Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.3, June 2016 – www.caeaccess.org

Authenticated Wireless Information Display System Using GSM Module

Varun Shukla
PSIT, Kanpur

Ankit Kushwaha
PSIT, Kanpur

Shivam Singh Parihar
PSIT, Kanpur

Shubham Srivastava
PSIT, Kanpur

Varun Pratap Singh
PSIT, Kanpur

ABSTRACT
In the world of data transmission, crowded places like colleges, hospitals, railway stations and various other places are facing the problem of wired notice boards with much complex circuitry which is problematic because one has to present in the office in order to change the information of the notice board. We suggest an authenticated system which can overcome these obstacles. We need to replace all this with a circuit that is prepared with the components like GSM module, a wireless display unit, microcontroller and some other important elements. Here it is important to mention that in a notice board based system authentication is very important which is the major cryptographic goal. Authentication can be achieved by various ways and in this paper we adopt one of the available methods along with the message display system.

Keywords
Authentication, Security, Wireless Communication, GSM (Global System for Mobile communication), Cryptography

1. INTRODUCTION
GSM came in existence in early 80's by European Telecommunications Standards Institute. At that time it stands for Group Special Mobile but now it is known as Global System for Mobile Communications. Initially it was used in Finland at early 90s. At present it is a very popular technology and over 200 countries in the world are using this. It has established as a default global standard for mobile communication. Nowadays GSM is used for making calls and sending SMS (Short Message Service) [17]. We use this feature to display information on the notice board then it will be very comfortable for sending information [6][7][8][12][13][19]. Now we display this information through the microcontroller. We program the microcontroller in such a way that it could only display specific information which has been sent by an authenticated user[9][10][11]. We know that a mobile number is unique [3][4]. It is important to understand some basic fundamentals and terminology of cryptography [5]. The input message is called as plaintext and represented by M. The method of securing a message by a method, so that it is not understandable by the external world is known as encryption and represented by E(M). The input encrypted message C=E(M) is known as cipher text. Cipher text can be converted back into a plaintext, M=D(C), is known as decryption. Here it is important to discuss major cryptographic goals [15].

1. Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy.
2. Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.
3. Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.
4. Authentication: This security process is very important during communicating over an insecure channel because an active intruder can use the absence of authentication for his/her own benefits. Authentication is also helpful for the integrity of the safe message. In many environments, it is important that communications between two or more are authenticated which means sender and receiver must trust each other's identity so that communication is done between legitimate sender and receiver [1][2].

There are three methods we can use to authenticate someone [18]:

Use something you have: In this example there can be a card or a key. The main disadvantage is that you can't apply such methods every time because one can forget her or his card anywhere or one can steal that.

Use something you know: All calculations related to the authentication fall into these categories. The advantage of using these calculations is that they can be efficient, and can be extended to the higher calculations and also number of entities by using this. When it is about the optimization of resources one can always look for this approach.

Apart from all this, there are biometrics machines asking for thumb impression and retina detection so it can be utilized for purpose of authentication. Such Authentication requires hardware and one to one interaction which is not possible in some cases and cost is also a matter of great concern. Authentication methods can be used in several other things to

strengthen the authentication and level of protocols. When a user uses one of these methods, then it called as one-factor authentication. Using two techniques together is called as two-factor authentication. We explain this with the help of an example. ATM machine utilizes two factor authentication in cash flow process. For authentication, one have to present the ATM card i.e. "something you have" and enter PIN "something you know" then it starts calculating and grants the permission if PIN is correct. With use of a one-way hash function we can enhance the storing of a password in plaintext on a system. Hash functions works on the methodology of one way trapdoor and produce message digest values. The Insecure channel is vulnerable to eavesdroppers and computations should be strong enough to maintain the cryptographic goals [14]. One kind of problem of authentication works like: In a client-server approach, a user is provided a problem from the server with a prompt for response. This problem comes into a challenge/response unit along with a PIN. This unit gives a response which is a function of PIN, the challenge, and a key is stored within the challenge/response unit. The response is sent back to the prompt from the server. The server keeps the PIN and the key inside the challenge/response unit and perform the same calculation and to verify the response. We use this specific characteristic for authentication which falls on the authentication category "something you have". So here this will directly enhance its security of the message. In this paper the use of some components like Power supply, LED, Buzzer, and Transistor is present. The system utilizes the idea of two party communication i.e. transmission and receiving.

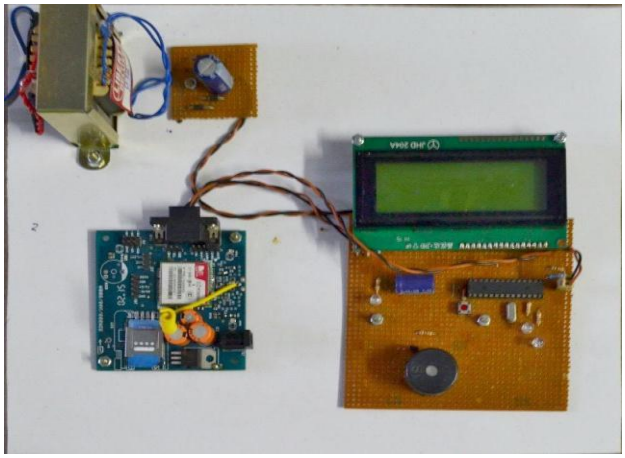

Fig1: GSM based Authenticated wireless information display system

1.1.Description of circuitry

The block diagram of the GSM based wireless notice board is as follows and shown in Fig-2 with the help of various components

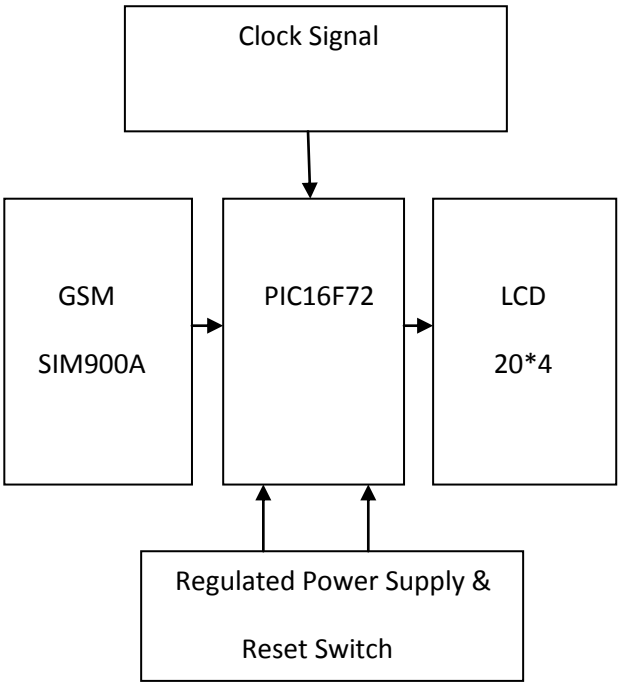

Fig2: Block Diagram of GSM based wireless notice board

Now for better understanding we describe the important components used.

1.2.GSM Module SIM900A

GSM Module SIM900A is dual band module, it operates at 900-1800 MHz. In Asian region SIM900A is widely used. It has baud rate of 9600(symbol/second) and operating voltage is 3.2V to 4.8V. Here in this paper SIM900A is used for receiving text form the authenticated number. After receiving text module will forward the number to microcontroller which will check authorization of the number. It has DB9 on which pin 2 and pin 3 connected to microcontroller's pin 15 and pin 16 for transmission and receiving

Fig3: SIM900A

1.3.Power Supply

Power Supply is the basic electrical source which is required to give supply to various components. We need regulated supply and for this we have DC regulated supply by the help of transformer, Full Wave Rectifier and IC7805.

1.4.Microcontroller PIC16F72

The microcontroller that is used is PIC16F72 and it has 28 pin, 8 bit microcontroller with Analog to Digital converter [16]. It has operating clock of 20 MHz and operating voltage is 2.0V to 5.5V. It has 3 ports which are port A, port B and port C. port A is input port while Port B and C are output ports. Here pin 2-7 is port A, pin 11-18 is port C and pin 21-28 is port B. PIN configuration is given in Fig-4. PIC 16F72 is programmed in this paper in such a manner that it accept SMS only from one authenticated number which is done by initial programmer who is authorized to do so. One can imagine the situation when the principal of the school has the authority to change the information. If someone else try to send the message or try to change the information of the notice board then it will not be allowed for that number to change information and it will directly delete the number. We have used a 4MHz crystal oscillator to give clock to microcontroller. A buzzer is installed at pin 12 which is driven by a transistor.

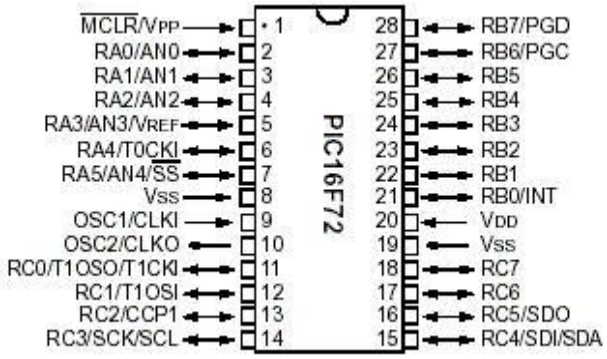

Fig4: PIC16F72

1.5.LCD

LCD is known as Liquid Crystal Display. Here we are using 20*4 LCD (16PIN) which can display up to 80 characters. It has 4 Lines in which 20 characters each. It has supply range of 2.7V-5.5V. Here authentication feature comes into play. The idea is that one number will be authenticated by the coding of microcontroller so if authenticated user sends the information to notice board by sending SMS then only microcontroller will allow to text and it will be displayed on the LCD. If someone who is not authenticated and try to send message then microcontroller will check the number and discard it.

Fig5: LCD 20*4

2. AUTHENTICATION ALGORITHM

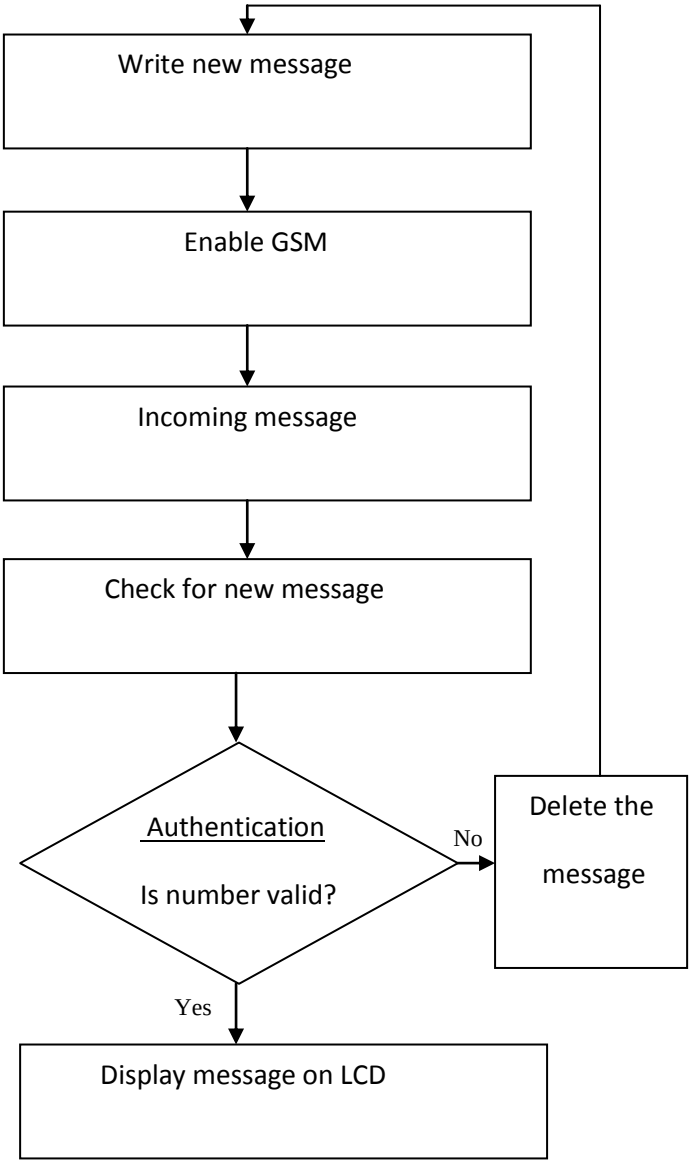

Fig6: Authentication Algorithm

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.3, June 2016 – www.caeaccess.org

3. RESULT AND DISCUSSION

The input interface is as shown in the figure.

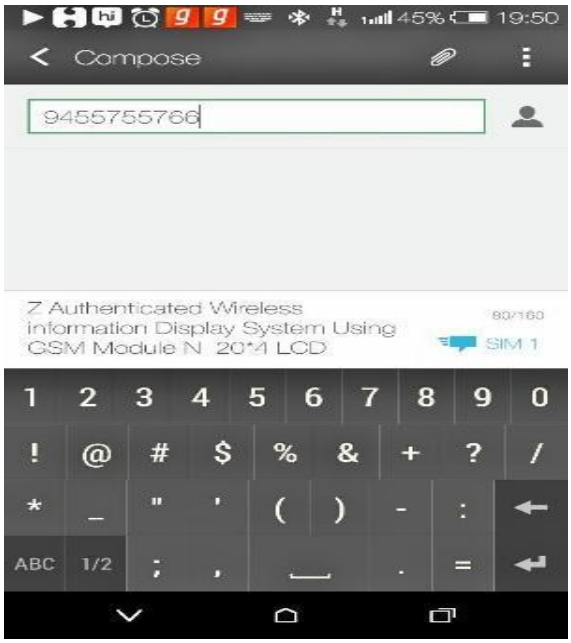

Fig7: Input mechanism

The displayed output is as shown in the figure.

Fig8: Output displayed

3.1.Authentication Process

In the Fig 7 we have sent a message to GSM module to display certain information on the Notice board. When GSM module receive the message then it first send number to microcontroller to check authenticity of the number. If number is found authenticated then message passes through microcontroller and it will be shown on LCD screen as output Fig 8 clearly showing the output of the LCD. If unauthenticated user sends message through it then it will automatically delete the message. In fig 9 it is clear that a number is authenticated during the programming of PIC Microcontroller to change the information of notice board.

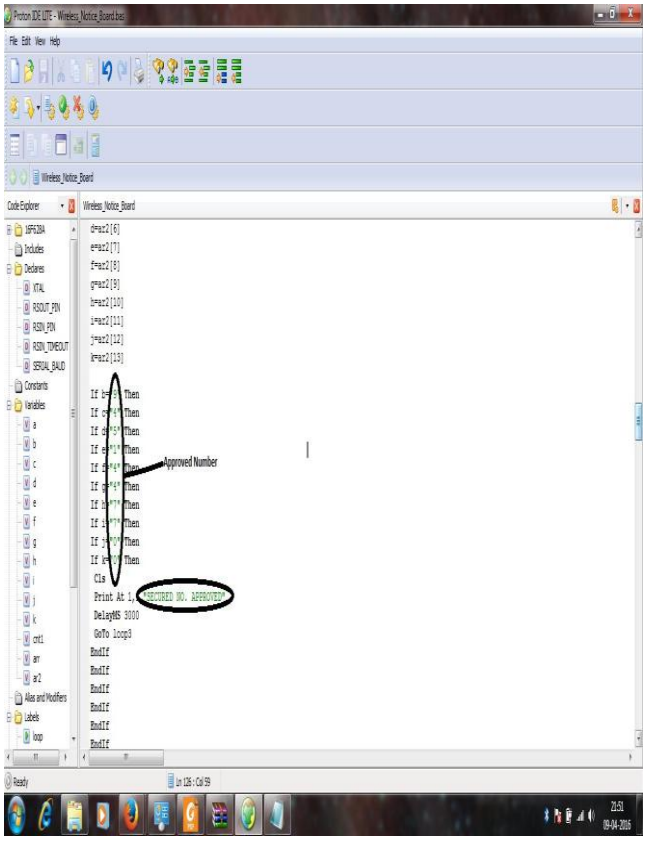

Fig9: Screenshot of Number authentication during programming of Microcontroller

In case number is not authenticated than it will delete the message and print that number is not approved as shown in the fig10 below.

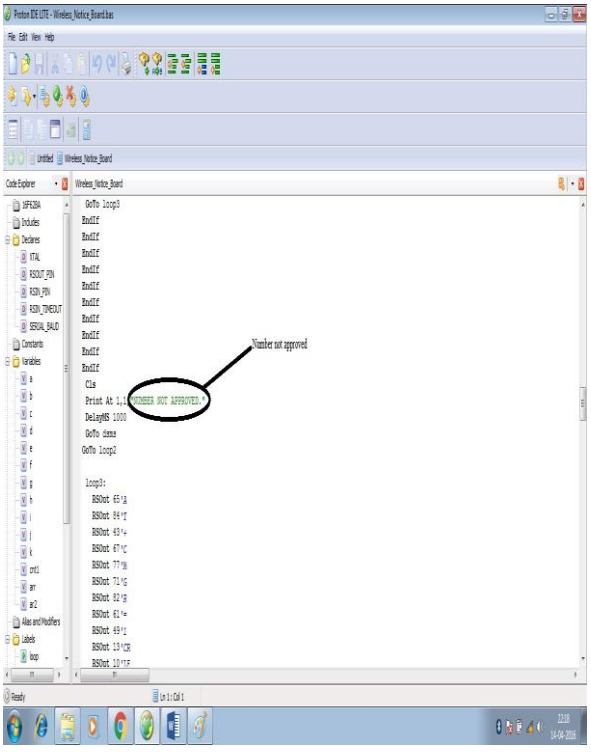

Fig 10: Screenshot of Number is not authenticated.

4. FUTURE SCOPE

This paper utilizes the authentication strength falls on the category "something you have". The future scope is of multiple utility. We can apply cryptographic algorithms like AES, RSA to encrypt the message in order to achieve another cryptographic goal of data security along with authentication. We can add some value addition in the display system like when the notice board doesn't have any message to display, it can show room temperature, date etc. We can also add text reader to speak the message out. The idea of many user authentication can also be applicable that means we can authenticate more than one number so that in the absence of some authority, a deputy can do the same.

5. CONCLUSION

World of Wireless Data Communication is growing day by day and we are looking towards more possible solutions of the problematic situations. We are now more focused towards concept likes authentication, data integrity so we can secure our wireless data communication. If we replace current system with this system then surely it will be very much beneficial in terms of maintenance and data sending. Here we have strength of authentication and cryptography that gives us extra befits in terms of secured data transmission. We can use this system at crowded places like Bus Stations, Airports etc. It will surely enhance efficiency and effectiveness of the system.

6. REFERENCES

[1] D. Balfanz, D.K. Smetters, P. Stewart, and H.C. Wong, "Talking to strangers: authentication in Ad-Hoc wireless networks," in Proc. Network and Distributed System Security Symposium Conference, 2002.

[2] J.Brandt, I.Damga°ard, P.Landrock and T.Pedersen,Zero-Knowledge Authentication Scheme with Secret Key Exchange, J.Cryptology, vol 11(1998), 147-160.

[3] D Dalwadi, N Trevedi and A Kasundra (Articles in National conference on Recent trends in Engineering and technology), INDIA,2011

[4] L Bollen, Eimler S and Hoppe H.U. "SMS-based Discussions Technology Enhanced Collaboration for a Literature Course". In Proceedings of the 2nd IEEE International Workshop on Wireless and Mobile Technologies in Education, 24- 27 May 2004, Germany, pp. 1-2, 2004.

[5] B. A. Forouzan, "Cryptography and Network Security", Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.

[6] C. Peijiang; Jiang Xuehua, "Design and Implementation of Remote Monitoring System Based on GSM," Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on, vol.1, no., pp.678, 681, 19-20 Dec. 2008

[7] Cooperation in wireless networks : principles and applications- FHP Fitzek, MD Katz Springer , ISBN 978-1-4020-4711-4,2006

[8] C.Darshankumar Dalwadi, Ninad Trivedi, Amit Kasundra, "WIRELESS NOTICE BOARD Our RealTime Solution" National Conference on Recent Trends in Engineering & Technology, May13-14, 2011

[9] J.Datta, Chowdhuri, S.; Bera, J., "GSM based condition reporting system for power station equipments," Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on , vol., no., pp.256,259, Nov. 30 2012-Dec. 1 2012

[10] GSM and Personal Communications Handbook-SiegmundRedl - MatthiasWeber- MalcolmW. Oliphant Artech House Publishers, 01 May 1998

[11] GSM Telecommunication standards-, European Telecommunications Standards Institute,April 2000 2nd edition

[12] C. Gehrmann, C.J. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, No. 1, pp. 29-37, 2004.

[13] GuifenGu; GuiliPeng, "The survey of GSM wireless communication system," Computer and Information Application (ICCIA), 2010 International Conference on , vol., no., pp.121,124, 3-5 Dec. 2010

[14] W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, New Jersey, USA, 2004.

[15] A. J. Menezes, P. C. V. Oorschot, & S. A. Vanstone, "Handbook of Applied Cryptography", 5th edn., CRC Press Inc., USA, 2001.

[16] Microchip PIC16F72 data sheet , 28 pin 8 Bits CMOS flash microcontroller with A/D converter

[17] M Samiullah, N S Qureshi," SMS Repository and Control System using GSM SMS technology", Europen Journal of Scientific Research 2012

[18] V.Shukla,A.Chaturvedi,N.Srivastava,"A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography", Communication on applied electronics (CAE), ISSN:2394-4714,volume-3,No-3,Oct-2015,pp 16-21

[19] Jianming Zhu, Sch. of Comput., Xidian Univ., Xi'an, China JianfengMa"IEEE Transactions on Consumer Electronics" (Volume:50 , Issue: 1)ISSN :0098-3063