Journal of Engineering Sciences
Vol 11, Issue 1, JAN/2020
ISSN NO:0377-9254

CRYPTOGRAPHY BASED SECURED LIFI FOR PATIENT PRIVACY AND EMERGENCY HEALTH CARE SERVICE

[1]D Niharika, [2]Md Ashraf, [3]Dr. D SubbaRao
[1]PG Scholar, MTech, Dept of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, T.S.
dudiniharika@gmail.com
[2]Assoc Professor, Dept of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, T.S.
[3]Professor & HOD, Dept of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, T.S.

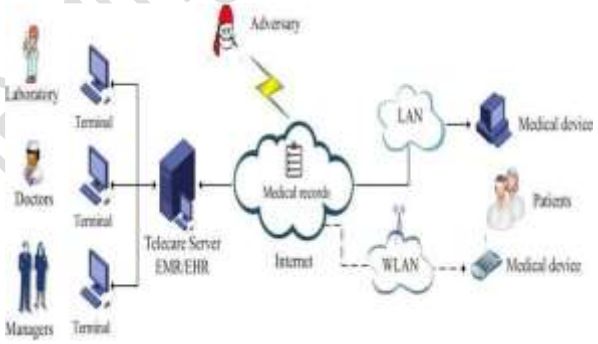
ABSTRACT

Visible light communication (VLC) has attracted a lot of attention in past several years. VLC systems can be used for both communications and indoor positioning. Several designs of VLC systems have been proposed and most of them require central units to control the light emitting diodes (LEDs) in the transmitters to avoid interference at the receiver side. In this paper, we propose a novel multiple access schemes for VLC systems that does not require central unit. The transmitters simultaneously broadcast different information. The receiver can extract the information from the superposition of the received signals from the transmitters. The received power from individual transmitters can also be determined at the receiver so that positioning algorithms can be applied. Simulation results show that our proposed scheme outperforms existing multiple access schemes for VLC systems without central unit.

I. INTRODUCTION

Advances in information technology and environmental concerns boost the rapid development of Electronic Medical Record/Electronic Health Record (EHR) systems, which collect, store, manage and share patient's healthcare associated information. Compared with traditional paper-based method, EMR/EHR provides low cost, high quality and more flexible medical records [1]. Owing to this transmission, Telecare Medicine Information Systems (TMIS) have been deployed to provide healthcare delivery services by accessing

EMR/EHR via the public network like Internet [2]. In a typical medical application scenario of TMIS as shown in Fig. 1, patients submit their healthcare data to a telecare server via wired/wireless medical devices in their home. After receiving the patient's medical records, the doctors perform the diagnosis at their clinical center and then transform the final clinical decisions and treatments to the patients through the Internet. Since the TMIS realizes convenient and efficient healthcare beyond the limitation of geographical distance, it attracts great attention and spreads into the market quickly [3-6].



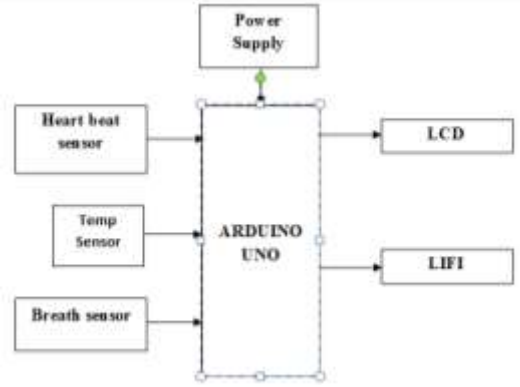
However, the sensitive medical records transmitted over the the Internet are not protected in most TMIS environments, and various attacks could be launched successfully by malicious adversaries. To protect patient's medical records, TMIS based healthcare should satisfy fundamental security and privacy requirements such as authentication, confidentiality, integrity, and user anonymity [7, 8]. As the authentication mechanism can prevent the medical resources from being accessed by malicious attackers and the session key used to encrypt the packets can ensure the confidentiality of EMR/HER, many authenticated key agreement schemes [9-13] have been developed to protect medical records security and preserve patient's privacy. For example, the authentication schemes for HIPAA privacy and security regulations [9-11] were proposed to provide authorization, authentication and key management. The

software solution [12] for sharing and querying of HL7 version 3 clinical documents was presented to provide security for data providers and protect the patients' privacy.

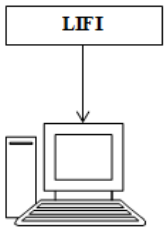
Recently, passwords and smartcards based authenticated key agreement schemes have been studied widely for TMIS [14-19]. However, these schemes have some limitations. Firstly, both smartcards and passwords could be forgotten, lost, stolen or duplicated. Secondly, if the authorized users share their smart cards and passwords with unauthorized users, there is no way for the system to tell who the actual user is. Thirdly, some of these schemes [14-15] require the server to maintain a password table for verification purposes, making them suffers from some possible attacks such as password disclosure attacks, stolen-verifier attacks and server-spoofing attacks. Besides, user's passwords are potentially vulnerable to offline password guessing attacks since their entropy are usually very low. To enhance the security, biometric characteristics are employed as a third factor to design a strong authentication scheme. Since the combination of the three factors can resist guess, forget, stolen, and duplicate issues [20], the three factors-based authentication schemes overcome the weaknesses existing in two-factor schemes. As the three factors provide many attractive properties, several three-factor authentication and key agreement schemes have been proposed for TMIS [21-28].

II. IMPLEMENTATION

BLOCK DIAGRAM



Receiver section:



POWER SUPPLY

The power supply section is the section which provide +5V for the components to work. IC LM7805 is used for providing a constant power of +5V.

The ac voltage, typically 220V, is connected to a transformer, which steps down that ac voltage down to the level of the desired dc output. 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 circuit removes the ripples and also retains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.

ARDUINO UNO

Arduino/genuino uno is a microcontroller board based on the atmega328p (datasheet). It has 14 digital input/output pins (of which 6 can be used as pwm outputs), 6 analog inputs, a 16 MHz quartz crystal, a usb connection, a power jack, an icsp header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a usb cable or power it with a ac-to-dc adapter or battery to get started. You can tinker with your uno without worrying too much about doing something wrong, worst case scenario you can replace the chip for a few dollars and start over again.

TECHNICAL SPECIFICATIONS

Microcontroller	ATmega328P
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limit)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
PWM Digital I/O Pins	6
Analog Input Pins	6
DC Current per I/O Pin	20 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB (ATmega328P) of which 0.5 KB used by bootloader
SRAM	2 KB (ATmega328P)
EEPROM	1 KB (ATmega328P)
Clock Speed	16 MHz
LED_BUILTIN	13
Length	68.6 mm
Width	53.4 mm
Weight	25 g

LIQUID CRYSTAL DISPLAY (LCD)

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on.

A **16x2 LCD** means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data.

The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD.

Fig. 16x2 LCD

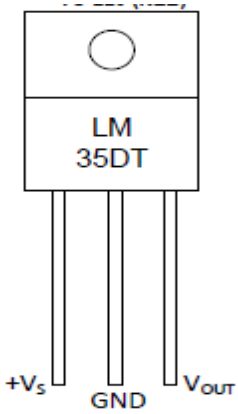
HEART BEAT SENSOR

HEART BEAT is sensed by using a high intensity type LED and LDR. The finger is placed between the LED and LDR. As sensors photo diode or a photo transistor can be used. The skin may be illuminated with visible (red) using transmitted or reflected light for detection. The very small changes in reflectivity or in transmittance caused by the varying blood content of human tissue are almost invisible. Various noise sources may produce disturbance signals with amplitudes equal or even higher than the amplitude of the Heart beat signal. Valid Heart beat measurement therefore requires extensive preprocessing of the raw signal. The new signal processing approach presented here combines analog and digital signal processing in a way that both parts can be kept simple but in combination are very effective in suppressing disturbance signals.

TEMPERATURE SENSOR

Temperature is the most-measured process variable in industrial automation. Most commonly, a temperature sensor is used to convert temperature value to an electrical value. Temperature Sensors are the key to read temperatures correctly and to control temperature in industrials applications.

Temperature sensor (LM35)



A large distinction can be made between temperature sensor types. Sensors differ a lot in properties such as contact-way, temperature range, calibrating method and sensing element. The temperature sensors contain a sensing element enclosed in housings of plastic or metal. With the help of conditioning circuits, the sensor will reflect the change of environmental temperature.

Pin Definition

The definition of gray-scale sensor pin is

1. Signal Output
2. GND
3. Power

LI-FI (LIGHT FIDELITY):

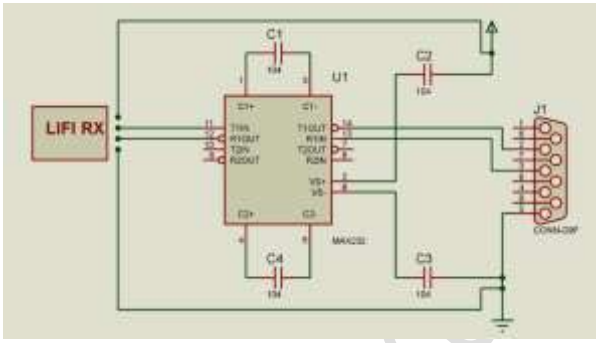
Introduction:

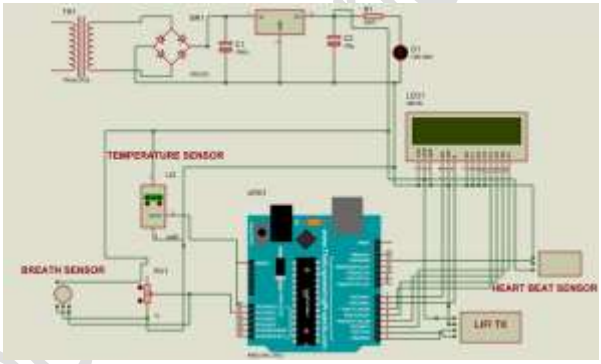
Whether you're using wireless internet in a coffee shop, stealing it from the guy next door, or competing for bandwidth at a conference, you've probably gotten frustrated at the slow speeds you face when more than one device is tapped into the network. As more and more people and their many devices access wireless internet, clogged airwaves are going to make it increasingly difficult to latch onto a reliable signal. But radio waves are just one part of the spectrum that can carry our data.

One German physicist, DR. Harald Haas, has come up with a solution he calls "Data Through Illumination"—taking the fiber out of fiber optics by sending data through an LED light bulb that varies in intensity faster than the human eye can follow. It's the same idea behind infrared remote controls, but far more powerful. Haas says his invention, which he calls D-Light, can produce data rates faster than 10 megabits per second, which is speedier than your average broadband connection. He envisions a future where data for laptops, smartphones, and tablets is transmitted through the light in a room. And security would be a snap—if you can't see the light, you can't access the data.

Li-Fi is a VLC, visible light communication, technology developed by a team of scientists including Dr Gordon Povey, Prof. Harald Haas and Dr. MostafaAfgani at the University of Edinburgh. The term Li-Fi was coined by Prof. Haas when he amazed people by streaming high-definition video from a standard LED lamp, at TED Global in July 2011. Li-Fi is now part of the Visible Light Communications (VLC) PAN IEEE 802.15.7 standard. "Li-Fi is typically implemented using white LED light bulbs. These devices are normally used for illumination by applying a constant current through the LED. However, by fast and subtle variations of the current, the optical output can be made to vary at extremely high speeds. Unseen by the human eye, this variation is used to carry high-speed data," says DrPovey, Product Manager of the University of Edinburgh's Li-Fi Program 'D-Light Project'.

III. RESULTS AND OUTPUT SCREENSHOTS





IV. CONCLUSION

In this paper, we have demonstrated that Mishra et al.'s authentication scheme suffers from various attacks and fails to provide several security properties. And then, we have proposed a three-factor authenticated key agreement scheme by using chaotic map-based cryptography to address these problems. The proposed scheme realizes the protection of medical data transmitted in the open channel and provides privacy protection during the remote diagnosing process, which enables the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis has proved that the proposed scheme can resist various attacks, and performance analysis has shown that the proposed scheme achieves better performance in comparison with other related schemes. Thus, the proposed scheme is more suitable for practical applications in TMIS environments.

REFERENCES

[1] S. Li, C. Wang, W. Lu, Y. Lin, D. Yen, ―Design and implementation of a telecare information platform‖, *J. Med. Syst.*, vol.36, no. 3, pp.1629-1650, 2012.

[2] L. Nguyen, E. Bellucci, ―Electronic health records implementation: An evaluation of information system impact and contingency factors‖, *Int. J. Med. Inf.*, vol. 83, no. 11, pp. 779-796, 2014.

[3] V.L. Patel, J.F. Arocha, A.W. Kushniruk, ―Patients' and Physicians' understanding of health and biomedical concepts: relationship to the design of EMR systems‖, *J. Biomed. Inform.*, vol. 35, pp. 8–16, 2002.

[4] J. Scholl, S. Syed-Abdul, A.L. Ahmed, ―A case study of an EMR system at large hospital in India: challenges and strategies for successful adoption‖, *J. Biomed. Inform.*, vol. 44, pp. 958–967,2011.

[5] C. Esposito, M. Ciampi, G. Pietro, ―An event-based notification approach for the delivery of patient medical information‖, *Inform. Syst.*, vol.39, pp. 22-44, 2014.

[6] P. Accenture, ―Overview of International EMR/EHR Markets: Results from a Survey of Leading Health Care Companies‖, http://www.accenture.com au-en/Pages/insight-electronic-medical-record-survey-summary.aspx, 2010.

[7] G. Perera, A. Holbrook, L. Thabane, G. Foster, D. Willison, ―Views on health information sharing and privacy from primary care practices using electronic medical records‖, *Int. J. Med. Inf.*, vol. 80, no. 2, pp. 94-101, 2011.

[8] J. Hur, K. Kang, ―Dependable and secure computing in medical information systems‖, *Comput. Commu.*, vol. 36, no. 1, pp. 20-28, 2012.

[9] C.D. Lee, K.I. Ho, W.B. Lee, ―A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations‖, *IEEE Trans. Inf. Technol. Biomed.*, vol.15, pp. 550–556, 2011.

[10] W. Ludwig, K.H. Wolf, C. Duwenkamp, N. Gusew, N. Hellrung, M. Marschollek, M. Wagner, R. Haux, ―Health-enabling technologies for the elderly – an overview of services based on a literature review‖, *Comput. Methods Progr. Biomed.*, vol.106, no. 2, pp.70–78, 2012.

[11] W.B. Lee, C.D Lee, K.I. Ho, ―A HIPAA-compliant key management scheme with revocation of authorization‖, *Comput. Methods Progr. Biomed.*, vol. 113, no. 3, pp. 809–814, 2014.

[12] V. Slavov, P. Rao, S. Paturi, T.K. Swami, M. Barnes, D. Rao, R. Palvai. ―A new tool for sharing and querying of clinical documents modeled using HL7 Version 3 standard‖, *Comput. Methods Progr. Biomed.*, vol. 112, no. 3, pp. 529–552, 2013.

[13] Y.C. Yu, T.W. Hou, ―An efficient forward-secure certificate digital signature scheme to enhance EMR authentication process‖, *Med. Biol. Eng. Comput.*, vol.52, pp. 449–457, 2014.

[14] T.F. Lee, C.M. Liu, ―A secure smart-card based authentication and key agreement scheme for telecare medicine information systems‖, *J. Med. Syst.*, vol. 37, no. 3, pp. 1-11, 2013.

[15] T.F. Lee, ―Verifier-based three-party authentication schemes using extended chaotic maps for data exchange in telecare medicine information systems‖, *Comput. Methods Progr. Biomed.*, vol. 117, no.3, pp. 464-472, 2014.

[16] X. Xu, P. Zhu, Q.Y. Wen, Z.P. Jin, H. Zhang, L. He, ―A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information system‖, *J. Med. Syst.*, vol. 38, no. 1, pp. 1-7, 2014.

[17] F.T. Wen, L.D. Guo, ―An improved anonymous authentication scheme for telecare medical information systems‖, *J. Med. Syst.*, vol. 38, no. 5, pp. 1-8, 2014.

[18] M. Farash, M. Attari, ―An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps‖, *Nonlinear Dyn*, vol. 77, no. 1-2, pp. 399-411, 2014.

[19] D. Mishra, ―Understanding Security Failures of Two Authentication and Key Agreement Schemes for Telecare Medicine Information Systems‖. *J. Med. Syst*, doi: 10.1007/s10916-015-0193-7, 2018.

[20] N. Radha, S. Karthikeyan, ―A study on biometric template security‖, *ICTACT J Soft Comput.*, vol. 1, no. 1, pp. 37-41, 2010.

[21] A. Awasthi, K. Srivastava, ―A biometric authentication scheme for telecare medicine information systems with nonce‖, *J. Med. Syst.*, vol. 37, no. 5, pp. 1-7, 2013.

[22] D. Mishra, S. Mukhopadhyay, S. Kumari, M. Khan, A. Chaturvedi., ―Security enhancement of a biometrics-based authentication scheme for telecare

medicine information systems with nonce‖, *J. Med. Syst.*, vol. 38, no. 5, pp. 1-11, 2014.

[23] Z. Tan. ―A user anonymity preserving three-factor authentication scheme for telecare medicine information systems‖, *J. Med. Syst.*, vol. 38, no. 3, pp. 1-9, 2014.

[24] H. Arshad, M. Nikooghadam, ―Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems‖, *J. Med. Syst.*, vol. 38, no. 3, pp. 1-9, 2014.

[25] X. Yan, W. Li, P. Li, J. Wang, X. Hao, P. Gong, ―A secure biometrics-based authentication scheme for telecare medicine information systems‖, *J. Med. Syst.*, vol. 37, no. 5, pp. 1-6, 2013.

AUTHOR PROFILE'S

D NIHARIKA doing post-graduation in VLSI and Embedded systems from Siddhartha Institute of Engineering and Technology in Department of Electronics and Communication Engineering.

MD ASHRAF, is currently working as Associate Professor in Electronics and Communication Engineering (ECE) at Siddharth institute of engineering and technology

DR. D SUBBA RAO, is a proficient Ph.D person in the research area of wireless communications from Rayalseema University, Kurnool along with initial degrees of Bachelor of Technology in Electronics and Communication Engineering (ECE) from Dr. SGIET, Markapur and Master of Technology in Embedded Systems from SRM University, Chennai. He has 16 years of teaching experience and has published 98 Papers in International Journals, 2 Papers in National Journals and has been noted under 4 International Conferences. He has a fellowship of The Institution of Electronics and Telecommunication Engineers (IETE) along with a Life time membership of Indian Society for Technical Education (ISTE). He is currently bounded as an Associate Professor and is being chaired as Head of the Department for Electronics and Communication Engineering discipline at Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, Hyderabad.