SAMS: An IoT Solution for Attendance Management in Universities

Gopinath Sittampalam
Department of Physical Science
Vavuniya Campus of the University of Jaffna
Vavuniya, Srilanka
s.gopi89@vau.jfn.ac.lk

Nagulan Ratnarajah
Department of Physical Science
Vavuniya Campus of the University of Jaffna
Vavuniya, Srilanka
rnagulan@univ.jfn.ac.lk

***Abstract*- An autonomous and effective platform for students' attendance management is presented in this paper by using most of the advanced technologies of the IoT (Internet of Things), such as mobility, wireless network, fingerprint sensor and cloud computing. The research aims at developing a smart device and a system to support attendance management in Universities. Smart Attendance Management System (SAMS) has been developed and implemented to record daily attendance of students in lecture halls and to provide web services for academic staff to manage and maintain attendance. The result reveals that the SAMS overcomes many of the limitations in the traditional methods of taking attendance and ensures the solutions are more accurate, secure, efficient and automatic.**

Keywords—IoT, fingerprint, attendance, portable, - autonomous, web service

I. INTRODUCTION

The emergence of the internet era changes the trend of learning. The availability of almost all information on the internet has caused students to be less motivated to attend lectures than ever before. However, direct participation in the lectures is always important for the success of their learning. Thus lecturers and administration of universities have to come up with different ways to ensure the healthy participation of students in lectures and practical sessions. In the Sri Lankan University system, each student must maintain attendance above 80 % for any course unit before writing their final examination. Student attendance is the main factor to assess the quality of learning process in Sri Lanka Qualifications Framework (SLQF), which is an important element of systems development in the higher education sector.

Most of the Universities are using traditional methods, where the printed attendance sheets used to collect students' signature. Students need to sign on attendance sheets in every lecture and practical session to ensure their participation. Lecturers take attendance of students manually for each lecture and practical session. This manual procedure has many limitations such as it increases the paperwork where the lecturer has to take care of the register and enter the attendance into the datasheet (or) database [1], and calculate and retrieve attendance for each student using software tools or a database management system. This procedure is a time-consuming activity, stressful and laborious and this valuable time would have been used for academic activities. Another disadvantage of this manual system is the accuracy level, which may decrease due to human errors. In addition to all these challenges, students can forge their absent friend's signature on attendance sheets. These fraud signatures make more difficulty in finding out absent students and initiate security problems. The researchers have tried to solve these problems and create various kinds of student attendance management systems for a decade. Many studies have been reported to improve and replace traditional paper-based attendance system using different technologies including RFID (Radio frequency identification) and Bluetooth [4-8]. RFID methods used to include an RFID tag (transporter) inside the student identity card. Students wave their identity card in front of the RFID readers to confirm their attendance in the lectures or practical sessions. These methods have some serious drawbacks such as there are no alternative ways to register a student attendance if a student forgets to bring his/her identity card and it is possible to make fault attendance using absentee's identity card. Implementing smart student identity cards and RFID based attendance system is also an expensive solution for the Sri Lankan Universities.

Biometric data allow a person to identify based on fingerprints, face, irises, retinal patterns, palm prints, voice, and gait, which are unique to the person. These techniques, which use physical data, are receiving attention as a personal authentication method that is more convenient than conventional methods such as a password or ID cards or signature [2]. Fingerprint data is more unique, reliable and easy to use among other biometric data. Fingerprint scanners are already been used in most of the workplace to manage employees' attendance and working hours. However, fingerprint scanners only will not solve the entire students' attendance problem as one student may have different subjects on different lecture halls, every lecture hall needs to use a fingerprint scanner, and students need to register their fingerprint on multiple fingerprint scanners. A student attendance data reside on multiple scanners, thus to collect attendance data, lecturers have to go through all fingerprint scanners in the lecture halls. IoT (Internet of Things) [3] technology can be used to resolve this problem in an effective way. The approach presented in this paper aims at producing an IoT derived SAMS (Smart Attendance Management System), which consist of PFS (Portable Fingerprint Scanner) and cloud-based centralized attendance management application. SAMS has been designed and implemented successfully and a lecturer or teacher can bring his/her PFS to take students' attendance and manage it smartly with the help of SAMS. SAMS successfully tested in ICT students of the department of physical science, Vavuniya campus of the University of Jaffna for a period of half a semester and a satisfactory result has been achieved.

II. SYSTEM ARCHITECTURE

Generally, University student attendance management systems have some essential functional and non-functional requirements such as user-friendly, reliability, mobility, less or no human errors, time and cost-effective, centralized management control, and customizable for the specific environment. IoT has the capability to provide the best solution to fulfil these important requirements. A good IoT

978-1-7281-1895-6/19/$31.00 ©2019 IEEE

system architecture should support heterogeneous devices, networks, data and application, to enable interoperability, scalability, and security [10]. There is numerous general architecture models proposed in the literature but there is no single model that suitable for attendance management in universities. Here we propose a layered architecture, which developed from various conceptual models such as reference model based on four layers [11], general IoT architecture with functional platforms [12] and the generic architecture of IoT web applications [13], as described below.

A. Layers of SAMS

A multilayer architecture designed to fulfil the requirements and provide multiple services to users of universities. The architecture consists of four layers Perceptual, Network, Middleware and Application layers, depicted in Fig. 1.

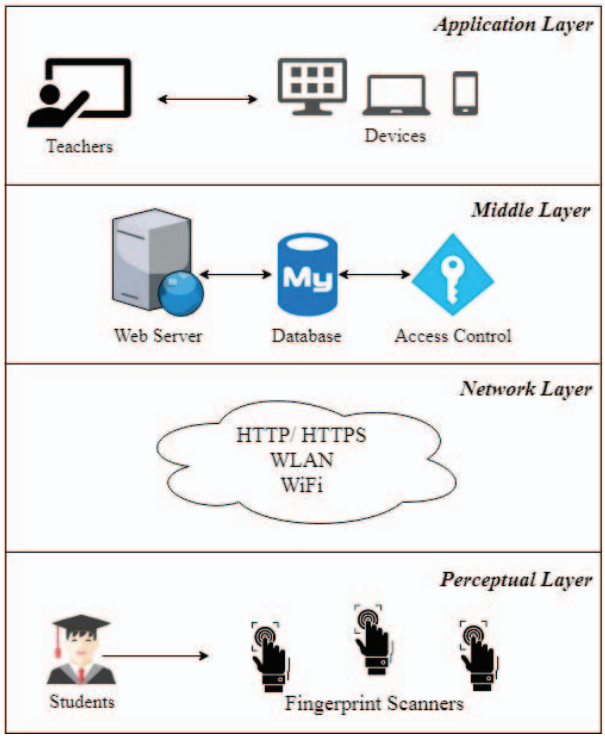


Fig 1. Architecture of SAMS

1) Perceptual Layer

This layer defines the environment, sensors, transmitters, actuators, and controllers. The environment is a lecture hall or laboratory and the sensors are fingerprint sensor and real-time clock. The fingerprint sensor is used to identify the students, based on their fingerprint. The real-time clock is used to find the time when the fingerprint was detected, as microcontroller does not contain an inbuilt real-time clock. A transmitter is employed to send the collected data from sensors to upper layers. An actuator (display unit) is used to show outputs and a controller integrates and issues control commands for sensors, transmitters, and actuators. Portable Fingerprint Scanner (PFS) is created as a device by combining all these elements.

2) Networking Layer

Wireless communication is most preferable for IoT. Several research papers point those different types of wireless networks possible in this layer such as WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) and WWAN (Wireless Wide Area Network) [10, 14]. WMAN and WWAN technologies are out of the scope of this research work. WPAN and WLAN protocols can be considered for this implementation. Bluetooth, ZigBee, and 6LoWPAN are categories of WPAN. Wi-Fi and Wi-Fi HaLow are categories of WLAN. WPAN technologies designed for short range applications and connecting wireless devices (Device to Device communications) [17]. On the other hand, Wi-Fi designed to connect a wireless device to the network including the internet for long range. The best wireless communication option for SAMS is Wi-Fi as it needs to work on an area about 100 meters and uses Device to internet communications [15] model. Star topology of Wi-Fi Sensor Network [16] used for SAMS which is depicted in Fig. 2. There are many application messaging protocols that havebeen suggested for the IoT system. Well known protocols are HTTP, COAP, MQTT and AMQP. The architecture of SAMS prefers request-reply interaction that means client issues the standard request and a server (middle layer) respond with appropriate data. HTTP selected as a messaging protocol for SAMS because it supports request/response Restful Web architecture [18, 19].

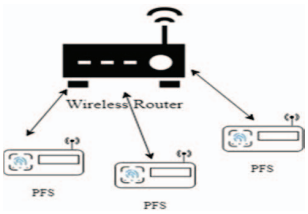


Fig 2. Topology diagram of SAMS

3) Middle Layer

The middle layer defines the OS and software, which is located between IoT devices and the application layer. This layer hosts server, programming language, and database to manage major operations such as aggregation, storage, filtering, validating, and decision making. The middle layer aggregates the data from lower layers and responses to the requests from the application layer. This layer provides efficient visualization to present smart services and user-friendly interface to the users. Authentication and access control mechanisms implemented in this layer to ensure security and privacy. Only authorized PFS allows to feed attendance data and the services are provided only to authorized users. Fig. 3 depicts the device authorization framework for SAMS.

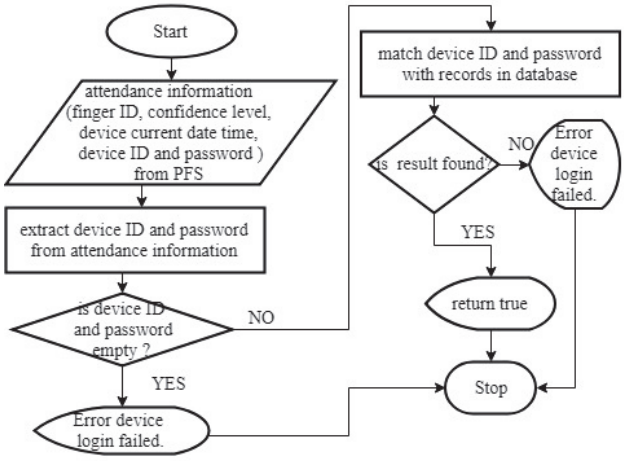


Fig 3. Flow chart of PFS authentication

4) Application Layer

The application layer provides different services to different clients. Admin, lecturer, and student are the clients, who benefit the services of SAMS. This layer focuses on the visualization of attendance data in a meaningful way to end users [10]. Two types of client applications are considered for client usage, which is a mobile application for smartphones and tablets and web application for desktop computers and laptops.

B. SAMS Services

- Registration service: This service handles by an admin user, who is responsible for adding lectures and students' account to SAMS. A username and password are given to all the lectures and students by admin to access their accounts. Especially students must register their three fingerprints with PFS.
- Data retrieval and visualization service: Each user can view full or partial attendance details based on their privileges. SAMS represent a summary of attendance in charts and all interface components built based on the user-centred design aspect.
- Access control service: Access control restricts the users and devices from accessing SAMS's recourses.
- Autonomous management: SAMS collect the attendance of many students but students belong to different courses and subjects. SAMS needs to make correct decisions to assign attendance to the particular subject for which attendance was taken by PFS. The decision is made by filtering and matching time and date attendance was taken, student's academic year, registration number and timetable.

III. System Implementation

A. PFS design and implementation

PFS is a smart object in SAMS, which responsible for functioning sensor, actuator and communicator. The integral parts of PFS are listed in Table I. Connection of integral parts is illustrated in Fig 4.

TABLE I. INTEGRAL PARTS OF PFS

No	Name of The Component
1	ESP8266 12E
2	WeMos D1
3	I2C Serial LCD 20X4
4	FPM10A Optical fingerprint sensor
5	PCF8563 RTC (real time clock)

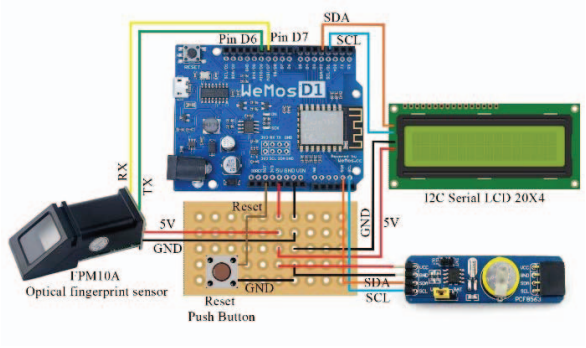
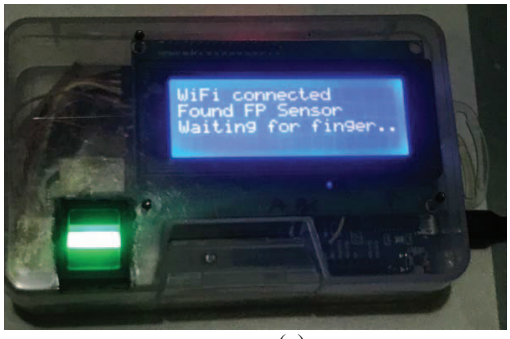


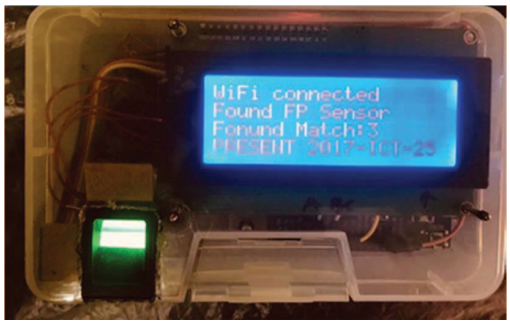
Fig 4. Circuit diagram of PFS

The component ESP8266 12E serves as a microcontroller and Wi-Fi adapter in PFS. As a Wi-Fi adapter, it connects with the Wi-Fi access point (Router) to enable internet connectivity to PFS. As the microcontroller, it stores and boots the program from Flash. ESP8266 12E is integrated with WeMos D1 development board. An optical fingerprint sensor is the main part of the PFS and the fingerprint processing includes two parts; fingerprint enrolment and fingerprint matching. When enrolling, the user needs to enter the finger two times and the system will process the two-time finger images to generate a template of the finger and store the template. In the matching process, the user enters the finger through the optical sensor and the system will generate a template of the finger and compare it with templates of the finger library. The system will return the matching result, success or failure. Optical fingerprint sensor communicates with the microcontroller using serial communication via TX connect with D6 (receiving pin), RX connect with D7 (transmitting pin). Semi-duplex asynchronous serial communication is used in this serial communication. And the baud rate is 115200bps. At power on, it takes about 500ms for initialization. LCD is used to display the status message of PFS to users such as Wi-Fi connectivity, fingerprint identification status, components loading messages and error messages. Fig.5(a) illustrates the PFS displays messages of the successful connection of Wi-Fi and sensors. A reset button is used to reload PFS. It will be useful when PFS lost Wi-Fi or fingerprint sensor unloaded. PCF8563 RTC module used as a watch in PFS, recognize the current time.



(a)

(b)



(c)

Fig 5. Messages of PFS. (a) Successful booting message, (b) error message, (c) fingerprint matched and registration number of a student.

The control program for PFS was written in C++ using the Arduino IDE. The control program is divided into five jobs connecting Wi-Fi, fingerprint identifying, display controlling, getting current time via RTC and sending and receiving data from the server. When PFS powered control program begins the process, first it loads all important libraries that needed for the fingerprint sensor, LCD module, Wi-Fi, Software serial and RTC. All code related to PFS initialization is written inside the setup method. The setup method will be executed only once. After the initialization program enters into a loop, which means that the code inside the loop will be executed until PFS switched off. PFS at running state, wait for a student's finger when it detected a fingerprint, will search the whole finger library for the matching finger. If matching found it returns a unique finger ID (an integer number) which has assigned in enrolment and confidence level (an integer number) of matching. If matching not found it returns -1. LCD module displays finger detection, fingerprint matched/ not matched and error information to users. Figure 5 (b) shows an error message when fingerprint matching not found. When matching found attendance data such as the finger ID, confidence level, current date time of PFS, device ID and password are sent to the webserver using an HTTP POST request. HTTP request contains information of destination hostname (domain name of the web server), URL (path to the request processing PHP file), length of the content (here attendance data), content type (here 'application/x-www-form-urlencoded') and content, which is depicted in Fig 6. Each PFS has an inbuilt unique device ID and password. Every time PFS sends an attendance data to SAMS. The SAMS extract device ID and password from attendance data and perform authentication. If an unauthorized person tries to inject an attendance data to the server, it will not allow without knowing the device ID and password. This process provides basic security for the system. ESP8266 12E does not have RTC like computers to remember date and time. PCF8563 RTC module provides date and time feature to PFS. With the help of RTC, PFS can detect what time attendance was made by a student. PFS makes a successful request to web service on the server. The web service returns a response message. The response message can be a successful present for a student which contains student registration information, which showed on Figure 5 (c) or error message such as device login failed or finger ID not found or error tries again. All these response messages display on an LCD module.

```
POST /fingerpost/postfinger.php  HTTP/1.1
Host: gopi89.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

fid=6&confi=110&DevDT=10:32:03 10-12-2018&Dname=PFS1037&Dpass=********

Connection:keep-alive
```

Fig 6. HTTP POST request generated by PFS

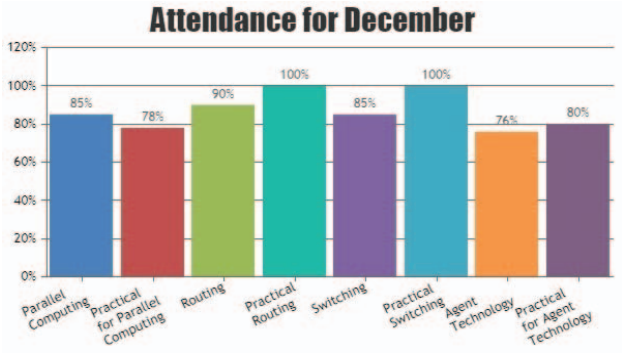
B. Implementation of Web services

Web services defined on middle and application layer. Middle layer implemented using Apache server, PHP (web programming language) and MySQL (relational database). PHP and MySQL enable the dynamic functionalities of SAMS. The database is employed to mainly store the attendance data captured by the PFS. The database is also used to store academic related data, such as timetable, lecture halls, lectures, and students information. SAMS can manipulate the recorded student attendance by querying the database for complex data retrieval. This includes automated operation, such as summarizing an individual student attendance by calculating the attendance percentage for a particular course unit [1].

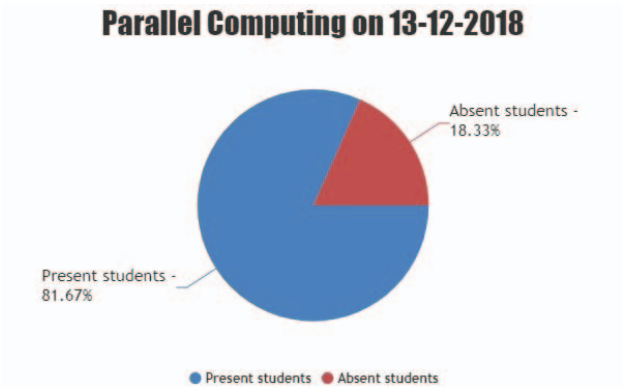
The major process of web server starts at a PFS sends a POST request (attendance data) to the server. The request processes by a PHP file (postfinger.php), which is located in the server. The PHP file contains the code to check attendance data before store it on the database. Each attendance data go through the various functions; ensure that the device ID, finger ID, the confidence level, the device current date time and password are not empty, verify received device ID and password details matched with existing details database, finds the student details of the finger ID, and finds the subject for which attendance was taken. Finding the subject has some difficulties because multiple subjects are conducted at the same time. To find a subject, a process first finds the academic year of the student from the subject code and search the time table based on device date and time. This search performed by selecting a column of timetable using the device current date and filtering subject code by matching device current time between the subject start and end time. Finally, the attendance information will be stored in the database. If special lectures or practical conducted on a time which was not allocated in timetable then the system may not find the subject. If the system could not find the subject automatically then the lecturer can assign attendance to the subject manually.

The application layer focused on visualization of services on client devices. User interfaces built by HTML, CSS, JavaScript, and Bootstrap framework, so interfaces are platform independent. The bootstrap framework mainly used to provide mobile-friendly graphical user interface (GUI). Visualization of attendance data includes different type of charts, which has done using CanvasJS framework. Fig.7 shows different screenshots of the chart from students and lecturers accounts. End users have different needs, according

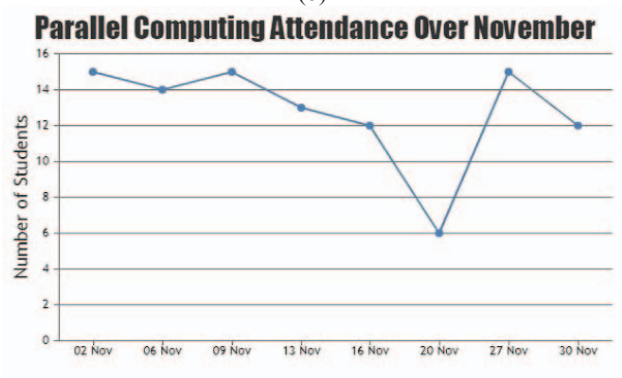
to their needs, SAMS can visualize the data in a meaning full way. For example, Fig 7 (a) represents the attendance data for a student, Fig 7(b) and Fig 7 (c) represent attendance data for a lecturer.



(a)



(b)



(c)

Fig 7. Different visual representation attendance data. (a) a bar chart displays one month summary of attendance for a student, (b) a pie chart displays students attendance for a subject of a day, (c) a line chart displays students attendance for a subject of a month.

IV. Cost Analysis

The cost of SAMS is economical than current commercially employed fingerprint attendance recorder systems. Table II depicts the cost analysis of the implemented system. Commercial fingerprint attendance recorders price vary from $60 to $185 and only provides record functionality that excludes analysing attendance recorders and smart interaction over the internet. SAMS only cost 22.95 US dollars and prove that it provides more functionality than current systems with minimal cost.

Table II. Cost analysis of Hardware implementation

Name of Component	Cost in USD
WeMos D1 with ESP8266 12E	$3.73
I2C Serial LCD 20X4	$4.78
FPM10A Optical fingerprint sensor	$7.65
PCF8563 RTC (real time clock)	$3.84
Push button, Prototype paper PCP and wires	$0.99
PFS Case	$1.96
Total	$22.95

V. Results And Disscussion

SAMS achieved two objectives here, collect students' attendance using PFS and provide automatic management of attendance data with less human intervention. SAMS is tested successfully in ICT students of the department of physical science, Vavuniya campus of the University of Jaffna for a period of half a semester. Summary of the statistically significant results of the questionnaires gathered from the students and lecturers is presented in Table III. The resultant table illustrates the comparison between traditional attendance system and the SAMS based on different parameters.

On the other side, several types of automatic attendance systems such as a barcode, magnetic stripe, Retina based, RFID and fingerprint based attendance system is suited for different needs and requirements. To differentiate between the most standard types of automatic attendance systems [9], Table IV discusses and describes the current generation of the common automated attendance systems concerning with different parameters. Traditional technology such as QR code, Barcode, Magnetic stripe and RFID imposed a long time for registration and error-prone, high resources (need transmitter and receiver), the possibility of forged identification, traditional manual management and individual personnel statistics for attendance management records, and it is not eco-friendly due to paper attendance cards and documentation. It is costly to produce students indent cards with RFID or Magnetic stripe. While the proposed system based on fingerprint and IoT technology can achieve several advantages such as user-friendliness, affordability, security, flexibility, fewer resources and data accuracy, automatic student identification without human interference, high security, indicating work status and generating the attendance report automatically, and it does not need to spend extra time and efforts.

Table III. Comparison Between The Attendance Systems.

Parameters	Traditional System	SAMS
Human effort	Need	No need
Attendance taking time	More than 15 minutes	Less than 5 minutes
Speed	Slow	High
Security	More vulnerable	Authenticated students only
Storage	papers, files	database
Management	Difficult	Easy
Accuracy	Low	High

Table IV. Features of Automated Attendance Systems.

Parameters	BC	MS	RS	RF	PS
Biometric	N	N	Y	N	Y
Resources	H	H	L	H	L
Accuracy	H	H	H	H	H
Purchasing cost	M	M	H	M	L
Speed	H	H	H	H	H
Security	L	L	H	L	H
Operating cost	H	H	L	H	L

Power consumption	L	L	H	L	L
Mobility of scanner	NP	NP	NP	NP	P

BC – Barcode, MS – Magnetic Stripe, RS – Retina Scanner, RF – RFID, PS – Proposed System, Y– Yes, N – No, H – High, M – Medium, L – Low, NP – Not Portable, P – Portable.

VI. Conclusion

The real innovation in IoT is not in the technology itself, but in its application in real-world situations. A new student attendance management system for Universities has been presented here. The system has some important functions such as fingerprint verifying, checking on attendances independently, and wireless communication. The performance of this system meets the needs of daily attendance management in universities and academic institutes. The system will be really beneficial for the students as well as the academic staff of the respective universities and institutes as with the advancement of this technology they can utilize their lectures in thebest way. Users are directed at what step to take next by providing them with timely information displayed on PFS. The system purchasing and operational costs are less compared with other attendance management systems. Physical size and weight of PFS is less and easy to carry. The PFS just need 5-volt direct current to work. So it can be powered by a battery or power bank. The system requires minimal initial calibration to initialize. All of its' characteristic points that this system is very useful in an institutional environment, schools, workplaces and any organization that requires strict authenticated and authorized users to be at the premises.

REFERENCES

[1] Mohammed, A. A., & Kameswari, J. (2013). Web-server based student attendance system using RFID technology. International Journal of Engineering Trends and Technology, 4(5), 1559-15563.

[2] Yongqiang, Z., & Ji, L. (2006, November). The design of wireless fingerprint attendance system. In Communication Technology, 2006. ICCT'06. International Conference on (pp. 1-4). IEEE.

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376.

[4] Shailendra, Singh, M., Khan, M. A., Singh, V., Patil, A., & Wadar, S. (2015). Attendance management system. In 2nd International Conference on Electronics and Communication Systems, ICECS 2015.

[5] Bhalla, V., Singla, T., Gahlot, A., & Gupta, V. (2013). Bluetooth Based Attendance Management System. International Journal of Innovations in Engineering and Technology (IJIET).

[6] Hanafi, H. F., Joe Meyer, C. M., Abd Wahab, M. H., & Abdul Kadir, H. (2009). PEAS : Portable Examination Attendance System : A Proposal. Portable Examination Attendance.

[7] Lodha, R., Gupta, S., Jain, H., & Narula, H. (2015). Bluetooth Smart based attendance management system. In Procedia Computer Science.

[8] Kassim, M., Mazlan, H., Zaini, N., & Salleh, M. K. (2012). Web-based student attendance system using RFID technology. In Proceedings - 2012 IEEE Control and System Graduate Research Colloquium, ICSGRC 2012.

[9] Rjeib, H. D., Ali, N. S., Al Farawn, A., Al-Sadawi, B., & Alsharqi, H. (2018). Attendance and Information System using RFID and Web-Based Application for Academic Sector. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 1

[10] Čolaković, A. and Hadžialić, M., 2018. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks.

[11] ITU, S.Y., 2001. global information infrastructure, internet protocol aspects and next-generation networks next generation networks–frameworks and functional architecture models. C:/Users/11598004/Downloads/T-REC-Y, pp.2060-201206.

[12] Chen, S., Xu, H., Liu, D., Hu, B. and Wang, H., 2014. A vision of IoT: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things journal, 1(4), pp.349-359.

[13] Díaz, M., Martín, C. and Rubio, B., 2016. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer applications, 67, pp.99-117.

[14] Kocakulak, M. and Butun, I., 2017, January. An overview of Wireless Sensor Networks towards internet of things. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-6). IEEE.

[15] Tschofenig, H., Arkko, J., Thaler, D. and McPherson, D., 2015. Architectural considerations in smart object networking (No. RFC 7452).

[16] Li, L., Xiaoguang, H., Ke, C. and Ketai, H., 2011, June. The applications of wifi-based wireless sensor network in internet of things and smart grid. In 2011 6th IEEE Conference on Industrial Electronics and Applications (pp. 789-793). IEEE.

[17] Mainetti, L., Patrono, L. and Vilei, A., 2011, September. Evolution of wireless sensor networks towards the internet of things: A survey. In SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks (pp. 1-6). IEEE.

[18] Naik, N., 2017, October. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE) (pp. 1-7). IEEE.

[19] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F. and Alonso-Zarate, J., 2015. A survey on application layer protocols for the internet of things. Transaction on IoT and Cloud computing, 3(1), pp.11-17.