**BIOMETRIC BASED ATTENDANCE SYSTEM USING IOT**

Jayachandra gupta.k1

School of Computer Science and Engineering (SCSE), VIT University, Chennai, India.

jayachandraguptanlr@gmail.com

***Abstract:*** The student biometric system facilitates the attendance automation. The most traditional way of taking attendance is by calling out their roll numbers during teaching hours which is time consuming. For overcoming these difficulties biometric attendance system is designed and implemented, this system improves the accuracy of attendance records and it will save the time of students as well as teachers. This paper provides a simple and portable approach for biometric based attendance system, based on Internet of Things (IOT), which captures the fingerprint data and is securely stores in cloud; this facilitates teachers to easily track the student’s presence.

**Keywords: Minutia Fingerprint, IoT, Fingerprint Scanner, Raspberry pi.**

1. **INTRODUCTION**

Biometric verification is thought to be the personality confirmation of an individual. As human unique finger impression is steady after some time and remarkable. And it can be utilized as a part of all applications relating to security. Attendance plays an important role in educational institutions. The classroom visit is most often used by teachers to collect student’s attendance. This process of collecting and managing student’s attendance will become cumbersome. Biometric systems have reached an advanced stage, allowing them to run on systems without disrupting portability [2]. With the recent development of many cloud-based computer and storage systems, data can be stored and secured safely. First, the fingerprints are the most dependable of biometric systems. This system includes fingerprint scanner, which is used to identify the student's identity. The Use of biometric scanners will safeguard the student’s data and store them safely in cloud in the form of a Google spreadsheet.

1. **LITERATURE REVIEW**

In the IoT based attendance system, the attendance is based on RFID and is integrated with NODEMCUESP8266 device. The attendance is given in the form of Google spreadsheets [3]. Whereas in Aadhar based biometric systems, the data is transmitted through the Gsm module wirelessly and data is taken from Aadhaar Central Identification Repository (CIDR). Sms alerts are sended to the parents in case of irregularity [7]. In the IoT based attendance system, they developed real-time attendance so that the student can track and maintain attendance through a mobile application [2]. In IOT based biometric access system, microcontroller is used along with Esp8266 to transmit the data and routers are used to transmit the captured data through the internet to the server, whereas server stores and compares the given template with stored template [1]. In design of wireless attendance system, spurious and networking problems are identified and solved. This system has the functions of fingerprint verifying, wireless communication and so on. Comparing with magnetic card, IC card and wired fingerprint attendance management systems, it solves the problem of replacer punching card and the trouble of laying the transmission lines [5].

1. **MINUTIAE FINGERPRINT**

Fingerprint recognition is the most widely used biometric identification method. Mostly automatic fingerprint recognition systems are based on local features called minutiae [9]. Therefore it is important to find these fingerprints correctly and to discard them correctly.

However, fingerprint images can cause skeletal and adulteration, skin variations and scarring with the scanning device, such as dirt, moisture, and unstable conditions. For this reason, some image enhancement techniques should be used before extracting thumbnails.

Fingerprint is a combination of ridges and valleys. Fingerprints are referred to as ridges, and the white space between them is called valleys [9].

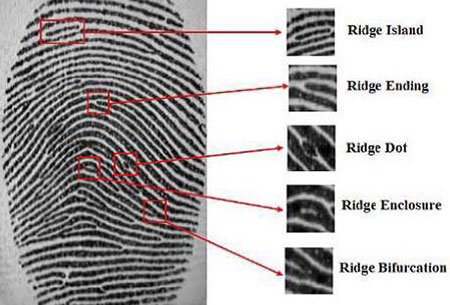


FIGURE 1: Minutiae Based Fingerprint Recognition

When compared to other fingerprints features, the minutia point features are different from the different types of orientation maps to distinguish between different types of fingerprints. Fingerprint representation using the minutiae feature when changing the point pattern by reducing the complex problem of fingerprint recognition [9].  
Since the original image is not rebuilt with accurate information, fingerprint-based fingerprint identification systems also help to maintain confidentiality and reduce the person's fingerprints. In contrast, the image resolution and global distortion details are more stable and stronger than other fingerprint schemes.

1. **RELATED WORK**

A popular technique known as histogram equalisation is used for fingerprint extraction. This technique is used for adjusting image contrast and intensities. This method is especially useful when a picture is represented by close contrast values ​​such as images in which background and foreground are bright at the same time, or both are dark at the same time [10].



FIGURE2: Histogram equalization applied to low contrast image

1. **SYSTEM OVERVIEW**
2. **Fingerprint scanner**

In the fingerprint scanner the image is captured and processed internally and stored in the memory. We are using R305device to capture the fingerprint image. This device captures fingerprint image and converts the image into minutiae points which is in the form of bits known as minutiae points.

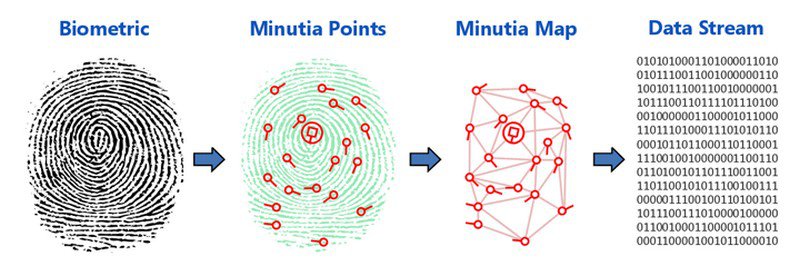


FIGURE3: Conversion of captured fingerprint into minutia points

1. **Internet of Things**

The Internet of Things (IoT) is a scene that allows the identification of objects or individuals. And it has ability to transmit data across the network without human interaction. The IOT is based on improved machine-to-machine (M2M) communication that includes wireless embedded sensors and actuators that help users to monitor and control devices remotely. This discovery has been made possible by incorporating electronics into daily physical objects, which enables seamless integration with existing infrastructure [5].

**C. Pushing Box API**

API (application programming interface) Continuous methods and protocol for accessing a web-based software application or web app. Pushing Box is a cloud service that provides cloud alerts based on API calls. The Pushing Box API makes it easy to launch a notification scenario by simply updating the DeviceID as argument. The Pushing Box API provides comprehensive functionality of Pushing Box service.

1. **IMPLEMENTATION**

The proposed system has a Raspberry pi which is connected to fingerprint scanner. The fingerprint scanner processes the user's fingerprint to verify the presence of participants. The inbuilt wifi module in the raspberry pi uploads data through a Push Box API to the Google spreadsheet. Rea API keys are generated in the cloud account so that these keys are embedded in the program to transmit the data with the help of internet provided.

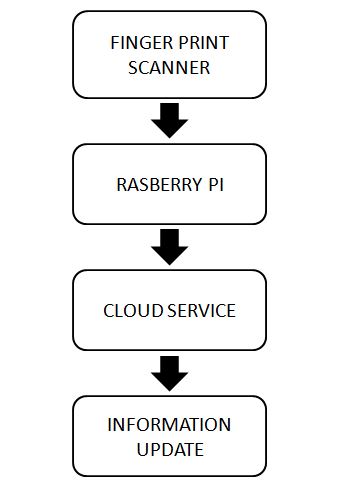


FIGURE4: Block diagram of implementation

1. **Fingerprint Scanner**

Fingerprint of the student is taken with fingerprint scanner. For each fingerprint an identification number is assigned. The identity number is stored in the memory of Finger print sensor (R305) as a template. For every time of attendance the actual image given is compared with the templates stored in the scanner. If the template is matched then the attendance is captured and the data is sent to the cloud through raspberry pi device else if the image is not matched it discards the image captured.

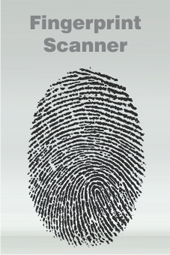
 

FIGURE 5: Fingerprint capturing

1. **Raspberry pi**

Raspberry pi is a device which is used to interface the components and it has inbuilt wifi connectivity. In the raspberry pi device the program is stored along with API keys to transmit the data to the cloud with the help of internet connection. Programs are processed in the device so that it is capable of transmitting data to the cloud.

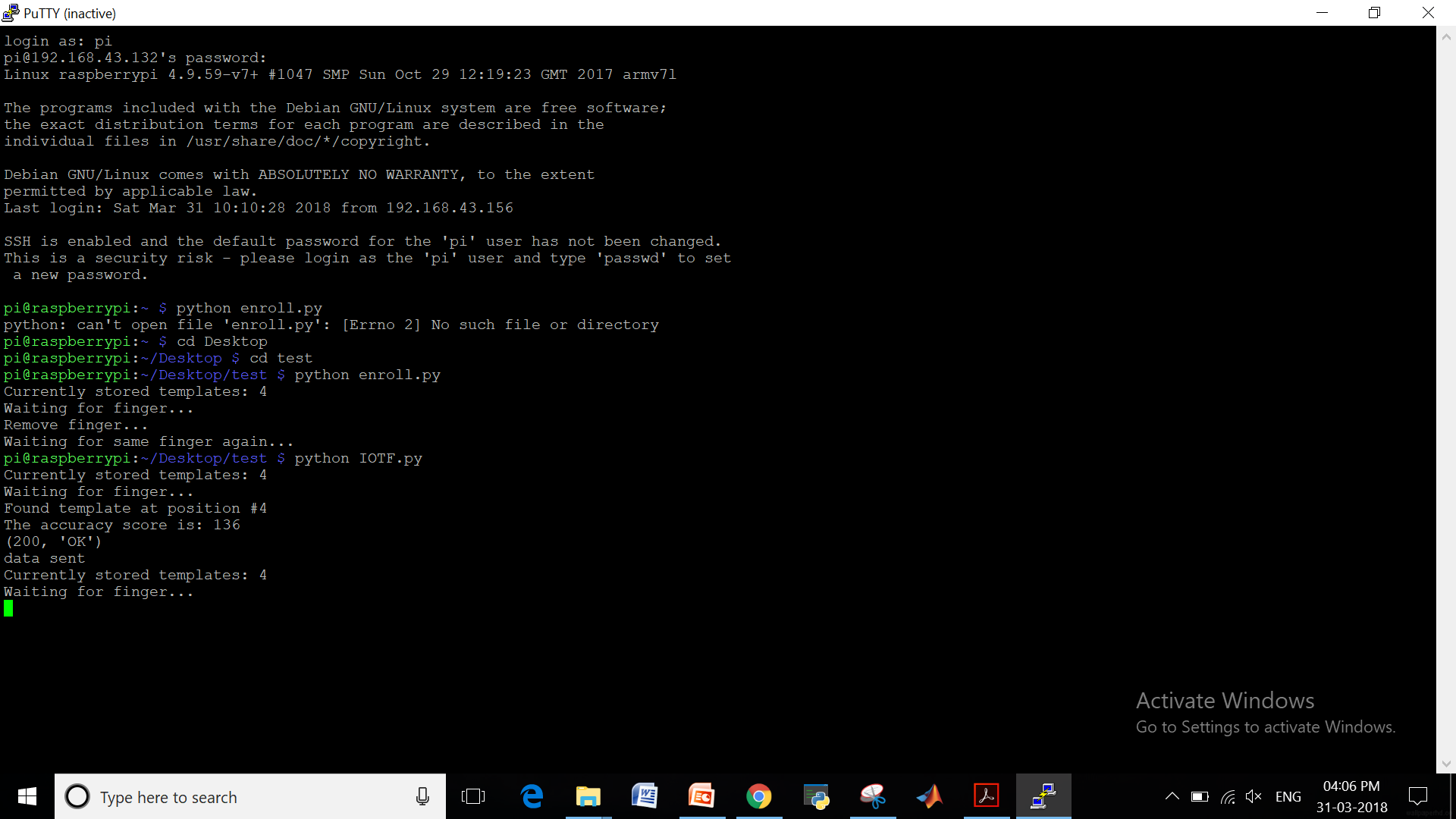


FIGURE 6: Sending user data to the cloud

1. **Cloud Service**

The data sent is received by the cloud service (thing speak) through APIs provided and the information is updated in the cloud. Administrator can easily import the data from the cloud in the form of Google spreadsheet by giving their login credentials.

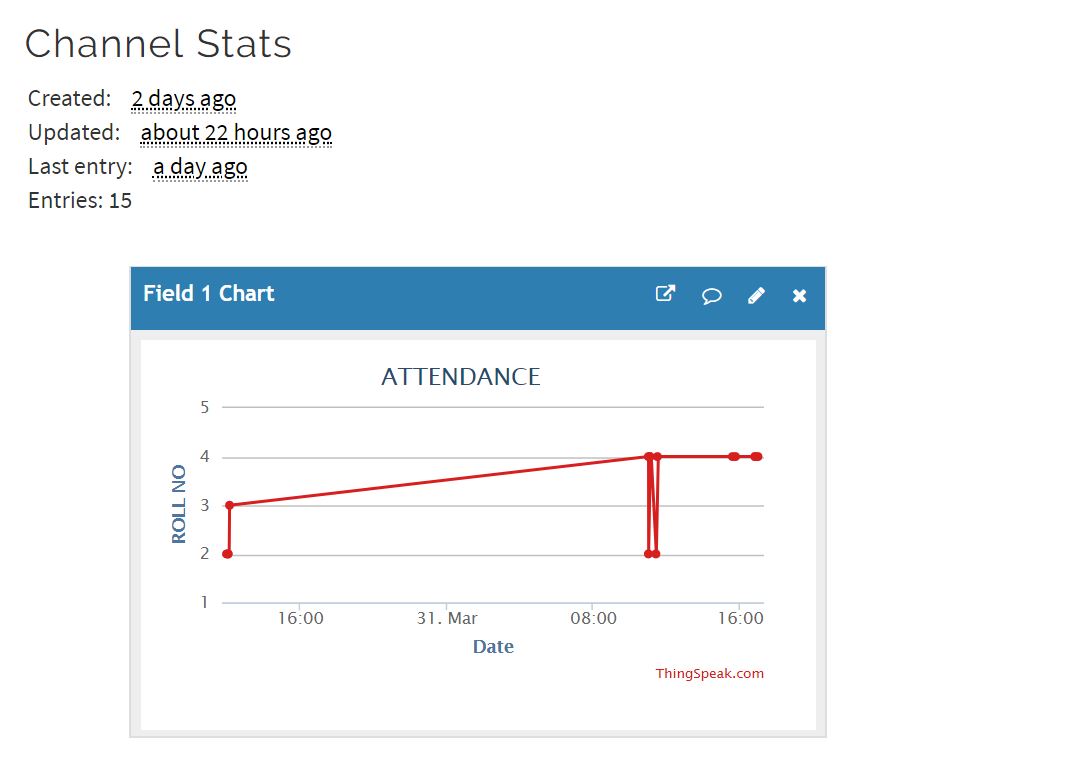


FIGURE 7: Received data on cloud

1. **Information update**

Information is updated in the cloud during transmission of data and the updated data can be imported easily in the form of Google spreadsheet [1].

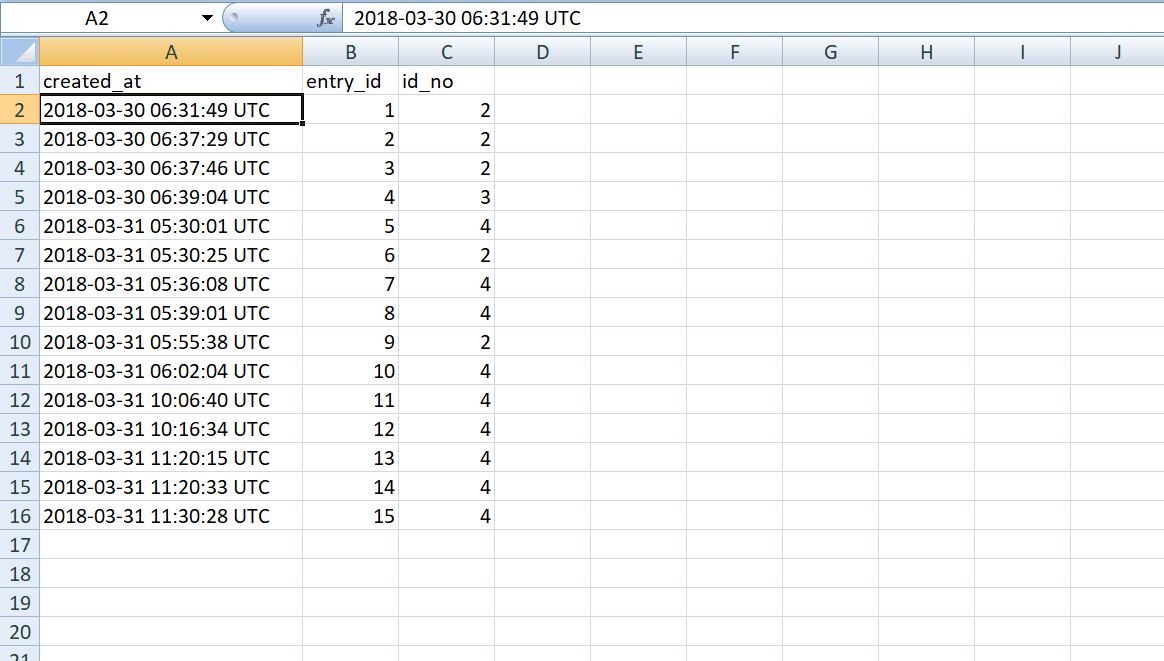


FIGURE 8: importing attendance data from cloud

1. **FUTURE SCOPE**

While there is a drastic development in the new technologies, many new methods can be used such as RFID technology, iris technology and we can adopt the new wireless technology like GPRS to eliminate the bad data transmission. We can also improve the system by wrapping it in a plastic cover. It's more compact and easy to use in the classroom. Configure the system to attend the lecture. When the student's existence is below a certain percentage, it will be better to automatically count the student attendance percentage. It will also suit for the corporate environment.

1. CONCLUSION

The traditional process of recording and maintaining of students' existence is very effective and time consuming. Biometric certification-based existence monitoring system has the ability to transmit the whole process. Internet of things (IoT) based portable biometric attendance system is valuable for educational institutions in this regard, which is very efficient and secure. Compared to traditional biometric attendance systems, the cost of the system is relatively low. By using cloud computing, all data is easily accessible and teachers can get data when needed. Use of fingerprint scanner ensures the reliability of the attendance list. The complexity of this system makes it easy to use and user friendly.

**REFERENCES**

[1] Divil Jain 1, Dr. P.S. Ramkumar2, Dr. K.V.S.S.S.S Sairam3,” IoT based Biometric Access Control System”,International Journal of Innovative Research in Science,Vol. 5, Special Issue 9, May 2016

[2] Devikar, Piyush, Ajit Krishnamoorthy, Aditya Bhanage, and Mohit Singh Chauhan. "IoT based biometric attendance system." *Int. J. Adv. Res. Comput. Commun* 5 (2016).

[3] Joshy, Annies, and M. J. Jalaja. "Design and implementation of an IoT based secure biometric authentication system." In *Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2017 IEEE International Conference on*, pp. 1-13. IEEE, 2017.

[4] Wang & Jingli, “The Design of Teaching Management System in Universities Based on Biometrics Identification and the Internet of Things Technology”, IEEE 10th International Conference on Computer Science & Education (ICCSE), Cambridge University, UK July 22-24, 2015,pp.

[5] Liu Ji. "The Design of Wireless Fingerprint Attendance System", 2006 International Conference on Communication Technology, November 2006.

[6] Sagar Wale, S.A. Patil, "Indigenous Development Of Automated Wireless FingerprintAttendanceSystem",INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 8, AUGUST 2014.

[7] Dhanalakshmi, Narra, Saketi Goutham Kumar, and Y. Padma Sai. "Aadhaar Based Biometric Attendance System Using Wireless Fingerprint Terminals."

 Advance Computing Conference *(IACC), 2017 IEEE 7th International*. IEEE, 2017.

[8] Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. (2012). Technical issues and challenges of biometric applications as access control tools of information security. International journal of innovative computing, information andcontrol, *8*(11), 7983-7999.

[9] <https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition>

[10] Barnouti, Nawaf Hazim. "Fingerprint recognition improvement using histogram equalization and compression methods." *Int. J. Eng. Res. Gener. Sci* 4.2 (2016): 685-692.