© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Engineering and Technology

Digital Memories based Security for Intruder Detection using RFID

Shyamala P, Veluchamy M

Department of Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

ABSTRACT

A system and method for identifying the intruder through RFID tag who has approached towards the door to access the secured room. The GSM component fixed on the door will send the RFID tag details to android application. This application will be accessed by security administrator and it will have two factor user authentication mechanism to validate the security administrator. In this proposed system, based on the RFID, the security administrator identifies whether the person want to access the door is an employee or intruder. This improves efficiency over intruder detection concept and yields a good result.

Keywords: RFID, Digital Memories, Intruder, Android, IOT, Security Administrator

I. INTRODUCTION

As, the IoT concept continues to grow, the security provided should be highly efficient. This is because it is embedded within our environment in daily life. The communication that takes place between software application and hardware components should establish a secured interaction between them. Even though, many techniques have been used to provide security such as biometrics authentication, single alpha numeric authentication, they are outdated& weak too. The issues with present authentication mechanism will continue to grow until a good feasible approach is developed.

There are wide varieties of strategies to identify a intruder or employee who want to access the door in an organization. But sometimes, the way of identifying leads to false predictions. So, researchers are keen on developing new methods. Moreover, physical security requires the design, implementation and maintenance of counter measures that protect the physical resource of an organization. Generally, the deliberate act of espionage could be a competitor sneaking into physical asset with camera or other resources.

In the emerging era of computing technologies, digital memory security is, the idea of storing user memories such as photograph, videos in to physical memories and validating the user using those digital memories in a given stipulated amount of time. So, these digital memories are highly specific to those user and except the user, it cannot be easily identified by third party people or intruder or hacker.

In this system, we propose a security framework for identifying an intruder through RFID and necessary security action are taken through android application which will be accessed by security administrator. An android application is developed with digital memory security concept to verify the security administrator. The details of the person, who want to access the secured room in an organization, will get notified in the android application. Through this system, the attacker can't able to breach the security asset of organization by any other means such as shoulder surfing, social engineering phishing attacks or other traditional attacks.

II. METHODS AND MATERIAL

A. Related Work

Research in RFID security has gained a lot in recent years. Many publications focused on security and privacy in RFID applications. Rotter el al has provided a detailed description about the possible security attacks in RFID. Researchers have provided various counter measures to mitigate those attacks. Rieback et al proposed RFID guardian that integrates various security mechanism into a single compact device. Some of the security concept such has auditing are not used earlier. However we use RFID tag to identify the employee and to retrieve the employee details using the tag and pass to application through GSM component which is fixed in the door.

Similarly in digital memories security concept for IoT have many related works for it. In 1945, the idea digital memories were conceptualized by Bush Memex. This concept is implemented in storing books, record etc. But, in today society, the development in technologies has brought this idea in to real time scenario. It showed a way for "life logging" which refers to the process of using the record generated by devices in various aspects of life known as "life logs" or human digital memories. The base technique behind the software is eliminating the threat of passwords being stolen and other phishing attacks happening in organization.

B. Existing System

In existing, the concept of Smart card based physical access system was used. A physical access system is coordinated network of ID cards, electronic readers. This system is developed for protecting the enterprise asset. Each employee of the organization is issued a smart card as ID which has enterprise details along with employee details. Each card stores protected information about the person and the person's privileges. When the person accepts the card, the details of the employee are feed into the card. When the card is placed near the electronic reader access is granted or denied depending upon the employee. So, based on this, the physical access system is secured in the organization. But, there are some drawbacks in this system which may pave the intruder to easily mitigate these security mechanism system .In this System, in case if the card is stolen and misused by intruder ,then the entire security system get breeched. Moreover, the authentication of card is done through electronic reader which is internally connected to Database. In case, if the intruder hack the database and make change over them, the system gets less secured. So, in our proposed concept the drawbacks of this system have been rectified and developed an efficient and secured system.

C. Proposed System

The system for intruder detection in an enterprise consist of: RFID detection, GSM component, android application(Digital memory security concept).These three components work sequentially to identify the person who want to access physical components.

- **RFID Detection**

Initially, the organization will issue a RFID card to their employees with unique 10digit code. So, each unique tag has its own employee details embedded with it. So, when an employee approaches toward the door, he places his RFID card over the RFID reader. It detects the tag and passes the "10digit" tag to the Renesas microcontroller. This controller forwards the tag to GSM component through UART communication channel.

- **GSM Component**

The GSM component receives the information from microcontroller through UART.GSM have also established communication between android application. So, whenever it receives a tag, it will send the tag details to android application. The communication takes place between GSM and Microcontroller over the UART channel. The GSM has configured with properly, so it sends the RFID details in a secured manner to android application which will be further accessed by security administrator. There is a LCD interface which is connected with controller. This LCD interface displays the status of the system. Such as "System Starts", "RFID sent successfully" etc.

- **Security Through Digital Memories**

The Android application is mainly developed with two factor user authentication to validate the security administrator in an effective manner. At first, the application will have alphanumeric login authentication. After that, the digital memories authentication takes place i.e., in the application a number pattern will be generated and group of images will be there. The security administrator should arrange the images according to the number with in short period of time like 15-20 seconds. By completing this authentication, there will be a image and a question related to that. So, by clearing all these levels only the security administrator gets validated. In the second part of application, he will receive notification with the employee photo, name, designation, privileges and other details, when any employee had come to access the door. By, verifying all the details, the security administrator grants the permission or denies it. If the permission is granted, the GSM receives notification and forward the information to controller. The controller sends the control message to open the door and door gets opened finally. In case if access gets denied, the LCD displays a message as "ACCESS DENIED".

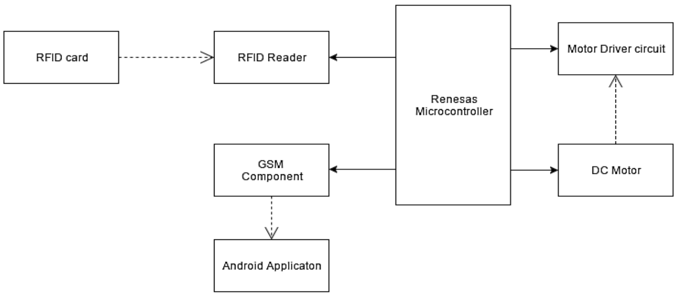

Figure 1. Block Diagram of the System

In this system, the Renesas controller (R5F100LE) is used because it is best suited for communication purpose. This controller has good operating frequency upto 32MHz.There are three communication protocols in it : UART, SPI, I^{2}C. In this system, UART protocol is used.

III. RESULTS AND DISCUSSIONS

A. System Architecture

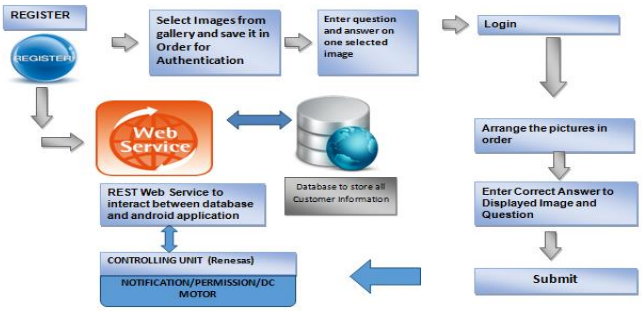
REGISTER
REGISTER
Select Images from gallery and save it in Order for Authentication
Enter question and answer on one selected image
Login
Web Service
Arrange the pictures in order
REST Web Service to interact between database and android application
Database to store all Customer Information
Enter Correct Answer to Displayed Image and Question
CONTROLLING UNIT (Renesas)
NOTIFICATION/PERMISSION/DC MOTOR
Submit

Figure 2 : System Architecture for the Intruder Detection using RFID

Firstly, the security administrator does the registration by selecting the necessary images and other details for authentication. This registration can be done only one time. Once, the administrator finishes the registration he can't undo or make any alteration too. Then Login authentication takes place. After that, based on the notification ,the security administrator takes the action accordingly. This is the overall architecture of the system.

B. Flow Chart

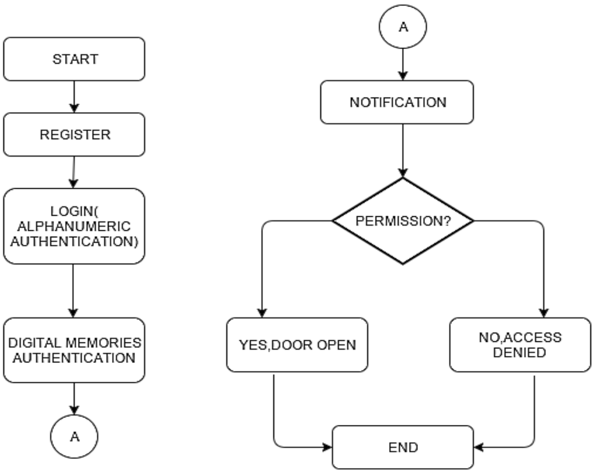

Figure 3. Flow chart Of the Proposed System

Flow chart depicts the order of execution in the system.

C. Comparison With Existing System

In existing system, employees in the organization have smart card to access the physical components such as door. There is a card reader which reads the smart card of the employee and permits them depending on their privileges. But, the same card can be misused by any other person too. This is one of the major drawbacks in the system. But, in proposed system the security administrator verifies the employee through the camera and checks the same employee picture is there on the notification. If both get matched and other details are also verified only, the person is permitted to access the room.

Table 1.Tabular Column for Comparing smard card system

Sr. No	CRITERIA	EXISTING SYSTEM	PROPOSED SYSTEM
1	Card	Smart card	RFID Card
2	Employee Verification	Only by smart card reader	Done by security administrator
3	Background reference	No	Log file maintained and often verified by higher administrator of organization.

IV. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, the concept of digital memories has been developed along with the intruder detection using RFID. So, it provides an enhanced security to identify intruder and them properly. In future enhancement, it can be developed with a camera which is kept in the door. This camera captures the snapshot of the person and sends to the administrator for further verification. So, the effectiveness of security can be enhanced a lot.

V. REFERENCES

[1]. C. M. El-Sayed, A. Mukhopadhyay, C. Urrutia-Vald´es, and Z. J. Zhao. the opportunity through dynamic policies and QoS pipes. Bell Labs Technical Journal, 16(2):79–100,2011

[2]. J. Huang, F. Qian, Z. M. Mao, S.Sen, and O. Spatscheck. Screen-off traffic characterization and optimization in 3G/4G networks.InProc. of ACM IMC, pages 357–364.ACM, 2012.

[3]. J. Huang, Q. Xu, B. Tiwana, Z. M.Mao, M. Zhang, and P. Bahl. Anatomizing application performance differences on smartphones. In Proc.of ACM MobiSys, pages 165–178.ACM, 2010.

[4]. G. Maier, F. Schneider, and A. Feldmann. A first look at mobile hand-held device traffic. In Passiveand Active Measurement, pages 161–170.Springer, 2010.

[5]. R. Want et al., "Bridging Real Virtual Worlds with Electronic Tags," Proc. ACM Sigchi, ACM Press, 1999, pp. 370ndash] 377.

[6]. M. Mitra, "Privacy for RFID systems to prevent tracking andcloning," International Journal of Computer Science and Network Security, vol. 8, pp. 1-5, January 2008.

[7]. C. Cremers, P. Lafourcade, and P.Nadeau, “Comparing State Spaces inAutomatic Security Protocol Analysis,” in Formal to PracticalSecurity, 1st ed. Berlin: Springer-Verlag, 2009, pp. 70–94.

[8]. M. Rieback, B. Crispo, and A. Tanenbaum, "The evolution of RFID security," IEEE Pervasive Computing, vol. 5, pp. 62 69, January-March 2006.

[9]. S. Karthikeyan and M. Nesterenko, "RFID security without extensive cryptography," in Workshop on Security of Ad Hoc and Sensor Networks - SASN'05,(Alexandria, Virginia, USA), pp.63-67, ACM, ACM Press, November 2005.