iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3364

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Crytanalysis Using Dotnet for Emergency Service and Patient Data

Mrs. T.vanitha[1], G. Divya Lakshmi[2], A. Harini[3], S. saranya[4], P. Sophia[5]
[1]*Assistant Professor, Department of ECE, St.Peter's College of Engineering and Technology, Chennai, India.*
[2, 3, 4, 5]*Student, St. Peter's College of Engineering and Technology, Chennai, India.*

Abstract: Health care is one such field, where WIFI is harmful because it emits the electromagnetic waves that affects patients with disorder. Hence LIFI emerged as the upcoming technology which causes no hazard to the patients and also provides more salient features like speed and broad spectrum than WIFI. The major drawback of transmitting data, in hospitals is to conform that it secure. As a result for this difficulty, the replica suggested here apply Elliptic Curve Diffie Hellman and SHA to allocate security. Elliptic Curve Diffie Hellman is used as an unbalanced function that it uses two keys which in turn makes it hard to hack. Secure Hash Algorithm functions as an additional merit used mainly for authentication purpose.
Keywords: Light Fidelity, Elliptic Curve Diffie Hellman algorithm, SHA, confidentially.

I. INTRODUCTION

The additional paper works are generated in hospital while observing patients and the man power is dissipated between doctors with documents can be minimized by using Light Fidelity as the network and brought in to safeguard the data. The abstract of using LIFI instead of WIFI is due to its broad spectrum that will never be filled in our existence, it causes no hazard to patients health distinct WIFI, which is highly harmful for the neurological disorders and the pace at which the data are transmitted are most quickly. It has few implementation amount as it use LED bulbs for transmission. Hence maintenance cost is low as it is just the light bulbs we use on regular basis. Due to its boasting speeds of up to 224 gigabits per second. Li-Fi could make a huge impact on the Internet of Things too, with data transferred at much elevated quantity with even more devices able to connect to one another. Furthermore, with rapid connectivity and data transmission it's an interesting space for businesses. The combination of IOT devices and Li-Fi will provide a wealth of opportunities for retailers and other businesses alike. Then the Li-Fi technology would be the foremost optimum solution on top of Wi-Fi technology. Li-Fi technology can also be old to enlarge wireless networks at your home, office or university. The Information that has to be transmitted from patient to doctor is measured and the best path for the transmission of the medical parameters is first determined using the Routing protocol Ad-Hoc On-Demand Distance Vector and Greedy Algorithm**.**SHA is used for data encryption/decryption as well as authentication. Hence, it provides at most privacy. Almost the health care parameters can be transmitted as control packets with various medical data sets in . The sensors such as heart rate, EEG, pulse rate and blood pressure which are basic information can be transmitted rapidly in case of patients whose health request continuous observation. Thus LIFI technique has been used with Cryptanalysis to gives a good network in private areas.

II. RELATED WORK

Harald Hars, Liang Yina, Yunlu Wang, Cheng Chena and Yunla Wang were the people who implemented lifi to the world. It transmits data through lights by modulating its force. Arul. R. Sharma has differentiated how LIFI runs better than WIFI mainly concentrate on how WIFI private fields can also use light fidelity. Subham Chatterjee describes how LED bulbs, can be utilized completely, not just using it merely as light bulbs as well as for data transmission in between the server. Jay .H. Bout talks about the problems faced with WIFI when the amount of users grows, the speed is reduced respectively. Prussian Kumar Maura, Japura Sharma, Vaishali Sahila, Hashish Robert and Mahindra Srivatsavat discuss the efficiency of ad-hoc on urging distance vector algorithm. Neha Trithani and Ganesan highlights us about using Elliptic Curve Diffie Hellman Algorithm for providing security for Cloud architecture. Ram Ratan Agarwal explains how the Diffie Hellman key agreement protocol is used to provide forward secrecy for web browser applications. Xing Jhang describes about using Diffie Hellman on IRIS nodes for key agreement and pair-wise key creation between the sensors amidst the network composed of IRIS nodes. In SIP environment, Jinhee Seo proposes an idea to reduce the execution time of TLS handshake authentication mechanism, Diffie Hellman based password authentication method can be used as replacement. This paper focuses on security. Many cryptanalysis hash functions are constructed to provide the data. Hash function create message digest of fixed length. In this observation is done using sensors and the data is wirelessly transmitted using wireless sensors. Wireless sensor involve RF signal for their data transmission. If the frequency of the goes

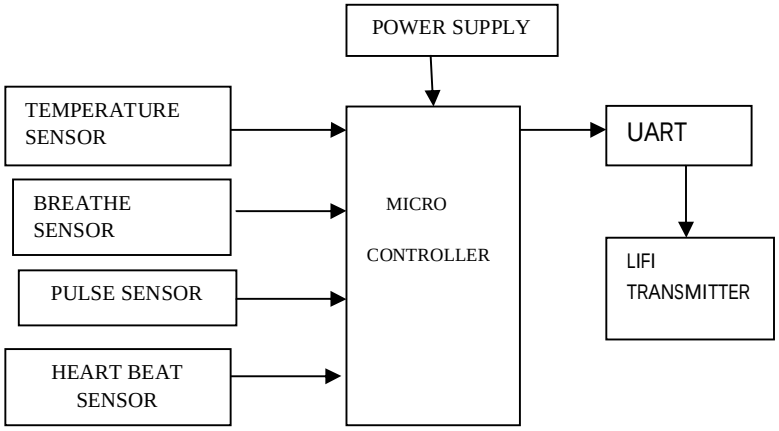
above certain range means it will become radiation and it will start affecting the patients. The increased radiations will easily affect the patients. So in order to overcome these drawbacks we are going for the proposed system

III. PROPOSED SYSTEM

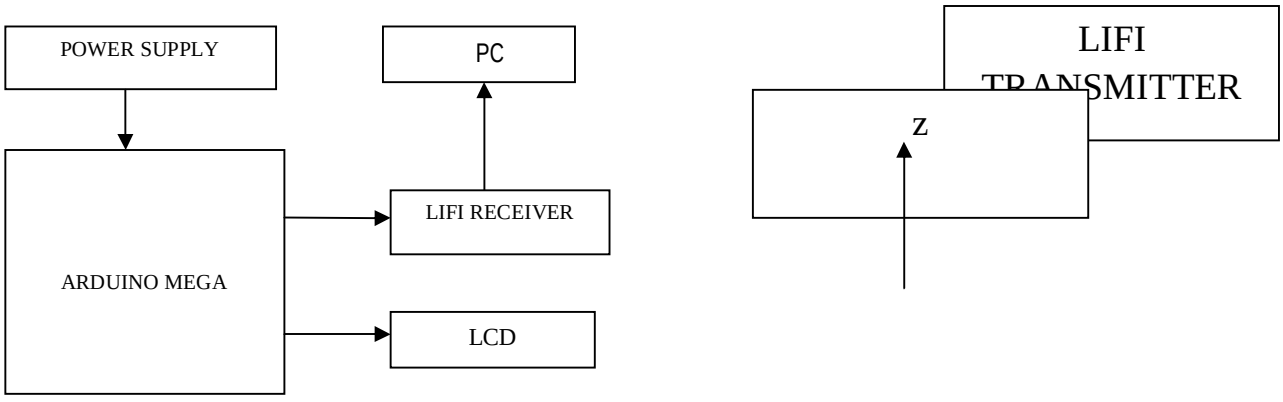
We have proposed the plan of summing the future technology LIFI with security through a series of algorithms. Elliptic Curve Diffie Hellman provides an unbalanced function of using keys with Secure Hash Algorithm. Monitoring is done using sensors and the data is transmitted using wireless sensors. Wireless sensor involve RF signal for the data transmission. If the frequency goes above certain range then it will become radiation and starts affecting the patients. The rapidly increased radiations will easily attach the patients. So in order to overcome these disadvantages the proposed system is used. The sensor will provide above 3000 samples values per second. It will be observed and filtered using microcontroller. All the sample values from the controller is transferred to the receiver section using visible light communication. The data will be monitored in the kit using the microcontroller and in the PC using DOTNET software. The result will be encrypted and decrypted using hash algorithm.

IV. BLOCK DIAGRAM

A. Transmitter Section



B. Receiver Section

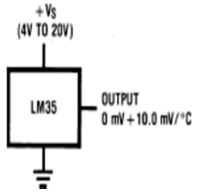


V. TEMPERATURE SENSOR

The first slave connected to a temperature sensor LM35. This senses the temperature of an engine and provides the level of temperature.

A. General Description

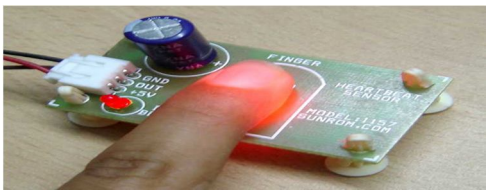
The LM35 series are accurately integrated-circuit temperature sensors, whose result voltage is linearly correspondingly to the Celsius (Centigrade) temperature. The LM35 thus has an control above linear temperature sensors calibrated in Kelvin, as the user is not required to reduce a huge constant voltage from its result to obtain convenient Centigrade scaling.

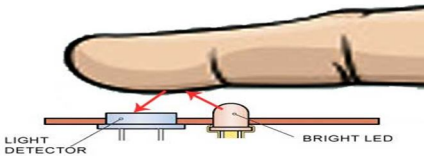


The LM35's compact output impedance, linear output, as well as particular inherent calibration make interfacing to readout or control circuitry especially easy. It can be handed-down with sole power supplies, or with plus and minus supplies. As it draws as little as 60 µA from its supply, it has very short self-heating, less than 0.1°C in still air. The LM35 series is accessible packaged in hermetic TO-46 transistor packages.

VI. HEART BEAT SENSOR

HEART BEAT sensor is constructed to provide digital output of heat beat during a finger is placed on it. When the heart beat detector is working, the beat LED shines in unison with each heart beat. This digital output can be associated to microcontroller straightly to estimate the Beats Per Minute (BPM) rate. It labour on the concept of light modulation by blood flow via finger at each pulse.





A. Heart Beat Sensor

Medical heart sensors have the ability of observing vascular tissue through the tip of the finger or the ear lobe. It is frequently used for health purposes, particularly when monitoring the body after physical training. HEART BEAT is recognized by using a high intensity type LED and LDR. The finger is set in middle of the LED and LDR. As Sensor a photo diode or a photo transistor can be used. The skin possibly light up with visible (red) using transmitted or reflected light for detection. The extremely small difference in reflectivity or in transmittance created by the varying blood content of human tissue are almost cannot be seen. Diverse noise origin may create distraction signals with amplitudes equal or even higher than the amplitude of the pulse signal. Valid pulse calculation consequently be in need of extensive preprocessing of the raw signal. The advanced signal processing approach presented here combines analog and digital signal processing in a way that both parts can be kept easy but in combination are very effective in suppressing disturbance signals. The structure narrated here uses a red LED for transmitted light illumination and a LDR as detector. With at most slight changes in the preamplifier circuit the alike hardware and software could be used with other illumination and detection concepts. The detectors photo current (AC Part) is converted to voltage and amplified by an operational amplifier (LM358).

VII. RESPIRATORY SENSOR

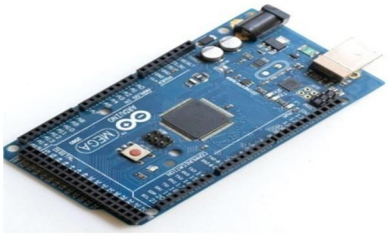
A. General Description

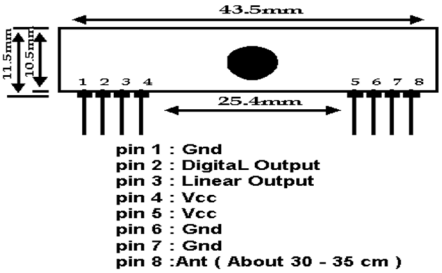
The Respiration Sensor is used to detect abdominal or thoracical breathing, in biofeedback applications such as stress management and relaxation training. Apart from measuring breathing frequency, this sensor as well gives an evidence of the relative depth of breathing. The Respiration Sensor for Nexus can be shabby over clothing, whilst for best results we advise that there only be 1 or 2 layers of clothing between the sensor and the skin. The Respiration Sensor is generally placed in the abdominal region, with the central part of the sensor just above the navel. The sensor should be set compressed enough to prevent loss of tension.

VIII. ARDUINO MEGA

Mega2560-CORE is a compact, utter and breadboard-friendly board base on the ATMega2560. Its design is based on the Arduino Mega2560,so we can use it as a Arduino Mega2560 development board. In a unlike place, it shortfall only a 6-foot download port and a reset switch. Mega2560-CORE has a matching download line and the other one end of the download cable is a USB interface, so it is very appropriate for use. Outermost (non-USB) power can come either from an AC-to-DC adapter (wall-wart) or battery. The adapter can be associated by plugging a 2.1mm center-positive plug into the board's power jack.

A. Arduino Mega





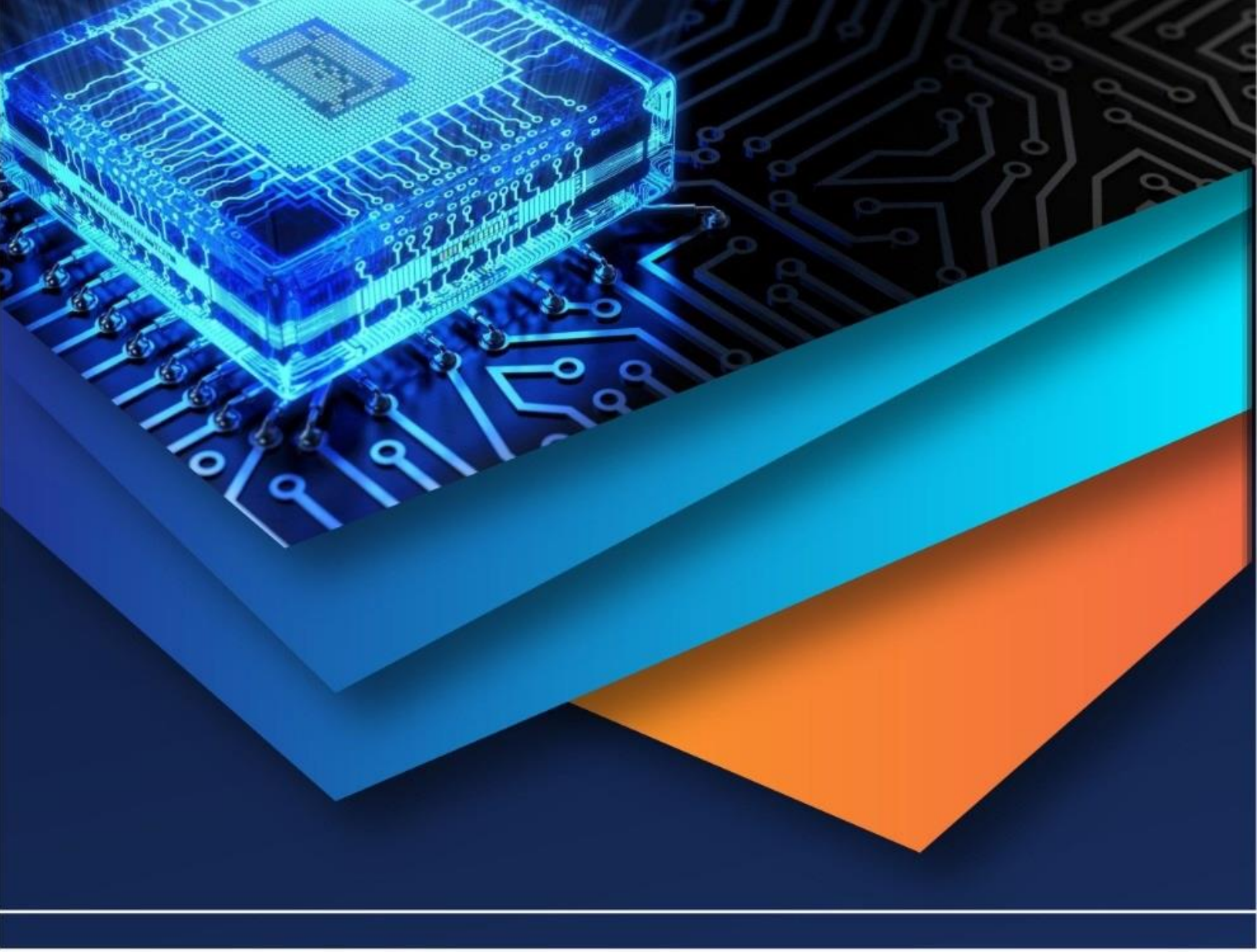
Pin Out Diagram

IX. CONCLUSION

The advanced plan of using the Li-Fi technology in Health Care arose merely as Wi-Fi is still sensitive in such areas as it is considered hazardous, toxic and unsafe. So eventually, it proceeds to extra man power and Paper work. Another significant feature executed in Li-Fi is Secured through Elliptic Curve Diffie Hellman and Secure Hash Algorithm, thus creating it safe. The future of Wi-Fi is highly undetermined with vastly compact spectrum of radio frequencies. Thus Li-Fi remains to be the upcoming field in another intimated area of wireless technology.

REFERENCES

[1] "Greedy Algorithm", International Journal of Scientific and Research Publications, Vol.3, pp.1-5,Annul Malik, Anju Sharma (2013).
[2] John Justin Thangaraj . S and A. Rengarajan (2016) "Unreliable Node Detection by Elliptical Curve Diffie-Hellman Algorithm in MANET", Indian Journal of Science and Technology, Vol.9, pp.1-6.
[3] Cheng Chen, Harald Hass, Liang Yin, Yunlu Wang "What is LIFI?", Journal of Lightwave Technology, Volume: 34, pp.1533 – 1544. International Journal of MC Square Scientific Research Vol.9, No.1 April 2017 96.
[4] Ganesan R and Neha Trithani (2014) "Data Security in Cloud Architecture based on Diffie-Hellman and Elliptical Curve Cryptography", International Association for Cryptologic Research.
[5] Christian Lederer, Roland Mader, Manuel Koschuch, Johann Grobsch ad, Alexander Szekely, Stefan Tilich (2009) "Energy-Efficient Implementation of ECDH Key Exchange Algorithm for Wireless Sensor Networks", Information Security Theory and Practice, Vol.5746, pp.112-127.
[6] Ayaz Ahmad, Mahfuzul Huda, Mohd Atif Kaleem, Rajendra Kr Maurya (2015) "Mobile Ad-Hoc Networks: AODV Routing Protocol Perspective", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, pp.514-517.
[7] Chaitya B Shah, Drashti R Panchal (2014) "Secured Hash Algorithm-1: review Paper", International Journal For Advance Research In Engineering And Technology, Vol.2,pp.26-30.
[8] Balaram Ghosal, Asim Kumar (2014), "Li-Fi a Green Energy Initiative", International Journal of Computer Applications, Vol.95, No.11, pp.1-3. Christian Lederer, Roland Mader, Manuel Koschuch, Johann Grobsch ad, Alexander Szekely, Stefan Tilich (2009) "Energy-Efficient Implementation of ECDH Key Exchange Algorithm for Wireless Sensor Networks", Information Security Theory and Practice, Vol.5746, pp.112-127.
[9] Balajee Maram, Sravanthi Dangani, "Group Key Exchange Analysis in Sensor Networks", International Journal of Distributed Sensor Networks, Vol.10, pp.1-12.
[10] John Justin Thangaraj . S and A. Rengarajan (2016) "Unreliable Node Detection by Elliptical Curve Diffie-Hellman Algorithm in MANET", Indian Journal of Science and Technology, Vol.9, pp.1-6



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY