IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Multifactor Authentication System

Prof. A. J. Jadhav[1], Diksha Shetty[2], Apurva Marathe[2], Pralay Nawasare[2], Roshan Ramdas[2]

Professor, IT, Rajarshi Shahu College of Engineering, Pune, India[1]

Student, IT, Rajarshi Shahu College of Engineering, Pune, India[2]

Abstract: Radio Frequency Identification (RFID) is used to track tags attached to the objects using electromagnetic fields. RFID is a short range wireless communication system which uses radio frequency technology for automatic target recognition. RFID consists of three parts: labels, antennas and readers. The technology used to identify every individual uniquely is known as biometrics. In paper[], this technique is consumed along with RFID and image processing for identity authentication. Biometrics also refers to the pattern recognition system where the users' bio data is being referenced from the database. The use of a cellular network known as GSM (Global System for Mobile Communications) is applied where mobile phones connect to other cells in the immediate locality. The paper[] shows an intelligent usage of GSM technology to generate one time password (OTP). GSM is highly used in making intelligent control and decisions in reference to sending relief supplies [].

Keywords: RFID, GSM, Biometrics, Image processing.

I. INTRODUCTION

In this paper we have tried to implement multifactor authentication by using RFID, Biometrics and GSM technology which will be more secure than other systems. Radio-frequency identification (RFID) technology system allows only authorized person to get the ration. RFID is different from other technologies because it contains all the sensor tags embedded in the tracked object itself. Bar code is not needed to track the object. RFID is mainly used for automatic identification.

The authentication is a process of verifying the legal user, it can be based on the following factors: possession factor such as identity cards and security token; knowledge factor such as passwords and personal identification numbers; and biometrics such as face, fingerprint etc. The most common form of authentication is the single-factor authentication, which only requires one factor for the user to log into the system. Login and password authentication models are weak and can cause loss to those who uses it. The Multifactor Authentication (MFA) requires the combination of two or more layers of authentication.

In this review paper, we have tried to identify the different approaches for authentication and also the amount of work that is done on multifactor authentication till date.

Biometric is used in security to mean measurable physical characteristics of a person that can be examined on an automated basis. Biometric system refers to the various single components like various sensors, matching algorithms and result. Biometric system differentiates a submitted fingerprint record to a database to determine the identity of an individual. Fingerprints remain sustained throughout life. In over 150 years of fingerprint differentiation no two fingerprints have ever been similar, not even those of identical twins.

GSM is used by digital cellular networks and mobile phones. Earlier GSM was a circuit-switched network using full duplex voice telephony and later data communications was added. Nowadays GSM involves transportation of packet data via GPRS. GSM includes a base station a network and switching sub system, GPRS core network, one operations support system (OSS).

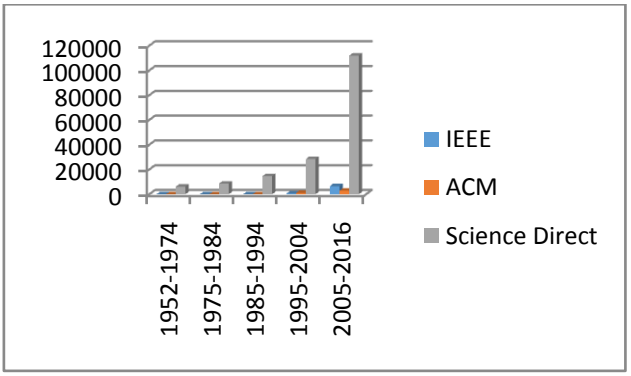

Fig. 1. Graph of work done till date using keyword "RFID" on IEEE, ACM, and Science Direct

II. VARIOUS APPROACHES USING RFID, GSM AND BIOMETRICS

A. Systems that used RFID:

In paper [8], the authors have proposed a system which contains door locking system which makes use of passive type of Radio Frequency Identification (RFID). With the help of RFID wireless automatic identification becomes a very easy task as the object or individual is marked with a code which is unique and the person or object can be identified with the help of that code, this code contains a RFID tag which is some way embedded into the target. RFID is not a single product but a comprehensive system,

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

A typical RFID system include three basic elements: RFID tag (transponder), reader (transceiver) and back-end application system (or database). For controlling, management, transaction and operation of various user's software is used. Hardware as well as software is used in this system. The hardware components are RFID reader, tags, USB connections and connecting cables etc. In addition, the author has used actuator i.e. stepper motor for this purpose. The RFID tag is detected when touched or come in the range of few millimeters from reader.
The author has successfully implemented security system which can various applications like to record attendance in class room of institute or in a secured zone so that only authentic person can enter in secure space.

B. Systems that used RFID and Biometrics:
In paper[5] a safe and secure web based attendance monitoring system is developed using Biometrics and Radio Frequency Identification (RFID) Technology based on multi-tier architecture, for both computers and smartphones. The attendance records of both students and teachers/staff members of an institution can be maintained by the system. At the time of admission student/teacher will be issued a RFID tag and also a biometric fingerprint scan will be performed.
The current location of the students, faculties, and other staff members anywhere within the domain of institution campus can be detected by the system. With the help of android application, one can receive live feeds of various campus activities, keep updated with the current topics in his/her enrolled courses as well as track his/her friends on a real time basis. An automated SMS service is facilitated in the system, which sends an SMS automatically to the parents in order to notify that their ward has successfully reached the college. Parents as well as student will be notified via e-mail, if the student is lagging behind in attendance. There is a functionality of automatic attendance performance graph in the system, which gives an idea of the student's consistency in attendance throughout the semester.

In this article, individual's biometric index, radio frequency identification (RFID), and image processing are brought together in order to offer a new model of identity authentication. The suggested system has been designed in two phases: producing identity authentication card and identity confirmation. The individual's biometric images are put on a contact-less card equipped with an RFID tag and for each identity authentication, the data on the card are compared with the online biometric image. If the individual's identity is authenticated, then there will be no need for him/her to punch in the personal information since his/her information will be retrieved from the database through their electronic personal code (EPLC). This article has made use of the HMAX model which works hierarchically based on human's and some animals' visual system for extracting the features of images. Template matching has been done on the features of image taking a threshold of 0.9. To test the mentioned model, FVC2008 standard dataset containing 800 fingerprint images (8 images for 100 people) was employed. The experiments indicate that not only does the above-mentioned model show invariance to picture rotation and its scale but it also proves to be 98 percent responsive on the given dataset.
The experimented pictures were also fed into the PCA model. The experiments show that the PCA has a lower identification coefficient than the HAMX model (70 percent) and it responds favorably only under controlled circumstances. In this project, the HMAX model was used as a method of extracting features from images. This model is based on the visual system of humans and some animals.
In paper [1], the author has proposed a concept of Multifactor Authentication (MFA) a specific step for confirming whether the system is claimed to be is authentic, where there a different factors of authentication such as knowledge factor, possession factor and lastly a inherence factor. So as for authentication, MFA uses two levels of security (RFID and Biometrics) To achieve this in the current system, the main purpose should be is to create a layered security defense mechanism to make it harder for a non-user so that he has no access to the database of the system. If by any means the non-user personal has successfully broken the first security barrier he still has to break in the other layer too making it hard to break in the target. The system has a hexadecimal format to read the users RFID which is the input given firstly.

The authentication process starts where the user has to use his fingerprints as in for identity. The data is now stored in the system authorization phase decides whether to accept or reject if two factors appear in the database. The main concept of RFID and Biometrics is that RFID contains Tags which will communicate with an RFID reader, when close to the proximity range will store and retrieve data and in the case of Biometrics is nothing but a pattern recognition system which uses bio data from a user and fetches information from the system and comparing it with the stored template. Two Data Strings are compared i.e. between RFID and Fingerprint Scanner where commonality is achieved. The only disadvantage is if either of the system is breached in, private information like name, address will be accessed.

In paper [6], the authors have developed a system that provides real time security managing methods that can be implemented using RFID, Biometric and Smart Messaging. In this system a real time security management system is developed using fingerprint (optical) as Biometric and ISO 14443 Mifare 13.56 MHZ smart cards to control the entry of staff to various sections for security purpose and for attendance monitoring. The basic methodology of this system developed in this paper is to provide security to any organization by restricting entry to the restricted areas by using the Biometric Machines.
The staff enters with the help of their RFID card and are verified with the help of biometric scanner and the doors

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

will open only if verification is true. Staff details, time of entry/exit get recorded in the Database which is used for their attendance processing. The database used in this system is oracle 10g. Any unauthorized attempt to open the door will get recorded immediately in the database and it activates the GSM modem to send SMS alert messages to the Security Staff mobile phones. The system proposed in this paper provides higher security and is a Contact-less card with biometric authentication, real time status monitoring and smart messaging which makes the security management more efficient and reliable.

C. Systems that used RFID and GSM:

In this by using the technology of wireless sensor networks (WSNs), radio frequency identification (RFID) and global system for mobile communication(GSM), a wireless communication and intelligent application system is constructed. The information processing subsystem uses this real-time data transmitted by GSM to make intelligent control and decision support to the whole process of materials dispatching, therefore, relief supplies are send to all the settlements in time and with high quality. It truly realizes the real-time data collection, analysis, assessment and dynamic monitoring in the process of distribution and transportation to ensure relief supplies reach each resettlement timely.

The system consists of wireless sensor nodes module perceiving environmental data of relief supplies, RFID module identifying and delivering data of a variety of relief supplies, precise positioning of moving objects module by car GPS chips and satellites, data transfer module by wireless communication networks GSM and data processing module which analysis and make decision for various relief supplies information in relief supplies information processing subsystem.

In paper [2], the author has proposed that in a Bank Locker Security System there will be 2 phases of password for double security. Firstly, the user has to use his RFID to access his account, RFID reader will scan and read the tags all along and send it to the micro-controller. If the user is an authentic one, the micro-controller will display the account holders name and details. While displaying the name to access further the user has to put password in the micro-controller, if valid an SMS will be send to the registered number of user.

The SMS is nothing but the One Time Password (OTP). If the password is correct the micro-controller will send the bank locker a control signal to open. This is a simple and a secure method than the other systems. Comparison of existing and proposed locker system is also done where the existing system is one referred password and the proposed system is two referred passwords. In existing system RFID Technology is used and in Proposed system RFID and GSM Technology is used. It clearly even shows that the existing system is insecure as compared with the proposed one.

In paper [5], the authors have proposed a new model for alerting the parents and automatic attendance marking by making use of RFID and GSM (Global System for Mobile Communication). RFID technology is different from other technologies as it contains all the sensor tags embedded in the tracked object itself. Whereas GSM involves transportation of packet data via GPRS. The microcontroller we used in this system is a LPC2148 microcontroller. It consists of an ARM 7 microprocessor. The programming related to this system is done in embedded C programming language.

The specifications of this microcontroller are maximum speed: 30 MHz The Voltage is 3.3V. Here system makes use of passive RFID tags as it has a longer life and is also easy to maintain. TDMA is used by GSM, to send voice or data in various time slots. The microcontroller is connected to a GSM modem. UART is used by the microcontroller, and it is operated through AT commands which are sent by the microcontroller to the modem.

Advantages of the given system is that it saves time and takes attendance automatically without any human intervention and disadvantage is that card can be misused and can be given to someone else to mark fake attendance as well as if card is swiped twice attendance will also be marked twice.

D. System that used RFID,GSM and Biometrics:

In paper [4], the author has implemented multi-stratum levels of security. At initial setup of procedure, the information is manipulated as the following data is not clear by encapsulation process. While using RFID cards if the card is near the RFID reader at a close range data retrieval is done where the information goes to the micro-controller. So it compulsory that at the 1st level of security biometrics is done. In biometrics the user has to first place his thumb on the scanner where the fingerprints have to match it with the stored template, only then next level of authentication is processed in the system.

If not the system will display a message 'INCORRECT'. If this process does not work the user has to show his RFID card with has a unique encapsulated code in order to recognize the user's identity. Improper use of card, so as to access the system will lead to beeping of buzzer and the LCD will notify a message. After the 2nd level of authentication is being approved, the system will generate an SMS to the users registered number so as to keep the user enrolled. As multi-stratum is there, it is clear that there will be no fraud in the system.

III. FUTURE RESEARCH DIRECTIONS

The main aim of this paper is to provide the guidelines to improve the authentication system. The outlines are given below:

- Train the system in such a manner that it determines the authentication in a more efficient and precise way with minimum error rate.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

- Achieve 100% accuracy in predicting the unauthenticated user with the help of above approaches.
- Include new and more improved authentication system.
- Design a system which will work with both offline and online.

IV. CONCLUSION

Now-a-days PIN code, RFID, Biometrics and password are individually being used for the authentication process which has become the weakest point of the system as it is more vulnerable to attacks by the Hackers. the problem with this system is the use of single factor authentication.
It cannot be recommended to have a multi layer with the same technology so a multifactor authentication can be used by combining various authentication systems. This proposal appears to demonstrate a better authentication by a web application because it can validate two factors.
It makes necessary for a valid user to input the correct combination of the authentication system for successful login into the system. Hence the use of both factors has possibility to enhance the security level in an access control system.

REFERENCES

[1] Chiou Liou, G. Egan, 1. Patel and S. Bhashyam, "A Sophisticated RFID Application on Multi-Factor Authentication" IEEE Eighth International Conference on Information Technology, pp. 180-185, 2011.
[2] R.Ramani, S.Valarmathy, S.Selvaraju and P.Niranjan," Bank Locker Security System based on RFID and GSM Technology", International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012
[3] Bhalekar Swati D., Kulkarni Rutuja R., Lawande Akshay K., Patil Varsharani V," Online Ration Card System by using RFID and Biometrics", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 10, October-2015
[4] Anooshmita Das, Manash Pratim Dutta, Subhasish Banerjee, C. T Bhunia," Cutting Edge Multi Stratum Secured Electronic Voting Machine Design with Inclusion of Biometrics RFID and GSM Module", 6th International Advanced Computing Conference.
[5] Sandhya Konatham, Bhamini Surya Chalasani, Nikita Kulkarni, Tarik El Taeib," ATTENDANCE GENERATING SYSTEM USING RFID AND GSM" Dept. of Computer Science University of Bridgeport, CT, USA..
[6] J. Basilio-Ramirez, H. Perez-Meana, V. Ponomaryov," Multifactor Authentication System Based on Biometrics and Radio Frequency Identification" 21-24 June 2016, Kharkiv, Ukraine.
[7] Ankush Vishwanath, Basappa Yelappa Haibatti, Pavan Krishna Kotekar, Rakesh kumar T S, Sandesh A, Shreyas M Belavadi,Sudarshan Patil Kulkarni , "RFID and GSM based three Level Security System "2013 Texas Instruments India Educators' Conference.
[8] Gyanendra K Verma and Pawan Tripathi, " A Digital Security System with Door Lock System Using RFID Technology", International Journal of Computer Applications (0975 – 8887) Volume 5– No.11, August 2010