Secure Authentication System

Shruti Vaishnav[1], Sneha Sunil[2], Ullas D G[3], Vishnu K Rao[4], Mrs K Panimozhi[5]

1,2,3,4 (IV year B.E., Department of CSE, BMS College of Engineering, Bangalore.)
5(Assistant Professor, Department of CSE, BMS College of Engineering, Bangalore.)
BMS College of Engineering, India

Abstract:*Security is very important in today's world. A secure authentication system is one which is one which enables efficient monitoring and verification of user entry. In our proposed system, we aim to provide dual authentication of the user by means of both RFID as well as fingerprint authentication. The access control mechanism is provided with a magnetic door lock.*
Wireless communication is enabled through the use ZigBee and Wi-Fi modules in combination with a Raspberry Pi computer. Finally for the purpose of monitoring the system, a camera will be used to capture images of the user as and when the system is accessed.

Keywords: *Authentication, RFID, Fingerprint, Raspberry Pi.*

I. Introduction

Security is defined as the state of being protected or safe from harm. Systems in the modern world need to be made secure. They also need to be protected from unauthorized access. This is where authentication comes into the picture. A secure system will need a proper authentication system to provide proper access control so as to prevent people from unlawfully accessing a particular system or location. The use of authentication systems covers a wide range of applications. They can be used in offices and schools for attendance management, military institutions for protecting confidential documents, ATM systems for security, colleges for safe storage of examination papers, courts of law for secure storage of court transcripts, etc.

There are various types of devices and methods that can be used for the purpose of authentication. Some devices like NFC(near field communication) cards, RFID(radio frequency identification) tags and smart cards are pre-programmed with certain unique data such as employee identification numbers, encrypted keys, passwords, etc.
These can be used to provide a form of monitoring and verification along with access control when used at chokepoints. This is because the users will have to pass through that particular chokepoint or checkpoint in order to access their objective.
Another form of verification or authentication would be the use of biometrics. This is a system where a user is authenticated by means of the unique features of the human body. Some of these systems would be fingerprint sensors which authenticate users by their fingerprints, face recognition software distinguishes between users based on their facial features, retina scanners verify users by scanning their retinas, hand geometry scanners, voice prints, etc.

RFID or radio frequency identification [1] is a type of technology where data is transferred in the form of radio waves between a tag and a reader. The tags are basically of three types:-
i) Passive: These tags have no power source of their own and develop an electromagnetic current in their coils when they come in range of a RFID reader.
ii) Semi-Passive: These tags do have a power source which keeps their chip powered at all times but do not power the antenna.
iii) Active: These tags have a power source and use it to power both the microchip as well as the antenna.
As a result of this active tags have the largest range but the passive tags have the longest life-span.
Data is stored on the RFID tags using the RFID writer and this data can then be accessed using the RFID reader.

Fingerprints are unique among human beings and provide a form of built-in authentication of a person's identity. Therefore we can use this concept of uniqueness in an authentication system to verify that a user is actually who he purports to be. A fingerprint sensor [2] uses the concept of total internal reflection in a prism to capture the image of a person's fingerprint and generate a unique ID for said fingerprint to be used in the process of authentication at a later stage.

Magnetic door locking mechanisms are very useful in implementing secure entry points to a particular locale.
They vary in size and strength from micro (1220N) to midi (3600N) to shear (8900N) of holding force. Different size locks can be used for different applications as the situations demand. They can work in either fail-safe modes(to protect people) where the lock will fail in the event of a power outage or fail-secure modes (to protect property) where the lock does not fail in the event of a power

outage, it does this with the help of a cylinder mechanism (as in traditional locks) which keeps it locked during power outages.

ZigBee technology operates under the IEEE 802.15.4 standard. It is mainly used for low power personal area networks (PANs). It traditionally supports star, tree and generic mesh networking topologies. If there are many ZigBee devices, data can be bounced from one device to the other to increase its range. It usually works in the2.4GHz frequency band and supports a data rate of 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band).
It can be used for a variety of applications like home automation systems, door locking mechanisms, smart energy systems, telecommunication systems, etc.

Wi-Fi(wireless fidelity) technology operates under the IEEE 802.11 standard. It has three other parts namely the 802.11a,802.11b and 802.11g protocols. 802.11b and 802.11g work under the 2.4GHz band whereas the 802.11a works in the 5GHz band. Wi-Fi enables devices to connect to a wireless LAN network (WLAN). The 802.11b and 802.11g networks can have a range of around 100m with a standard antenna. We can use Wi-Fi to send or transfer data across a WLAN to whichever device needs the data. 802.11g and 802.11a provide a transfer rate of 54Mbits/s whereas 802.11b provides a data transfer rate of 11Mbits/s.

The next part i.e. section II deals with the different existing authentication systems, section III deals with our proposed system for a secure authentication system, section IV, V and VI deals with the conclusion, acknowledgement and references respectively.

II. EXISTING WORK

There are and have been many authentication systems in the world. They each provide the security, verification and monitoring needed in their own way. This section will shed some light on some of these systems and show their working and other implementation features.

To start with, an attendance system has been implemented using passive RFID chips and an RFID reader [3]. The reader was placed in a fixed location and whenever a chip came within range of the reader, a current was induced in the card and it sent an acknowledgement signal with the unique identifier code of the student. Also a single reader was able to identify many numbers of chips within a short period of time. A graphical user interface(GUI) was also used to produce an automatic system which gives better performance than the traditional pen and paper based systems. Each individual tag referred to the each user's unique ID and the system used Bluetooth for communication. One of the drawbacks of this system was that it provided no way of monitoring as to whether the student actually came to class or not.

A system was also developed for authenticating transactions with an ATM [4]. It used the RFID technology in conjunction with using LPC2148 as a series controller of ARM7 for unique identification of the user with a low frequency RFID tag. First the user has to scan his RFID tag upon which he is prompted to enter his unique PIN(Personal Identification Number), then a Transaction Authentication Code (TAC) which is a 4-digit code is forwarded to the user's cell phone using GSM. The TAC is different for every transaction. The user will have to register his phone number with the bank at the time of his joining. This system provides a useful additional layer of security but is complex with the addition of a GSM module.

A final system using RFID was developed to maintain the attendance of students in an educational institution.
It was simple and effective. The components it used were RFID tags and reader. The software used for database creation were VB.net and MySQL 2008. The system worked as follows. The students were made to pass through a certain strategic chokepoint wherein the RFID tags came within range of the reader. The student's details were extracted from the card and the database was updated with their attendance records. The students and faculty could then access these records by means of an easy GUI interface. The problem with this system was that it had a very low level of security [5].

Another technique was the use of smart cards for the purpose of user authentication. A smart card is a plastic card with a built-in microprocessor. It is usually used for financial transactions.
Using smart cards a voting system was proposed [6]. This system consisted of three parts, the online vote capturing phase, instant online counting phase and result declaration phase. A secret password was given to each user when he or she registered for the voting process. The voter would first approach the voting terminal and insert their smart card into it. They would then be prompted to enter the secret voter card ID(VID) that was provided to them. Along with this an appropriate biometric system was also used for verification purposes. This enables voters to cast their vote securely and since the process is online, it allows for quick and efficient counting of votes and faster declaration of results. The system provided confidentiality and

security to the entire process of elections. This process however does not seem feasible on a large scale basis.

Another scheme of providing authentication with smart cards is to protect a server in a network from malicious remote users in distributed systems. This authentication scheme consisted of three phases and involves a server and anuser [7]. The first phase was a registration phase where a smart card containing personal details of the user was given to the user. This was for the purpose of authentication later in the process. Once the frist phase is completed, the user can perform the next phase i.e. the log-in phase as many times as needed. Successful login only occurs when the password entered by the user is correct and his smart card is valid. This scheme therefore provides a two level authentication scheme (password and smart card). The last phase is the password changing phase. Here the user can freely change his password and the information will be re-written on his smart card as well. A disadvantage of this process would be that the smart card may not be able to carry out heavy computations and so some schemes use pre-computation phases to speed up the process. This technique is also susceptible to t dictionary attacks wherein the attacker tries every word in a password dictionary to hack into the user's account provided he somehow gets a hold of the user'ssmart card or manages to forge a new smart card with the user's details.

Near Field Communication (NFC) technology may also be used for the purpose of authentication. NFC works on the principle that two devices usually portable ones like smart phones can communicate with each other when kept within 4cm of each other. A system for authentication in smart phones was developed using this technology [8]. Here two smart phones were kept beside each other and the user slides his/her finger across the screen of both of the phones. The phones then extract the feature values from the movement on each screen to authenticate each other. When the phones are in the same near field, the system generated the same cryptographic key for them both. This key can then be used by another higher level system to communicate confidentially. These upper systems need not care about how the near field communication was carried out and can just operate on the cryptographic key generated by the phones. The user is asked to swipe across the two phones' screens multiple times and the uses the generated correlated information to verify the smart phones. This system can be easily implemented in technology that already uses near field communication. This is a sort of light-weight system which cannot be used for systems that need higher levels of security.

Another method of monitoring was implemented using an Android application [9]. This was an attendance monitoring system developed for the office environment. It provided a system of monitoring of the employee location throughout the office and maintained records of where and when employees accessed which areas of the office. It follows client-server architecture. Every employee is given a unique identification number by the office. This number along with other information is stored on the employee's smart phones, tablets, etc. The employee is then required to install the required APK files on his android device and his GPS (global position system) must be activated. This entire system hinges on the GPS being turned on and will not function without it. When the employee enters the office, the application automatically connects to the office network via the internet and makes a note of his login time. The system keeps track of his location by monitoring the different places he visits using the GPS. When he leaves the office, the central server is sent a notice which then makes a note of his employee ID and logout time. The major drawback of this system is the fact that it requires every employee to own a smart phone or any other android device and also that the GPS and mobile data has to be permanently on while he is in the office campus. This would drain the power sources i.e. batteries of the devices quickly.

A different take to this problem of authentication is provided by means of a graphical password system [10]. This system follows one of two methods. In recognition based systems the user is required to identify an image or a set of images he had selected previously in a registration stage. These systems are also called cognometric or search metric systems. The user is first expected to select and memorize images during the registration stage and during the login phase, he is again presented with those images wherein he has to select the correct images among the decoys that are also presented. But these systems are not acceptable replacements for password systems. The other type of graphical password systems is the recall based systems wherein the user has to reproduce a image he/she created in a previous registration stage. In this system the image is divided into a number of grids and the user is asked to select a few particular grids which will be his password. The user is asked to upload an image of his choosing at the time of registration along with his/her details. This system is however susceptible to people peeking over the user's shoulder and seeing which grids he is selecting. To avoid this, the creators of this system have implemented a program which generates a number of randomly moving and clicking mouse pointers which prevents potential "peekers" from figuring out the correct grids.

Moving on to biometric systems, a newer system for attendance monitoring and authentication was implemented using a fingerprint sensor [11]. In this system a fingerprint sensor and an LCD screen was placed at the entrance of every room. As the students entered they placed their finger in fingerprint sensor which identified them and their record was updated in the database. They were then notified of this by means of the LCD screen outside the room. The system is pretty straight-forward and works in this way. First a repository of fingerprint feature sets was created and stored in a database. The student's fingerprint was then recorded by the sensor and compared with the templates from the database. If a match was found, the student's information was retrieved from the database and his attendance was recorded and his presence was verified. The system was designed to be online only from thirty minutes of the start of the lecture after which no attendance was marked. Any errors in fingerprint sensing would lead to incorrect matches with the database templates. One of the drawbacks of this system was that the students had to form long queues and wait for their fingerprints to be scanned. They also had to wait for the LCD screen to notify them as to whether they had been correctly marked.

Another fingerprint authentication system [12] used algorithms to acquire and test unique features in the user fingerprints. The main features they used were ridge bifurcations and ridge endings. A ridge bifurcation is when a ridge in the fingerprint divides into two other ridges and a ridge ending is when a ridge in the fingerprint ends abruptly. This system has four main steps. The first is acquisition where a live scan fingerprint of the user was acquired i.e. fingerprint image got without first imprinting it on paper. Then the fingerprints were represented in the appropriate format (e.g.Greyscale). Then the feature extraction step is carried out whereby the ridge bifurcations and the ridge endings were noted down, and in the final step matching was carried out between a test and a reference fingerprint and the verification may be reduced to a pattern matching problem. In the ideal case the system would just count the number of "spatially matching pairs" between the two images.

Finally another authentication system was developed using face recognition [13]. This system integrated the face recognition technology with personal component analysis (PCA) algorithm. A log for user clock-in and clock-out is also provided. Its main components were Open source computer vision library (OpenCV) and Light Tool Kit(FLTK). The user stood in front of a camera at a distance not more than50cm and his photo was taken as input to the system. Extraction of the frontal face profile was carried out. This image was converted to grey scale and stored in the repository. The Principal Component Analysis (PCA) algorithm is executed on this image and then the generated Eigen values are stored in an xml file in the database. When a user's face is scanned for recognition, the frontal face is again extracted and Eigen values are again calculated for this image using the PCA algorithm. These values are then compared and matched with the stored data for the closest match possible. This system has the drawback of being very complicated as it involves digital image processing on a larger scale and may also be a bit time consuming if done in a real time system.

TABLE I: ADVANTAGES AND DISADVANTAGES OF EXISTING SYSTEMS

System	Advantages	Disadvantages
A Lightweight System to Authenticate Smartphones in the Near Field without NFC Chips[8]	• Simple human finger movement is used achieve near field authentication. • The simplicity of the movement makes system more users friendly and saves a user's learning time.	• This system provides authentication only within few centimetres • Two smartphones are in near field, the system assigns the same cryptographic key to both.
Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems[7]	• This system is secure against active attacker. • The analysis has shown that the scheme is secure against offline-dictionaryattack with the Smart card.	• If the smart card is damaged, problems will arise in the authentication process.

Smart Attendance System[5]	• It is quick and easy to implement. • In this System, Smart Attendance System using RFID can replace the manual system that transformation of information can be delivered without a hitch.	• Verification of records is absent. • Smart Attendance System one of the major drawback is securing the system is very low so this method can't be used in real world application.
A smart location based time and attendance tracking system using android application.[9]	• Tracking of employees is easier using this system. • Accurate login and logout time.	• Every employee need to have an Android phone. • High power consumption.
Graphical Password Authentication System[10]	• In theory, human beings remember pictures more easily as when compared to text passwords. • This system implements effective means of preventing over the shoulder "peeking" at the user's password.	• Implementation of this system is complex and authentication of system takes time because this system uses both image and text words. • If there are fewer grids in the system, one can easily predict the pattern. If we increase the number of grids then it is difficult for the user to remember the pattern.
Development of Academic Attendance Monitoring System Using Fingerprint Identification[11] And An Identity-Authentication System Using Fingerprints[12]	• It provides efficient biometric verification. • It is reliable, secure and replaces traditional pen and paper base system.	• Time consuming to secure the system. • If there is any wound to the finger then it might not allow to authenticate system.
Study of Implementing Automated Attendance System Using Face Recognition Technique[13]	• The system provides an accurate login and logout time maintenance system as well as authentication.	• System is complex and time consuming.

III. PROPOSED SYSTEM

In this section, we will present our secure authentication system. The components which we will use are fingerprint sensor, RFID reader/writer module as well as RFID tags, a ZigBee module along with a magnetic door lock to provide the access control. Finally we require a Wi-Fi module to send the collected data to a centralized data base. We will use MySQL to create and maintain our database. A Raspberry Pi computer will be used to integrate all of these modules into one system in an efficient manner.

The first phase of our system is registration. In this phase all the valid user's information (username, user_id) will be inserted into the database. A unique number generated for the fingerprint and image of the user will also be saved in the database. The next step would be issuing a RFID card to each user. Second phase is the authentication phase.

Here the user needs to scan his RFID card. Once it is detected, the user inputs his fingerprint. The verification is done by comparing the generated fingerprint value with the stored value in the database. If it matches, the camera captures an image of the user and stores it in the database. Once all the authentication process is done, the magnetic door lock will open.

We stated the process of identifying a valid user in the above paragraph. Now we are going to explain what happens if an unauthorized person tries to access the system. If the RFID tag fails to scan more than three times then image of the person will be captured and stored in the database for future use. The system will shut down at the same time. If RFID is scanned but the fingerprint fails to match

even after three attempts, an image is captured, stored in the database and the system is shut down.

Figure 1 shows the working of our system.

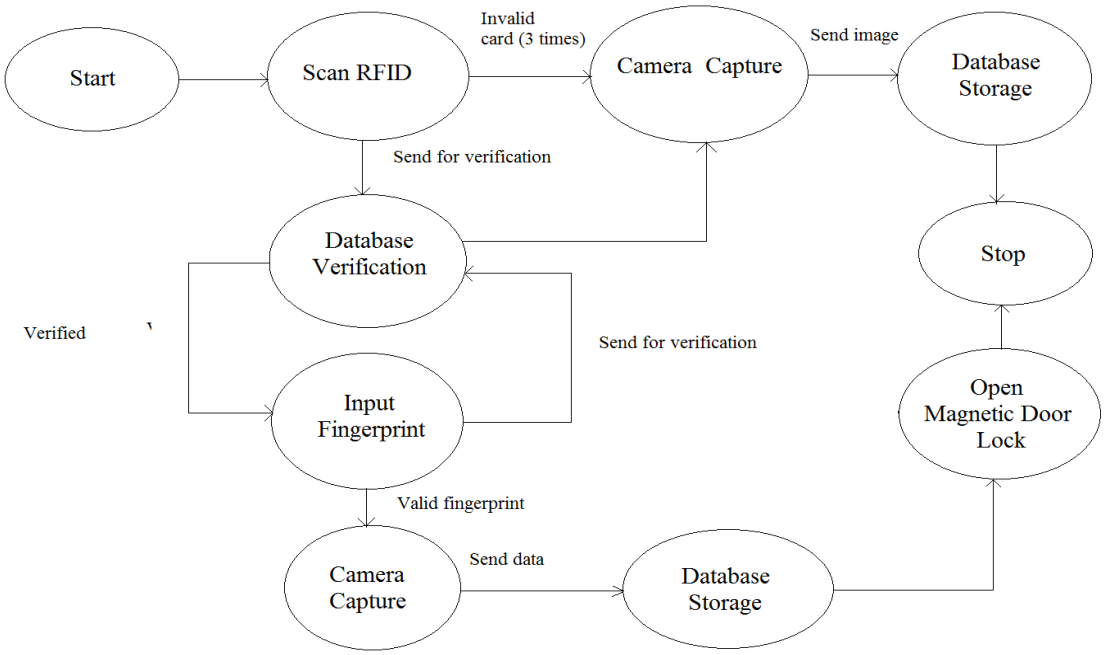

Figure 1 Secure Authentication System Methodology

IV. CONCLUSION

We have mentioned the importance of system authentication process in everyday life. With our system we will try to solve the existing problem of authentication by providing RFID tags. For further validation, we have included fingerprint module, thus providing dual authentication. For the purpose of security, we have included magnetic door lock. Monitoring is done through image capturing. This model helps us solve the problem of access control. By doing this project we wish to create a safe and secure authentication system which can be used in a variety of locations. We also aim to improve our skills and knowledge in the field of IoT enabling technologies.

V. ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the Technical Education Quality Improvement Programme [TEQIP-II] of the MHRD, Government of India.

REFERENCES

1. ChristophJechlitschek "*A Survey paper on Radio Frequency Identification (RFID) Trends*" 2013.
2. Future Electronics "*Advanced Fingerprint Module for Arduino"*.
3. RiyaLodha, Surchi Gupta, Harshil Jain, Harish Narula, D.J. Sanghavi College of Engineering,Mumbai-400014, India "*Bluetooth Smart based Attendance Management System",* ICACTA, 2015.
4. Ms.Soniya B. Milmile and Professor Amol K. Boke, Department of Electronics and Communication Engineering, GHRAET, RTMN University, Nagpur, India "*Review paper on Real Time Password Authentication System for ATM",* IJAICT Volume 1, Issue 7, November 2014.
5. PushpaS.Gagare, PriyankaA.Sathe, Vedant T. Pawaskar, Sagar S. Bhave*"Smart Attendance System*", IJRITCC, January 2014.
6. SrivatsanSridharan, Department of computer science, International Institute of Information Technology, Bangalore "*Implementation of Authenticated and Secure Online Voting System*", 4th ICCCNT, July 4 - 6, 2013.
7. Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, Senior member, IEEE and Li Xu, Member ,IEEE "*Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems",* IEEE Transactions on Parallel and Distributed Systems, VOL. 25, NO. 7, July 2014.
8. Lingjun Li, Xinxin Zhao and GuoliangXue, Arizona State University "*A Lightweight System to Authenticate Smartphones in the Near Field without NFC Chips*", IEEE ICC 2013 - Wireless Networking Symposium.
9. Shermin Sultana, AsmaEnayer and IshratJahanMouri, Department of Computer Science and Engineering, Stamford University Bangladesh ,Dhaka, Bangladesh "*A Smart, Location Based Time And Attendance Tracking System Using Android Application*", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol. 5, No.1, February 2015.
10. SayliChavan, ShardulGaikwad, PrathamaParab and GovindWakure, Department of Information technology, MCT's Rajiv Gandhi Institute of Technology, University

of Mumbai, Mumbai, Maharashtra, India *"Graphical Password Authentication System*", IJCSMC, Vol. 4, Issue. 4, April 2015, pg.324 – 329.

11. Tabassam Nawaz, SaimPervaiz, ArashKorrani, Azhar-ud-din, Software engineering department, Faculty of Telecommunication and Information Engineering, University of Engineering and Technology, Taxila, Punjab, Pakistan "*Development of Academic Attendance Monitoring System Using Fingerprint Identification*", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.
12. Anil K Jain, FELLOW, IEEE, Lin Hong, SharathPankanti, Associate Member, IEEE and Ruud Bolle, FELLOW, IEEE "*An Identify-Authentication System Using Fingerprints*", Proceedings of the IEEE, VOL. 85, NO. 9, September 1997.
13. NirmalyaKar, MrinalKantiDebbarma, AshimSaha and DwijenRudra Pal "*Study of Implementing Automated Attendance System Using Face Recognition Technique",* International Journal of Computer and Communication Engineering, Vol. 1, No. 2, July 2012.