ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

Gesture and Touch Screen based password for more secure authentication with wireless communication

Rose George Kunthara [1], Rincy Merin Varkey [2], Noyal Mary James [3]

Assistant Professor, Department of Electronics and Communication, St Joseph's College of Engineering & Technology, Palai, Kerala, India[1, 2]

PG Scholar, Department of Electronics and Communication, St Joseph's College of Engineering & Technology, Palai, Kerala, India[3]

Abstract: User authentication is a fundamental component in network communication. There are various types of authentication systems such as textual passwords, smart cards or tokens, biometric authentication etc. But the current authentication systems suffer from many weaknesses. This paper presents a multifactor authentication scheme. Here we are having two levels of security. In the first security level the user have to provide a gesture after wearing a 3D glove unit. The second level of security consists of a touch screen for drawing the pattern. The communication between these two levels is wireless, using Zigbee technology. The security analysis of this method shows that this scheme is sustainable to the vulnerability attacks during authentication process.

Keywords: authentication scheme, textual password, shoulder surfing

1. INTRODUCTION

The increase of computer usage has given rise to many security concerns. One major security concern is authentication, which is the process of validating who you are to whom you claimed to be. In authentication process, the originator of the communication and the respondent transacts some identification codes of each other prior to start of the message transaction. Several methods have been proposed regarding the authentication process from time to time[16].

The most common authentication system is textual password. Here the user pick passwords that are easy to remember and enter this during authentication. The vulnerabilities of this method have been well known. One of the main problem is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. Many authentication systems, particularly in banking, require not only what the user knows but also what the user possesses (token-based systems)[4]. However, many reports have shown that tokens are vulnerable to fraud, loss, or theft by using simple techniques. In order to avoid these problems Biometric payment system was implemented. The main advantages of this system is its uniqueness, increased security, reduced fraud etc . One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic[2]. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text. The disadvantages are login process is too slow and it takes more storage space.

From the above observations we came to know that the existing authentication schemes suffer from many weakness.. Using more than one password scheme can ensure authentication confidentiality, reliability, integrity and security. So here we present a multifactor authentication scheme. The system is designed in such a way that there are two levels of security. First is a gesture unit and the other is a touch screen unit. The advantages of both gesture and pattern schemes is utilised here.

The remainder of this paper is organized as follows: Section II discusses related works. Section III describes about proposed system. Section 1V shows the results of the project . The conclusion is presented in the last section.

2. LITRATURE SURVEY

The most common authentication method is the textual password authentication system. In [14] Kue et.al had a study on human selection of mnemonic phrase based password. In this paper, they hypothesize that users will select mnemonic phrases that are commonly available on the Internet. Mnemonic passwords could become more vulnerable in the future. From the above observations we can see that using textual password alone is not so efficient. They are vulnerable to many attacks. Many authentication systems, particularly in banking,require not

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

only what the user knows but also what the user possess, ie, token based and smart card system. In [10] Santhosh et.al developed a secure dynamic authentication scheme for smart card based networks. In [11] Sarjie et.al proposed a Smart card based secure authentication and a key agreement protocol . But the main disadvantages of smart card based authentication schemes are, they are vulnerable to fraud, loss or theft.

Biometrics systems and mainly multi-biometric systems provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy. Several systems were introduced. In [2] Chowdhury made a paper on Revolution in authentication process by using biometrics. In [3] Dileep et.al did a survey on biometric finger prints. In this paper they have concluded that fingerprint payment system is used for various kinds of payment system instead of the tension of cards to place with them and to memorize theirs difficult passwords. One of the main drawback is its intrusiveness upon users personal characteristics. It is expensive, identification is slow and unreliable.

To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. Because simply adopting graphical password authentication also has some drawbacks, so in [16] Ziran et.al proposed some hybrid schemes based on graphic and text were developed. In this paper, they proposed a stroke-based textual password authentication scheme. In [5] Huanyu et.al proposed a scalable shoulder –surfing resistant textual password authentication scheme. In this paper, they propose a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS).As an extension to that in [9] Shakir et.al developed a S3TFPAS: Scalable shoulder surfing resistant textual-formula base password authentication system.

In [4] Fawaz developed a three dimensional password for more secure authentication. It is a multifactor authentication system, which creates a 3d virtual environment.

Here we have proposed 3 dimensional and touch screen based password and the results have been presented.

3. PROPOSED SYSTEM

In this section, we present a multifactor authentication scheme that combines the benefits of two authentication schemes. We have to satisfy the following requirements.

- Simple Low Cost design
- Efficient Encryption Algorithm
- High level security
- Efficient use of advanced technology

The system is designed in such a way that there are two levels of security. The Gesture unit is the first level of security. It consists of an accelerometer connected on a wearable gloves and a zigbee unit. When the user need to provide the password he/she has to wear the gloves and provide the gesture to unlock the system.. If the 3-D axis provided by the user is correct then the system will go to the next level of security else it prompts with a warning alarm. The communication between these two security levels is done using Zigbee technology.

In the next level of security we are having a touch screen which is mounted on top of a Graphical LCD. The GLCD will
display matrix shaped boxes where we have to draw the pattern. If the entered password is correct the access will be granted or else the access is denied and the system will go back to the first security level.

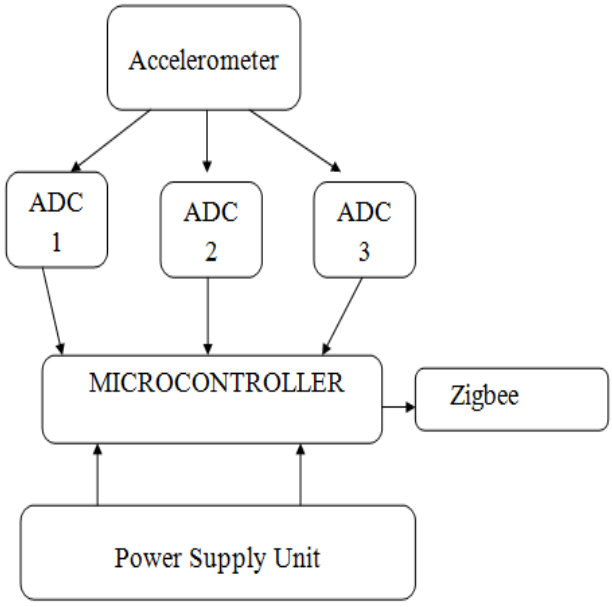

Fig1:Gesture side

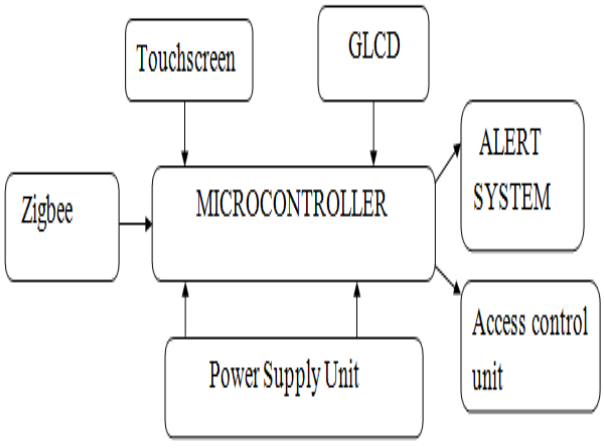

Fig2:Pattern side

The 3D unit is placed in a Glove and it is communicating with the control unit using Zigbee technology, the gesture

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

shown by the user will be transferred to the control unit using Zigbee.
This communication can be later used for to and fro communication between control unit and the wearable glove unit for implementing next higher level of security.

3.1 BLOCK DIAGRAM DISCRIPTION

3.1.1 Power Supply

The ac voltage, typically 220V RMS is connected to a transformer, which steps down the voltage to the desired level. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator and filter circuit removes the ripples. Here in our project the power supply section consist of a Voltage Regulator (7805),Capacitors 100uf 25 v (Electrolytic) , .1uf (Ceramic).When we plug a 12 v to the DC jack, the Regulator will Adjust it to 5v so that the controller (Renesas) and related modules will work fine. The capacitors are provided such that it should filter out the unwanted noises from the supply.

3.1.2 Micro Controller

A digital computer having micro-processor as the CPU along with memory and I/O device is called a micro-controller. A micro controller is essentially designed for a dedicated application(s) and hence it is called 'dedicated microcontroller'.
Here in this project the device is powered by Renesas's 16bit R8C/25 family micro-controller. Renesas is the world's third largest micro controller manufacturer. The R8C Tiny series microcontrollers belong to the popular M16C platform. It has been specifically designed to provide the lowest-cost system solution for general-purpose applications. These MCUs are fabricated using a high-performance silicon gate CMOS process, embedding the R8C/Tiny Series CPU core, and are packaged in a 52-pin molded-plastic LQFP. The R8C/25 Group has on-chip data flash (1 KB x 2 blocks), 64KB ROM and 3 KB RAM. The 16-bit CPU can be directly clocked at 20 MHz and execute 89 instructions, each configurable with multiple addressing modes .

3.1.3 Accelerometer

An accelerometer is an electromechanical device that will measure acceleration forces. The ADXL335 is a small, thin, low power, complete 3-axis accelerometer with signal conditioned voltage outputs. The product measures acceleration with a minimum full-scale range of ±3 g. It can measure the static acceleration of gravity in tilt-sensing applications, as well as dynamic acceleration resulting from motion, shock, or vibration. The user selects the bandwidth of the accelerometer using the CX, CY, and CZ capacitors at the XOUT, YOUT, and ZOUT pins. Bandwidths can be selected to suit the application, with a range of 0.5 Hz to 1600 Hz for the X and Y axes, and a range of 0.5 Hz to 550 Hz for the Z axis. The ADXL335 is available in a small, low profile, 4 mm ×4 mm × 1.45 mm, 16-lead, plastic lead frame chip scale package (LFCSP_LQ).Rather than using additional temperature compensation circuitry, innovative design techniques ensure that high performance is built in to the ADXL335. As a result, there is no quantization error and temperature hysteresis is very low (typically less than 3 mg over the -25°C to +70°C temperature range).Here in this project accelerometer is attached with gloves to detect gloves position.

3.1.4 Resistive Touch Screen

A touchscreen is an electronic visual display that can detect the presence and location of a touch within the display area. The term generally refers to touching the display of the device with a finger or hand. Touchscreens can also sense other passive objects, such as a stylus. Touchscreens are common in devices such as game consoles, all-in-one computers, tablet computers, and smartphones. There are two types of touch screen capacitive and resistive.

A resistive touch screen is constructed with two transparent layers coated with a conductive material stacked on top of each other. When pressure is applied by a finger or a stylus on the screen, the top layer makes contact with the lower layer. When a voltage is applied across one of the layers, a voltage divider is created. The coordinates of a touch can be found by applying a voltage across one layer in the Y direction and reading the voltage created by the voltage divider to find the Y coordinate, and then applying a voltage across the other layer in the X direction and reading the voltage created by the voltage divider to find the X coordinate.

3.1.5 Graphic Liquid Crystal Display

The Graphical LCDs are thus used to display customized characters and images. The Graphical LCDs find use in many applications such as video games, mobile phones, lifts etc. .The 128x64 Graphical LCD is divided into two equal halves with each half being controlled by a separate KS0108 controller. Such LCDs (using KS0108 controller) involve paging scheme, i.e., whole LCD is divided equally into pages.Each page can display 64x64 pixels and is controlled by its own controller..Each page has 8 lines numbered 0-7. Each line has 64 positions that contain a 1 pixel wide by 8 pixel tall strip.
A buzzer is used here to provide sound alert for each process.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

4. RESULTS AND DISCUSSIONS

4.1 Gesture Side

This is the first level of security. After wearing the gloves we have to provide the gesture. If the password that we entered is correct there will be a display on the LCD,"PASSWORD ACCEPTED". At the same time there appear matrix shaped boxes on GLCD at the pattern side. If the password entered is wrong the display says that, "WRONG PASSWORD".

Fig3:Password accepted

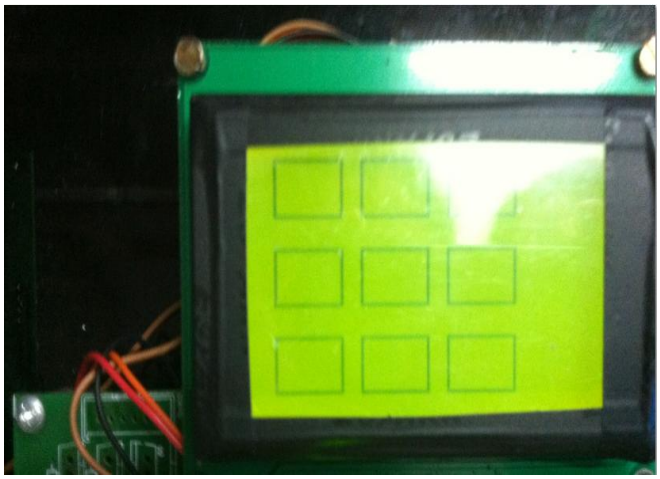

Fig4: GLCD ready to accept pattern

4.2 Pattern Side

This is the second level of security. After entering a correct password in the gesture side, matrix shaped boxes appear on GLCD which is ready to accept a new pattern. Draw a pattern
on the GLCD screen. If the password entered is correct there will be a display on GLCD,"ACCESS GRANTED". If the password entered is wrong there will be a display, "PASSWORD WRONG".

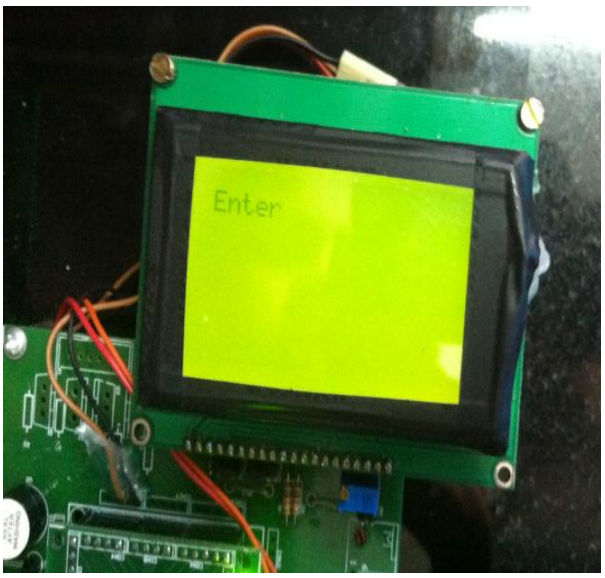

Fig5: Password accepted

Fig6: Access granted

5. CONCLUSION

Current authentication systems suffer from many weaknesses. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Users tend to resist using biometrics because of their intrusiveness and the effect on their privacy**.** It is really challenging to develop a secure authentication system free from all those weakness.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 9, December 2013

So we have developed 3 Dimensional and Touch screen based authentication system. Here we ensure authentication reliability, integrity and security. This is a simple low cost design with an efficient encryption algorithm. This authentication system can be used in places where high security is demanded such as in bank lockers and storage rooms where all confidential files are kept.

REFERENCES

[1] Bandyopadhyay, S.K., "User authentication by Secured Graphical Password Implementation" Information and Telecommunication Technologies, 2008. APSITT.,IEEE,22-24 APRIL ,pages(7 - 12)

[2] Chowdhury, A.," Revolution in authentication process by using biometrics" , Recent Trends in Information Systems(ReTIS),IEEE2011,DECEMBER(21-23),pages(36 - 41)

[3] Dileep Kumar, Dr.Yeonseung Ryu, Dr.Dongseop Kwon," A Survey on Biometric Fingerprints: The Cardless Payment System"Biometrics and security technologies,2008,ISBAST

[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE." Three-Dimensional Password for MoreSecure Authentication", Transactions on instrumentation and measurement,Vol.57.No.9,IEEE September 2008 pages(1929- 1938)

[5] Huanyu Zhao ; Xiaolin Li," A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", Advanced Information Networking and Applications Workshops, 2AINAW '07, Volume: 2,IEEE 2007,pages(467 - 472)

[6] Jaidhar, C.D.; Tapaswi, S.," Highly secured remote use authentication scheme using smart cards, Industrial Electronics and Applications (ICIEA), 2012 IEEE(18 – 2 JULY),pages(1001 - 1005)

[7] Panigrahy, S.K.; Biswal, P.K.; Jena, S.K.," Novel Protocol for Smart Card Using ECDLP", Emerging trends in engineering and technology,ICETET'08,IEEE (16 – 18 JULY),pages(838 - 843) [8] Maghooli, K.; Afdideh, F.; Azimi, H.," A unimodal person authentication system based on signing sound", Biomedicalandhealthinformatics,IEEE2012,EMBS,pages(152 - 153)

[9] Shakir, M. ; Khan, A.A. , "Scalable shoulder surfing resistant textual-formula base password authentication system", Volume: 8 ,IEEE 2010 ,pages(12 -14)

[10] Dr. Santhosh S Baboo and K Gokulraj.," A Secure Dynamic Authentication Scheme for Smart Card based Networks ",International Journal of Computer Applications,2010 by IJCA Journal ,volume11,DECEMBER, 2010

[11] Sood, S.K. ; Sarje, A.K. ; Singh, K.," Smart card based secure authentication and key agreement protocol", Computer and Communication Technology (ICCCT),IEEE 2010,pages(7 -4)

[12] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967

[13] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[14] Kue,Sasha,Lorrie,"human selection on mnemonic based Password",SOUPS,2006 JULY 12 – 14,pages(67 - 78)

[15] Xiaoyuan Suo Ying Zhu G. Scott. Owen," Graphical Passwords: A Survey" Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005),IEEE,(5 – 9)DECEMBER,(pages:10 – 472)

[16] Ziran Zheng, Xiyu Liu, Lizi Yin, Zhaocheng Liu," A Stroke-based Textual Password Authentication Scheme", First International Workshop on Education Technology and Computer Science, IEEE 2009.