Biomedical Research 2016; Special Issue: S217-S222 *ISSN 0970-938X*
www.biomedres.info

The design and analysis of a hybrid attendance system leveraging a two-factor (2f) authentication (fingerprint-radio frequency identification).

Parvathy Arulmozhi[1*], JBB Rayappan[2], Pethuru Raj[3]

[1]Department of Electronics & Communication Engineering, SASTRA University, India

[2]School of Electrical & Electronics Engineering, SASTRA University, Tamil Nadu, India

[3]Infrastructure Architect, Global Cloud Center of Excellence, IBM India, Bangalore, India

Abstract

With the overwhelming acceptance and adoption of RFID tags, a variety of everyday automation activities are being systematically accelerated and accomplished across different industry verticals. The passive RFID tags can be easily observed within 20 feet and hence can be applied to supply a unique RFID code for every tagged entity. For granting more powerful two-factor authentication, fingerprint images of students and other stakeholders are also being carefully captured and stored in network-accessible database systems locally as well as remotely for data and disaster recovery. This sort of arrangement significantly enhances the veracity of the participants' attendance and participation in their learning and professional assignments. For example, for schools, colleges and universities, the attendance details of students and scholars can be minutely captured and leveraged. In this paper, we have explained a framework for highly accurate attendance system. We have described how the local and the remote (AWS cloud) execution of data capture, processing, and storage happens and the distinct advantages of cloud-based data processing. Considering the need for higher network performance requirements, we have demonstrated how the seamless convergence of RFID with Li-Fi communication is to realize heightened cloud performance.

Keywords: Cloud computing, Two-factor authentication (2FA), Fingerprint images and radio frequency identification (RFID) system.

Accepted on August 06, 2016

Introduction

Undoubtedly authentication has been a prime requirement for assuredly identifying a variety of users. Generally, it is classified into one factor (1F), two factors (2F), three factors (3F) and multifactor [1]. This kind of authentications is verified by either biometric or RFID system. Biometric signals play an important role in the identity access management [2]. It is the legitimate method for finding an individual's physical or behavioural identity like fingerprint recognition, facial expression identification, voice identification, iris recognition, palm recognition, etc. The key characteristics of the fingerprint images are brought out by using a bifurcation method and it is compared with the database to secure the certification [3,4]. If it is equal to the unique number of the tag, then the user's details are sent to its corresponding email address. For this purpose, there is a seamless integration between RFID tags and fingerprint images.

RFID technology is basically used for automatic recognition of various animate as well as inanimate things. Now, it has been extensively used in various smart environments with continuous monitoring, measurement and management. Any RFID tag is similar to a barcode, but they are more efficient and easy to design [5]. A typical RFID tag consists of 3 components like RFID readers, tag sand antenna. The tags are locked to the object to be recognized and the antenna that can emit radio waves excites the tags. Tags are safeguarded with predetermined format data which involve in radio frequency range and communicate with the reader, which is called a transceiver circuit sends out the carrier and receives the backscattered signals from the tags [6-8]. Any RFID tag is composed of a chip and an antenna that gives out low-power radio waves to excite the tags. The chip is comprised of FSK-encoded signals picked up by the reader and processed for filter operation.

A back-end database server is used for storing fingerprint images and for comparison of the tag number. If the number is matched, then the details are sent to the e-mail ID via the internet [9]. The breathing system is incompetent to the user because it does not pick out the desirable person with suitable tag. For figuring out the current issue, the integrated fingerprint RFID system gets itself integrated with the cloud server for online monitoring by providing an efficient web interface or

suitable cloud services like Elastic Compute Cloud (EC2) and Simple Storage Service (S3). Storing a fingerprint database is an important role in reducing the execution time. If the database is stored locally, the operating system and configuration of the system drives the communication resources leisurely, so the processing time is increased [10]. At the same time if it is stored on a virtual machine (cloud server) the execution time is significantly reduced by using cloud platforms like Storage Area Network (SAN) and Network Attached Storage (NAS).

Traditional RFID System

In the smart environment, the communication devices such as RFID reader are communicated to cloud server with Wi-Fi module for security reasons by providing a multi-level authentication.

Table 1. *Limitations of RFID system.*

S. No	Modules	Hardware	Software	Identification Factor	Authentication Level	Cons
1	Automatic RFID System	Reader, Passive tags, and Antenna	Back end server(SQL Access) Front end server(VB) RFID software(Real term)	Unique No(14 Bits)	1FA	Loss of privacy
2	RFID with cloud server	Reader, Passive tags, and Antenna Cloud Server.	Cloud Server, RFID software(Real term)	Unique No(14 Bits)	1FA	Loss of Privacy, security and RFID Collisions and Attacks are not defined.

As mentioned in the Table 1, the readers are attached to back end server and cloud server and it operates with multiple tags for various applications. In the meantime, it is more difficult to secure the privacy of the system. If the system uses a smart environment security and privacy both are main concerns that needed to be considered. To conquer the problem, the fingerprint RFID system was introduced on cloud with three-factor authentications (3FA).

Proposed Methodology

The proposed attendance system is to run on both local as well as remote clouds (a kind of hybrid clouds). The local system involves a commodity server with a traditional SQL database (we have used MySQL DB). On the cloud side, we have check in with the two key storage management systems (Storage area network (SAN) and network attached storage (NAS)), We have stored students' fingerprint images captured in different views on both local as well as remote systems. We have tested how the local and remote image processing and query execution happen in order to identify the time taken by both systems. The projected work is classified into four divisions

- Why Fingerprint and RFID are for next-generation Attendance Systems?
- Installation and Configuration of Database and MATLAB Software on AWS EC2 Instances
- A Brief about the prominent Cloud Storage Systems
- Time complexity analysis of fingerprint DBs on local as well as remote machines

Why Fingerprint and RFID are for next-generation Attendance Systems?

The first step in this method is to capture the RFID unique number by RFID reader using the RFID software such as Putty, Real term, and hyper terminal followed by the second step were the fingerprint was ensured using the recorded data through identification and verification. Bifurcation was used to extract the features and it was compared with the database. Micro Soft access was used as the database back-end and MATLAB with its two design forms in the front end of the user.

A collection of fingerprint images: Mathematical models were the base of image processing to secure a reliable biometric system. In this work, the first process describes the collection of vein images of the fingerprint from the individual user.

Table 2. *Finger's vein image details of different users.*

Users	X-Value	Y-Value	Various Position of Angles (in °)			No of Terminations	No of Bifurcations
			A1	A2	A3		
101_1	135	67	-2.36	1.05	0.79	27	6
102_2	133	101	2.36	-2.62	-0.52	60	3
101_3	198	101	2.36	-2.36	-0.79	4	46
102_4	194	117	2.36	0.79	-0.79	69	3

101_5	200	NaN	2.36	NaN	-1.05	39	20
102_6	214	136	0	0	0	42	42

Table 2 depicts the six finger's vein images that were extracted by minutiae method. The number bifurcations count was decreased as the number of instructions called by the MATLAB program features were extracted from it. Then the collected input data was passed on to next process to ensure the original data by using a Minutiae method.

Minutiae method: In the biometric system, the minutiae based techniques represent a vein pattern of the fingerprint by using its local features like end points and bifurcations. To extract minutiae, crossing number method is employed. A pixel-wise operation is performed to obtain the bifurcation points and end points. The various positions of the angles and the total number of bifurcations were used to reduce the time complexity in a virtual machine as it gives a better solution for authentication and has been a more reliable system cloud environment.

Enrolment model for fingerprint images: As illustrated in Figure 1, the biometric data (Fingerprint) of each user was first examined in the local server and it was verified in cloud server also. So it resolves the problem that we mentioned above and realizes 3FA.

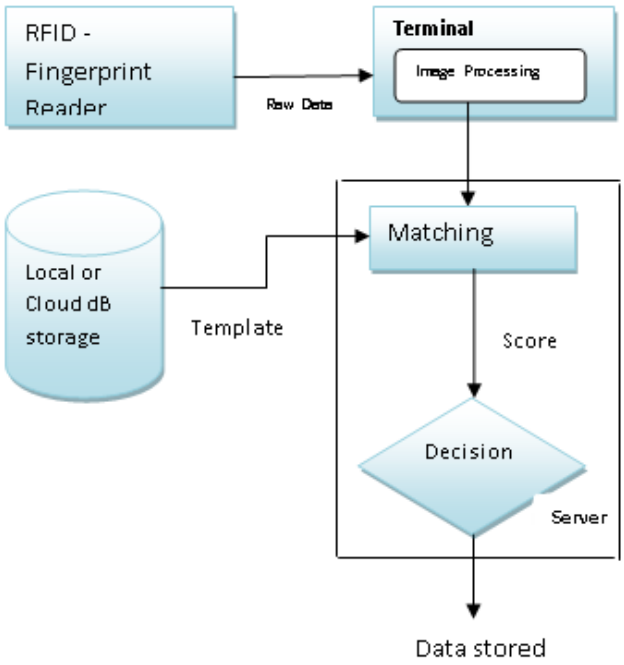


Figure 1. *Flowchart showing the matching process of RFID data with fingerprint.*

The algorithm steps:

1. RFID card was initially sensed by the reader.

2. RF reader starts to match the string which was available on the card with anyone of the database entries as

$RF_i.RF_i.^T = I$, $RF_i.RF_j.^T = 0$

$R_{iRF+fingerprint\ of\ individual}$

3. Figure print matching will be analyzed if the reader was recognized

$FP_i.FP_i.^T = 1$, $FP_i.\ FP_j = 0$

4. The input pattern is pre-processed and is converted into a binary pattern as:

B(i)=1 if I(i) ≥ T

= 0 I(i)<T

I(i)-pixel value of grey image,

B(i)-Value of binary image, T-Threshold value

5. Morphological algorithm governed by the binary image to thinning the images for identifying shapes of every individual $\{(A \oplus B) \oplus B1 \oplus B2 \ldots\}$

A-Binary image

B-Structuring element

6. Minutiae algorithm was then imposed on the result of the previous step to acquire the features which had a unique identity for authentication

The goal of this process is to reduce the noise or any distortions in the original image [11]. The salt and pepper noise which was random black and white pixels on the image was removed by using Gaussian blur which is expressed using the equation:

$$G_n(X_1, Y_1) = \frac{1}{2\alpha^2} e^{-(x^2+y^2)/2\sigma^2}$$

Where α denotes the blur radius ($\alpha = x^2+y^2$), σ the standard deviation of Gaussian distribution which will create a matrix to find the edges of the image addition with noise. The database is created for the corresponding fingerprint images and it is stored in Cloud machine and local machine for the validation.

Installation and configuration of database and MATLAB software on AWS EC2 instances

The Amazon Web Services (AWS) Free Tier is intended to enhance the hands-on experience with AWS Cloud Services. It includes services with a free tier available for 12 months followed by AWS sign-up date, as well as additional service that does not automatically expire at the end of 12 months. After creating an AWS account, it was used for any of the products and services, listed below, for free within certain usage limits

- Get the Amazon Web Services (AWS) cloud login
- Access the EC2 service from the cloud.
- Finally, launch the program and compute the output.

Creating an elastic compute cloud (EC2) instance using the AWS console: Virtual servers are described by the Amazon EC2 service for virtual storage. Compute-intensive and cluster-based applications are efficiently run in cloud server with a unique platform like EC2. AWS Console can be accessed via the Amazon Web Services which creates an instance (a compute resource), checks the status of user's instances and even terminates an instance. When an EC2 instance was launched, the user receives a Public IP address .That address was changed if the instance is stopped or restart .So, public IP can be changed every time. To conquer this problem, an Elastic IP can be emotionally involved to an Instance which does not change after the stop/start process. So the user can liberally access the instance for N no of times with same IP address called Elastic IP. It is "permanent" in the sense that the user owns it and associates it to a specific AWS instance ID.

A brief about the prominent cloud storage systems: In general, the cloud architecture was chosen uses two concurrent platforms called Cloud storage and Non-cloud storage. The first method is Non- cloud storage it is based on Storage Area network (SAN) and the second is cloud storage it is based on Network Attached Storage (NAS). SAN is important to know which hardware device such as hard disks in the SAN support. Then the NAS devices are able to be tied up to make an SAN unconventionally with manual and computerized decision.

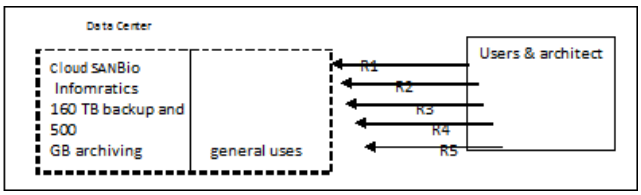


Figure 2: 5 routes for the backup process on cloud storage system.

Entire network routers are represented by R1, R4 AND R5 respectively in Figure 2. To explain the syntax of the algorithm:

continue (st))- It detect a failure job

report (st))-System gossip back the job status

stop (st(job))-demand are terminated

record (st(job))-It tells the completion of job request

rerun (st(job))- completing time is include to the entire job

check (Rx.st(traffic))-to check the network status

Time complexity analysis of fingerprint DBs on local as well as remote machines

The RFID tag unique number is detained by the fingerprint reader for first level authentication. Then it ensured by the fingerprint images for the second level (2 FA). If the fingerprint is matched with unique RFID code obviously, it has been sent to the user's mail via the internet. The database system will utilize the hardware together with software. The various organizations are in need of increasing data in size and number for internet applications. To storing a huge amount of data independently in these are not possible and leads them in demand for storage space. So by using a fingerprint RFID with cloud storage gives a well-organized model for authentication. It plays a very important role in proposed methodology for reducing the time complexity. In this work the execution time of fingerprint program is analysed and, the time complexity is compared with local database and cloud database. The following Figure 3 shows the absolute declaration of the time complexity of the program with different database storage in Local, Cloud and shared machines.

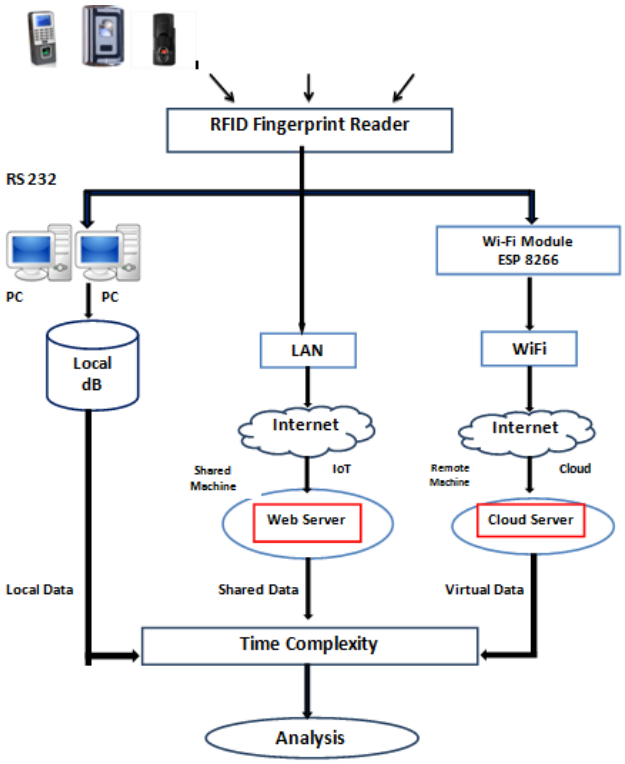


Figure 3. Summarized workflow diagram of cloud database and local database.

The RFID reader is connected to the local machine by RS 232 cable and it is connected to cloud machine with RFID Wi-Fi module. Subsequently, the RFID-Fingerprint MATLAB program is executed on all machines to compare the complexity. To execute the program in the cloud server, we get the login in an Amazon cloud with Infrastructure as a service (IaaS). The Amazon public cloud offered a three services such as IaaS PaaS and SaaS .If any customer under IasS, He/She can get a complete virtual machine .When the PC- based program (MATLAB) is executed on are mote machine , the execution time is very minimum rather than the web-based program (Java).

Fast data access from cloud storage using Li Fi system

As elucidated elsewhere, we leverage cloud environments to host the attendance application and the support systems such as the MATLAB and SQL database. The problem here is the time to transfer data from classrooms to the faraway cloud is definitely on the higher side. This squarely depends on the

Internet speed. Correspondingly the response time after the processing at the cloud is also equally longer. That is, the network performance affects the cloud performance and hence we decided to embark the usage of RFID system with Li-Fi communication. With the increasing usage of the Wi-Fi technology, the radio frequency, which is already scarce, is getting blocked slowly and hence the traffic is bound to increase sharply. So we have used Li-Fi and found out that the combination of RFID and Li-Fi works wonders for cloud communication. The cloud application performance becomes good with this initiative.

The advantage of LI-FI

1. Tremendous data transfer rates and less traffic
2. Safe and secure (no-body can hack it,) since no signal penetration through walls.

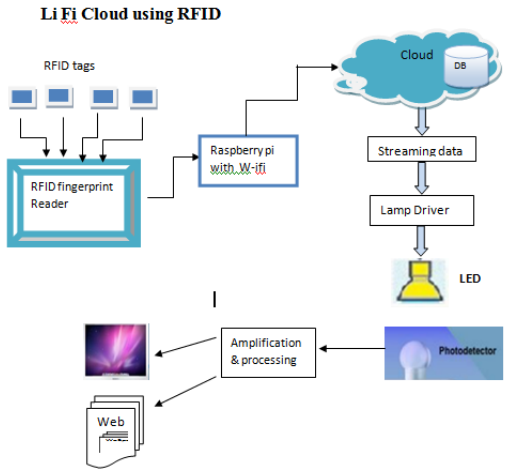


Figure 4. *Single core architecture using RFID system with LiFi cloud.*

The functioning of Li-Fi is simple, yet amazing. It needs only two parts, ones is first is LED (transmitter) and other is photo detector (receiver). LI-FI uses the Visible Light Communication (VLC). Which uses visible light between 400 and 800 THz (780-375 nm) with 1 and 2 km distance. In this work the Raspberry pi (single core) is connected to cloud server to upload the fingerprint database and lifi system (indoor) is used to access the data (Figure 4).

Results and Discussion

The RFID reader is connected to the local machine by RS 232 cable and it is connected to cloud machine with RFID Wi-Fi module. Subsequently, the RFID-Fingerprint MATLAB program is executed on all machines to compare the complexity. To execute the program in the cloud server, we get the login in an Amazon cloud with Infrastructure as a service (IaaS). The Amazon public cloud offered three services such as IaaS PaaS and SaaS. If any customers are under IasS, the user individual can get two platforms like SAN or NAs on a virtual machine. The results are shown in two approach, first it show how fast the fingerprint Matlab program is executed in cloud machine and local machine and second it demonstrate how fast the internet data are accessed by the user with LiFi system.

Execution time for fingerprint DB in local machine

System reporting time=Number of failed jobs × backup time=10 × 4=40 seconds

Job completion time=10/0.4=25

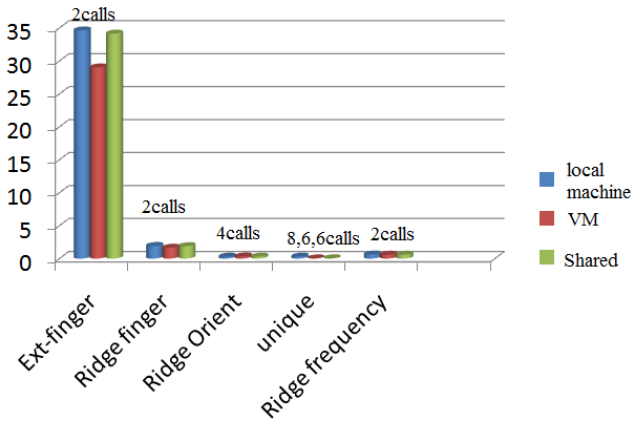
Additional time due to network quality: 1% risk-control rate

Total expected time=40+25+25=90 sec.

Execution time for fingerprint DB in cloud machine

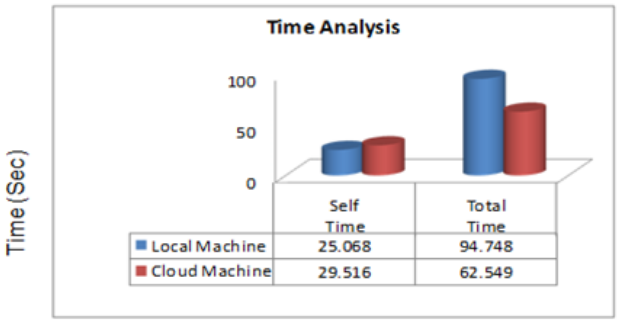
Total additional expected time=10+25+25=60 sec.

The graph 1 shows the results of instructions are called by number of times



Graph 1. *Actual execution time and number of instructions called by two machines.*

The following graph 2 shows the results of program execution times with 4.448 seconds of difference with local machine and 32.199 seconds of difference with cloud machine. EBS volumes are particularly well-suited for database-style applications (MATLAB).

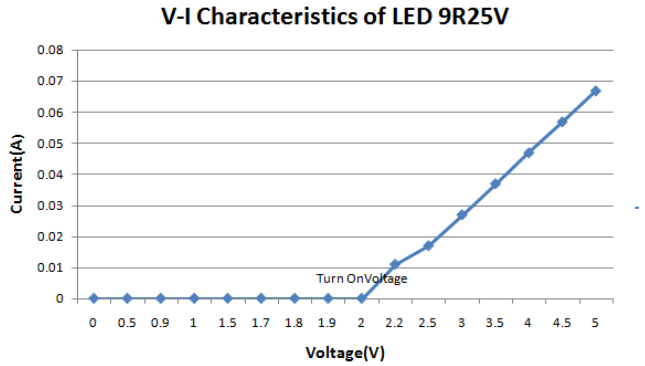


Graph 2. *Actual execution time for non-cloud (local) and cloud machine.*

This experimentation was made possible through the utilization of an Elastic Compute Cloud (EC2) virtual machine from the Amazon Web Service (AWS) public cloud and the solutions obtained have been clearly exemplified in this presentation.

Current versus voltage characteristics of LED

In optical wireless communication systems due of non-linear V-I characteristics of LED. The output power consider as function of the input current. The measured current-voltage characteristics of Red LED used in experimental setup (Multisim 10). The LED has a threshold value called as turn on voltage (TOV). As shown in the following graph 3. Further increasing the voltage allows the current to flow the output optical power nonlinearly as a function of the current.



Graph 3. *Turn on voltage of the 9R25V LED.*

To avoid the electro-optical efficiency the LED should be operated with limited dc current. By changing the input power of LED and amplifier circuit, the Bit Error Rate (BER) is calculated. The BER is directly proportional to data rate.

Conclusion

Applications are being taken to cloud environments in order to reap the originally envisaged benefits of the cloud idea. Through this experiment, it is proven that when the fingerprint database is also with the cloud application, the real-time performance is being achieved. That is, the parents, teachers and other stakeholders get informed about the developments in time in order to ponder about the next course of action. This arrangement of the double check (RFID and Fingerprint) comes handy in reducing the human errors. The hybrid application (running on local as well as cloud servers) also enhances the system availability, scalability, and controllability. Nowadays, with the faster maturity and stability of Li-Fi technologies and solutions, we have investigated the data transmission using the Li-Fi system. The result is awesome and the data and response transmission times have done considerably. It is clear from the experimentation that the cloud access and usage times will be substantially less with the Li-Fi technologies.

References

1. Kassim M, Mazlan H, Zaini N, Salleh MK. Web-based student attendance system using RFID technology. Control System Graduate Research Colloquium (ICSGRC) 2012 IEEE, Selangor, Malasiya.
2. Noman ANM, Rahman SMM, Adams C. Improving security and usability of low-cost RFID tags. Ninth Annual International Conference on Privacy, Security and Trust (PST), 2011, Montreal, Canada.
3. Xu H, Veldhuis RNJ, Kevenaar TAM, Akkermans TAHM. A fast minutiae-based fingerprint recognition system. IEEE Syst J 2009; 3: 418-427.
4. Zheng R, Zhang C, He SH, Hao P. A novel composite framework for large-scale fingerprint database indexing and fast retrieval. International Conference on Hand-Based Biometrics, 2011, Hong Kong.
5. Kulkarni G, Chavan N, Chandorkar R, Waghmare R, Palwe R. Cloud security challenges. 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2012, Bali, Indonesia.
6. Sun Y, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. Int J Distributed Sensor Networks 2014.
7. Han J, Susilo W, Mu Y. Identity-based data storage in cloud computing. Future Gen Comput Syst 2013; 29: 673-681.
8. Parvathy A, Rajasekhar B, Nithya C, Thenmozhi K, Rayappan JBB, Amirtharajan R Raj P. RFID in the cloud environment for Attendance monitoring system. Int J Eng Technol 2013; 5: 3116-3122.
9. Gao Y, Hu X, Peng L, Liu H, Li F. A differential evolution algorithm combined with cloud model for RFID reader deployment. 4th International Workshop on Advanced Computational Intelligence (IWACI), 2011, Wuhan, China.
10. Chu L, Wu SJ. An integrated building fire evacuation system with RFID and cloud computing. 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, Dalian, China.
11. Prakash R, Agarwal P. The New Era of Transmission and Communication Technology: Li-Fi (LightFidelity) LED & TED Based Approach. Int J Adv Res Comput Eng Technol 2014.

*Correspondence to

Parvathy Arulmozhi

Department of Electronics & Communication Engineering

SASTRA University

India