Design of a secure, performance efficient and low-cost Attendance Monitoring System using IoT

Goutham R[1], Arpana Debnath[2], Ashutosh Roy[3], Dr. Vidya Raj[4]

[1,2,3] BE in CSE, The National Institute of Engineering
[4]Professor, Dept. of CSE, The National Institute of Engineering, Karnataka, India

Abstract - *Cost reduction on the newer developed embedded systems has resulted in many IoT devices being developed for efficient computations at cheaper costs. These systems can be used for various purposes to reduce expenses and one such application would be to monitor attendance of students residing in hostels. This paper will present an Attendance Monitoring System we developed for the purpose mentioned above.*

Key Words: IoT, Biometric, Cloud, Raspberry Pi, Bcrypt, OTP

1. INTRODUCTION

In recent years, increase in number of open source software and hardware has led to an increase in the number of cost effective embedded systems. One of them being the Raspberry Pi running Linux which constitutes a small computer. Thus, embedding devices on these computers is a goal in order to make efficient, cost effective products.

Taking a look at the current attendance system in the college hostels, it is manual. From a list of names written down in a log book, the respective name has to be searched for, identified and then marked for that day. This increases the time taken and decreases efficiency. Also log books can be easily damaged and the data recorded in it can be lost. Moreover, this task does not require an intuitive quotient and can be computationally automated.

To curb these cons, an automated attendance system, that will be more efficient and less time consuming is proposed and is called, “Attendance Monitoring System”, referred to as AMS henceforth. A cost-effective fingerprint scanner will be integrated with the Raspberry Pi to develop the embedded system. Relevant information adhering to the corresponding scanned fingerprint’s user will be stored in a cloud after the enrol process. As and when required, it can be retrieved by both the embedded system for identification, and the hostel manager for monitoring and updating through the front-end client-side web application that would be provided. The manager can keep track of the attendance and make changes to it, such as remove graduated or moving out students, enroling new inmates and marking permitted leave for respective inmates from the database.

2. RELATED WORK

In [1] Jordi Sapes and Frnacesc Solsona discuss how cost reduction has led to an increase in embedding devices on Raspberry Pi systems to make commercially competitive products. They present a low-cost fingerprint recognition system embedded into a Raspberry Pi with Linux.

Trupti Rajendra Ingale has surveyed the various biometrics that can be integrated with an IoT device in [2]. Of these options [3] Dhvani Shah and Vinayak Bharadi have opted a fingerprint biometric integrated with a Raspberry Pi and connected it to the cloud to reduce cost of computational resources and take advantage of the cloud’s scalability and flexibility. They also used encryption algorithms like RSA and enhanced AES to encrypt the connection between the Pi and the cloud over the internet.

From the survey done, it was found that the Raspberry Pi made for an effective microprocessor for the purpose of biometrics, especially for fingerprint scanner. The added bonus of running an OS on it allows for complex computations to be performed on it. The GT511Cx series of fingerprint scanners/sensors gives a very good cost/performance ratio, thereby making it a good choice for the fingerprint scanner and also provides a performance comparison between the GT511C1R fingerprint scanner and the fingerprint scanners on an Android phone and an Iphone. It was evident from the comparison that the GT511Cx scanners was not the best option. However, at this time, the odds of every student being able to own a smartphone with a fingerprint scanner is very low. Hence the GT511Cx module was chosen over the smart phone fingerprint scanners. Insights gathered on the IoT and cloud technologies will help in the development and deployment of both, the server and client-side web applications. Please note that the ‘x’ in GT511Cx refers to the various versions (GT511C1, GT511C3, GT511C5) of the fingerprint scanner model that is compatible with the Attendance Monitoring System.

It should also be noted that the various systems developed in the references above have not developed a security system for the authentication of the manager except a login page that will protect it from human exploitation.

To solve this problem, we have developed an OTP authentication system. Also, they don’t provide any further analysis from the data collected other than the record of attendance marked.

3. ATTENDANCE MONITORING SYSTEM

Figure 1 represents the architecture of the attendance monitoring system built. Fingerprint scanner will be integrated with the Raspberry Pi. The scanner can store a certain amount fingerprint templates depending on the model used. These templates will be stored against an unique ID ranging from 0 to any limit the model provides. For identification purposes these templates have to be linked to its specific owner via an Unique Identification Number

(UIN). For this purpose, the templates stored in the scanner will be copied to an SQLite database where it is stored against the UIN.

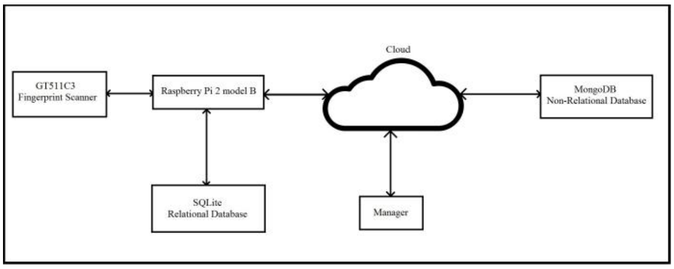

Figure -1: Architecture

A web interface is developed for use by the manager to view the recorded attendance data and perform any corrective actions in case of exceptions. The interface is hosted on a cloud, where connections between the raspberry pi and MongoDB database is made with the client. MongoDB will contain complete information of a student which will be used to perform analytical operations.

As shown in the high-level design represented in figure 2, the attendance monitoring system is a client-server model. The client module includes both the web interface and the scanner-client module. The server module contains the login-controller module and User-controller module which will provide operations that the manager can perform.

The manager has to login to the interface with credentials and must enter an OTP that would be generated in the cloud and sent to the manager's phone via SMS. This is done to provide a twofold security as this manager will have access to sensitive data. The interface provides the manager with five functionalities:

1. Login
2. Attendance monitoring
3. Enrol/Delete
4. Select and view analysed results
5. Handle exceptions

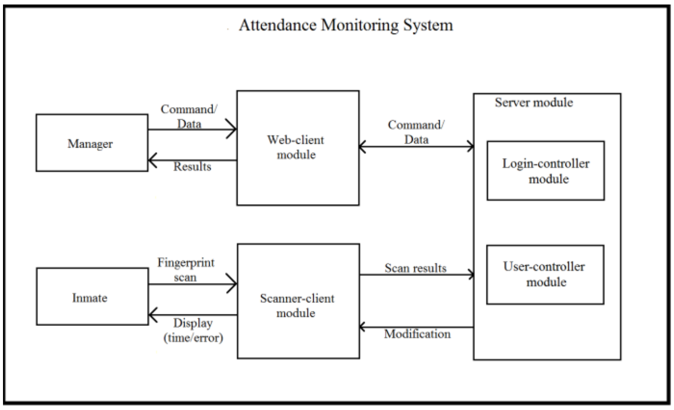

Figure -2: High-level design

Fingerprint templates stored during the enrolment process will be moved to the SQLite database where each template will be stored against its respective Unique Student Number (USN) or any other identification number. Identification is done when a student presses the fingerprint scanner. If identified, attendance is marked else is prompted to retry. Further failure would indicate non-registration and will prompt the student to enrol. The manager can delete records and templates of students that have evacuated by executing the delete operation.

Using the collected attendance data, analysis is made based on punctuality and frequency of the number of students marking their attendance to recognize patterns in their behaviour. A spike in either of the parameter can be related to an activity or circumstance that could have happened or is happening at the moment.

3.1 COST

Table 1 represents the survey done on three readily available processors for developing the AMS. It can be noted that Raspberry Pi is the most affordable one with immense community support. This helps in troubleshooting any problems encountered while developing and maintaining the system.

Hosting a website on a cloud is cheaper than hosting it on a dedicated server or virtual private network (VPN). Cloud hosting provides multiple servers, so even if one fails, the server is migrated to another one. But, VPN is restricted to its physical restrictions. One has to pay for only the services used from the cloud hosting. Whereas VPN's charge for a package. So, even if most services are not used, it is required to pay the full amount.

Table-1: Processors comparison

Raspberry Pi 2 model B	Beaglebone Black RevC	HummingBoard
1 Gb RAM	512Mb RAM	1 Gb RAM
26/40 GPIO pins	65/92 GPIO pins	26/36 GPIO pins
4 UBS ports Immense Community Support	1 USB port Meagre Community Support	2 USB port Meagre Community Support
Affordable (?3800)	Affordable (?4495)	Expensive (?11985)

3.2 PERFORMANCE

Authors in [1] have performed several tests to record the performance of the system they built based on response times and analysed the behaviour of each component.

Response times for each URI performed by the server varied but altogether it was satisfactory. Identify and Enrol operations had a higher probability of working at the first attempt than the second and third attempt. The margin in between the attempts is huge, therefore the probability of requiring a second or third attempt is very low. The effectiveness of the fingerprint scanner with an android mobile and iphone is also made. Without any movement the system fared well against the other two. CPU and Memory usage peaked at start-up and remained normal for the entirety of the system's processes. The client side of the system used a lot of CPU and memory for certain URI's.

3.3 SECURITY

Cryptographic hashing algorithms like SHA-6, SHA256 can be attacked using brute-force and hash collision. So, these problems have led to a new password scheme called *bcrypt* i.e. Blowfish Encryption Algorithm, which uses a 128-bit salt and encrypts a 192-bit magic value and makes use of expensive key setup in eksblowfish. This algorithm minimises the impact of the attacks by introducing a work factor which alters the expensiveness of the hash function. Therefore, the work factor can be increased to slow down the attacks made by faster computers.

In the proposed design, a two-fold security mechanism is used: password and OTP. Passwords will be encrypted with bcrypt and stored in the cloud.

One Time Password (OTP) is a randomly generated password that is used for authentication. It remains valid for a short duration of time, usually 30 to 500 seconds. The length of an OTP is 6 and the set size of all possible characters in the OTP is 62. So, the total number of possible sets of the pair of OTPs are 62^{12}. Out of that, 62^6 are equal OTP pairs. The probability of collision of two OTPs is:

$$62^6 / 62^{12} = 1 / 62^6 = 1 / 56800235584 = 1.7605561^{-11}$$

The probability of collision is very low and thus can be relied upon for a secure authentication system.

In the proposed design, algorithm for the OTP mechanism is as follows:

1. Generation of a random 6-digit number (OTP) and save it in the mongoDB mapped to user with timestamp.
2. This OTP is sent to the manager's mobile as a text message using twilio.
3. When the manager enters the OTP, check the current time with the timestamp to see validity
4. If valid, login is successful, otherwise ask for new OTP and repeat from step 1.

4. CONCLUSIONS

The proposed design has shown that the possibility of low cost embedded systems and its integration with cloud technology results in very efficient systems. This design can be extended for other use-cases like offices, libraries, etc. IoT is the future and accustoming to it is the right decision to be made as it solves a lot of problems for a day-to-day basis.

IOTA Tangle is a new cryptocurrency developed for the IoT ecosystem. It promotes micropayments by eliminating transaction fees as miners are not involved in the transactions. IOTA tokens can be used with this system, say for letting students to pay their fines using the cryptocurrency, machine to machine.

REFERENCES

[1] Jordi Sapes and Francesc Solsona, "Embedding a fingerprint scanner in a raspberry pi", Multidisciplinary Digital Publishing Institute, 2016.

[2] Trupti Rajendra Ingale, "A Review paper on biometrics implementation based on internet of things using raspberry pi", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 2, 2015.

[3] Dhvani Shah and Vinayak Bharadi, "IOT based biometrics implementation on raspberry pi", International Communication, Computing and Virtualization, 2016

[4] http://static.usenix.org/events/usenix99/provos/provos_html/node5.html