric and irreconcilable characteristics. This feature among us can be applied intelligently to ensure security while consuming less manpower. Biometric authentication is considered to be the identity verification of an individual using either a biological feature which possesses physiological characteristic like a fingerprint or a behavioural characteristic like a signature [1]. As human fingerprint is stable over time and unique it can most certainly be used in all applications pertaining to security or attendance over other biometrics.

According to Sharifah et al. [2], system robustness towards its operating environment, security of biometric data within the system, concerns over biometric system testing and reporting and assurance of interoperability are the main challenges ahead of designing a Biometric access control system. The accuracy of these biometric systems is determined by two factors which are false acceptance rate (FAR) and false rejection rate (FRR). FAR means the rate at which the biometric measurements from two different individuals is mistaken to be from the same individual whereas mistaking two biometric measurements from the same individual to be from two different individuals signifies FRR [3]. In Zhang et al. [4] fingerprint based student attendance system using GSM was developed. Here a GPRS based system was used to store fingerprint data along with student details. Administrators could interact with the incoming data from the device through a central server. In Maio et al. [5] implementation of a wireless network for class attendance system using facial recognition and GSM is discussed and that system consists of a camera that captures the images of the classroom and sends it to the image enhancement module. The attendance is exported to the database server. Here ZigBee network is used for communication between classroom and authenticated authorities. According to Mahalinga et al. [6] biometric attendance management system using Wi-Fi was developed in which the system scanned the fingerprints placed on the sensor and compared them against those stored in the database successfully.

Internet has already proliferated the whole world and also has the luxury of being a standardized architecture, so by adopting these internet technologies and extending it in appliance control inside homes we can suddenly get the full advantage of everything that has been developed over 30 years in the field of internet. The Internet of Things (IoT) is a system of interrelated beings that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Because of the volume of internet and IoT, the prices become cheap and affordable with time and therefore it's wiser to design things based on IoT than any other propriety design. IoT devices are built in such a way as to make them look very simple and mundane and hence will be

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

simple plug and play modules which will be easier to deploy, scale, adopt, teach and learn. IoT can be enabled using various technologies such as RFID and near-field communication (NFC), Optical tags and quick response codes, Bluetooth low energy, Low energy wireless IP networks, Wi-Fi, ZigBee, Z-Wave, LTE-Advanced, etc. The proposed system uses Wi-Fi Technology as IoT enabling technology as it's now becoming a standardized technology for connecting devices with one another, its low cost of deployment, expandability, etc. The main purpose of this paper is to illustrate Biometric Access Control System for time and attendance management using a R305 Fingerprint sensor, Silicon Labs C8051F380 as core MCU and ESP8266 12E as Wi-Fi communication module.
The paper is organized as follows. In Section II, proposed system's workflow, dataflow and control flow are described. In Section III System Architecture is explained. Section IV comprises of Tests and Results related to the proposed system and paper is concluded in section IV.

II. METHODOLOGY

Work flow of the proposed system is described in Figure 1. After the system starts, user needs to give command by pressing respective buttons connected to the microcontroller, corresponding operation is performed by the Microcontroller and Fingerprint scanner. Upon the unsuccessful completion of that operation user is alerted and the system goes back to receive command and if the operation is successful the corresponding results are displayed and the necessary information (user data, date, time etc.) is posted to the webserver through ESP8266 and Wi-Fi router over the internet.

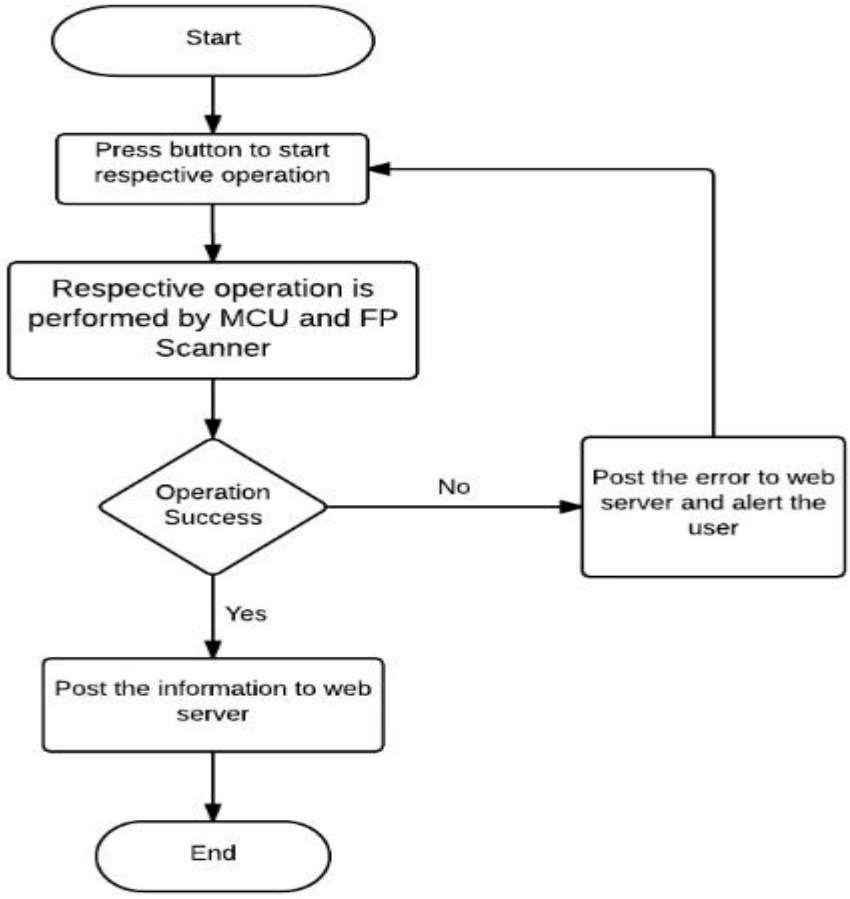

Figure 1: Flow chart of the proposed system

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

In the process of implementing the system, various steps including knowledge gathering, circuit planning and coding were done. In this attendance system initially all the participating users need to enroll themselves in the system. Enrollment or registration comprises of fingerprint capture, character file generation, template file generation, template number generation and storing the template file in device FLASH memory and then uploads the registered user's character file to MCU which then sends it to Web server through ESP8266 Wi-Fi module and Wi-Fi router over internet. Here care should be taken to avoid duplicate entries and in order to do that, we need to match the new fingerprint with the stored fingerprint templates present in FLASH. Once the users have enrolled themselves then fingerprint matching operation can be done on a daily basis/as or when required, in order for their attendance measurement. In this measurement process user's fingerprint is captured and is matched with all the registered users. Then system returns with the users registered name and stores the date, time of measurement in centralized webserver for further maintenance. The false acceptance rate of the system is less than 0.1% and false rejection rate of the system is less than 0.3 %. So the administrator who's in the webserver end will have access to all the necessary information of the users. Steps involved in registration process are explained in Figure 2.

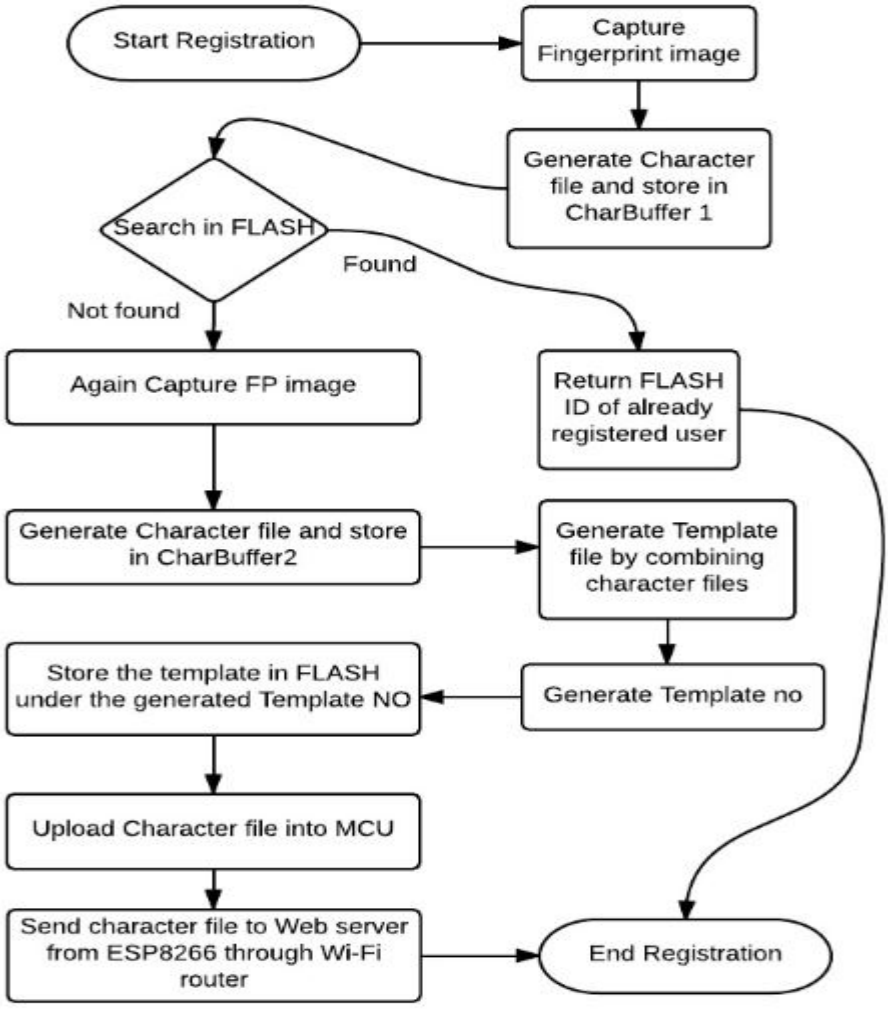

Figure 2: Flow chart for user Registration

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

III. SYSTEM ARCHITECTURE

Block diagram helps us understand the interrelationships and functions of a system. The interflowing elements of the system are as shown in Figure 3.

- **Fingerprint scanner** - R305 Fingerprint scanner is used here to capture and process the fingerprint image.
- **C8051F380 Microcontroller** - Silicon Labs C8051F380 acts as a core MCU which performs all input/output operations.
- **ESP8266 Wi-Fi module**- ESP8266 12 E Wi-Fi module acts as a communication module between C8051F380 and web server.
- **Wi-Fi Router-** Its used to send incoming data from ESP to web and vice versa.
- **Web server** - Used to store the attendance related information.
- **Power Supply system-** Provides power supply as per the requirements.

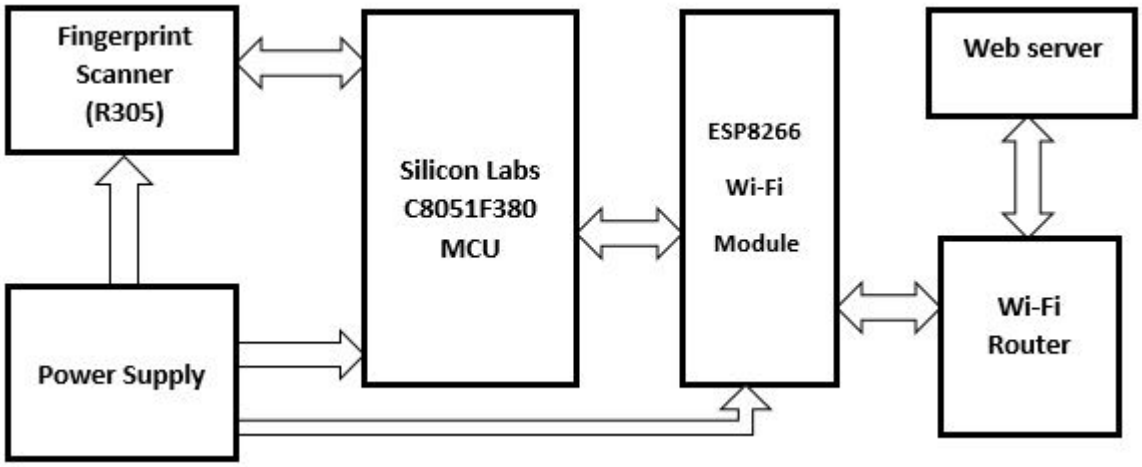

Figure 3: Block Diagram of the proposed system

Fingerprint sensor used here is R305 sensor which can store up to 256 fingerprints. This is suitable for home or any small environment. But for a larger environment such as school/industry we need to store more fingerprints. So for this purpose we need a microcontroller to export fingerprint character files from scanner to web server and as there is IoT involved we need a Wi-Fi communication module. We choose Silicon Labs C8051F380 as a microcontroller and ESP8266 as a communication module. Here fingerprint image acquisition and fingerprint image processing commands are given by C8051F380 to the sensor using UART interface through serial communication. C8051F380 communicates with ESP8266 also using UART interface. ESP8266 and Web server communicates via a Wi-Fi router. R305 needs 3.6V, whereas C8051F380 and ESP8266 need 3.3V each for proper functioning.

IV. TESTS AND RESULTS

All sections of the system were tested. After looking at the tested results it can be understood that the system is effective and also is highly responsive. There was no false identification of users. The users who were identified were automatically enrolled for attendance. Locally fingerprint acquiring and processing operations took place within 2 seconds. But 2 seconds of delay was observed for the information to reach Web server. During the testing period internet speed through which the router communicated with the web was 2 Mbps.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 9, May 2016

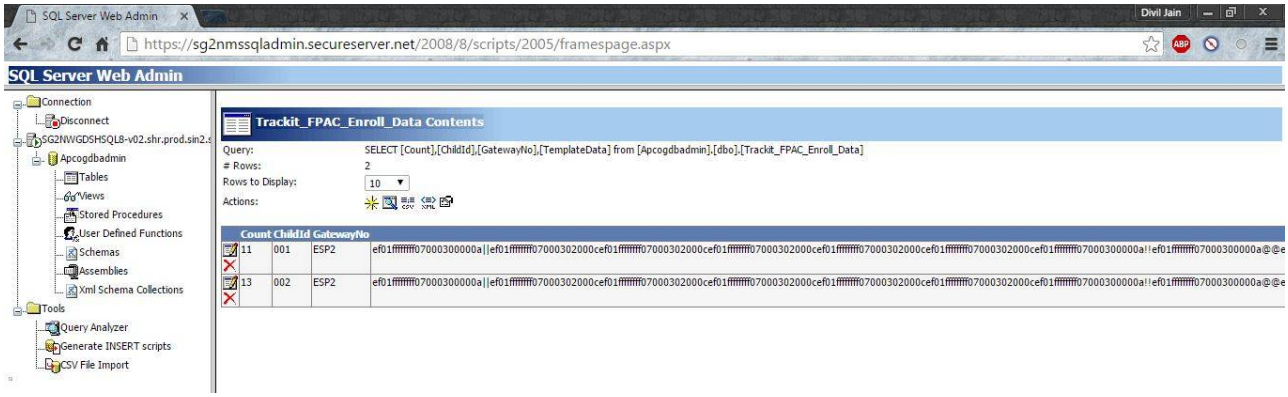

Figure 4: Results uploaded in the web server

In Figure 4 it can be seen that character files of users have been uploaded to the web server. Each character file is stored under a separate ID (ChildId). Count is the identity field set by database. Gateway number is the ID of the communicating ESP.

V. CONCLUSION

Because of the efficient design criteria, system was able to be designed using low cost. As the new wave IoT is coming in there are plenty of IoT enabled devices for home automation/industry automation and these devices can also be controlled remotely using biometric authentication over internet. New access control policies such as shift based, person based, group based etc. with corresponding criteria's can be setup in Web server if any change in access control is desired.

REFERENCES

[1] Prabhakar S., S. Pankanti and A.K. Jain., "Biometrics Recognition: Security and Privacy Concerns", IEEE Security & Privacy., Vol. 1, No 2, pp.33-42, 2003.
[2] Sharifah Mumtazah, Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan., "Technical issues and challenges of biometric applications as access control tools of information security", International Journal of Innovative Computing, Information and Control., Vol. 8, No 11, pp.7983-7999, 2012.
[3] J.L. Dugelay, J.C. Junqua, C. Kotropoulos and R. Kuhn., "Recent Advantages in Biometric Person Authentication", International Conference on Acoustics, Speech and Signal Processing.,Vol. 4, pp.4060-4063, 2002.
[4] Zhang Yongqiang and Liu Ji., "The design of wireless fingerprint attendance system", Proceedings of International Conference on Communication Technology., Vol.1, pp.1-4, 2006.
[5] D.Maio and D. Maltoni., "Direct gray-scale minutiae detection in fingerprints", IEEE transactions on pattern analysis and machine intelligence., Vol.19, No 1, pp.27-40, 1997.
[6] Mahalinga V.Mandi, Ashwini K.S, Chaitra H.S, Kavitha R and Kavitha U., "Biometric Based Attendance Management System Using Wi-Fi", International Journal of Emerging Technology and Research., Vol.1, No 5, pp.32-36, 2014.