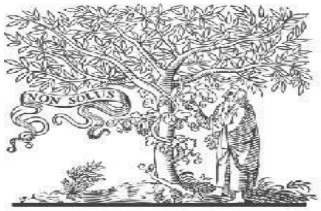
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

Link : https://ijiemr.org/downloads/Volume-12/Issue-05

10.48047/IJIEMR/V12/ISSUE05/34

Title **A THREE-TIER APPROACH FOR LIGHTWEIGHT DATA SECURITY OF BODY AREA NETWORKS IN EHEALTH APPLICATIONS**

Volume12, Issue 05, Pages: 347-356

Paper Authors

Dr. Syeda Ms Amina Begum, Furquan Ahmed, Syed Abrar Ahmed, Ahmed Javed

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A THREE-TIER APPROACH FOR LIGHTWEIGHT DATA SECURITY OF BODY AREA NETWORKS IN EHEALTH APPLICATIONS

1 **Ms Amina Begum,** Assistant Professor, Department of ECE, Deccan College of Engineering and Technology, Telangana, India. aminabegum@deccancollege.ac.in

2 **Furquan Ahmed**, Department of ECE, Deccan College of Engineering and Technology, Telangana, India. Ahmedfurqan846@gmail.com

3 **Syed Abrar Ahmed**, Department of ECE, Deccan College of Engineering and Technology, Telangana, India. Ahmedsyed536@gmail.com

4 **Ahmed Javed**, Department of ECE, Deccan College of Engineering and Technology, Telangana, India. ahmedjaved142@gmail.com

ABSTRACT: Wireless body area networks (WBANs) can enable e-health applications under Internet of Things (IoT) scenarios. However, to use WBAN technologies in practical applications, sensitive data collected by wireless sensors must be protected when transmitted across a network and until accessed by authorized applications or end-users. Specifically, it is necessary to provide confidentiality, integrity, authentication and access control in WBANs. This paper presents a security approach to provide these security services in a layered WBAN system using lightweight cryptography. Layer 1 consists of the communication between the sensor nodes and the base station (data acquisition); Layer 2 involves the communication between the base station and a data repository (data storage); and Layer 3 deals with the communication of end-users to the repository (data access). In the past, security has focused only on Layer 1 and for limited security levels. In this paper, security concerns in the three layers of a WBAN system are studied and addressed. As primary contributions, the design details of a secure WBAN system prototype and the impact of lightweight cryptographic engines on the performance of the primary use cases in the WBAN system are highlighted from data acquisition until data use. We present a novel WBAN system prototype that ensures most of the required security services for standard security levels.

Keywords *– The IoT, e-health, secure WBAN, security services, lightweight cryptography, attributebased encryption.*

1. INTRODUCTION

The demand for advanced healthcare applications is expected to grow with the progressive deployment of the Internet of Things (IoT), including remote patient monitoring, which has become a reality to continuously track vital sign data (e.g., blood pressure, blood oxygen levels, heart rate, etc.) from individuals. Then, collected information could be accessed by an authorized healthcare provider to enable, for example, the timely detection of clinical deterioration. In this context, a prominent enabling

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

technology in the IoT ecosystem to monitor patients' vital sign data is then wireless body area network (WBAN). AWBAN is composed of small smart devices that play an important role as both data collectors and data gateways in WBAN applications. Such sensors can be either situated in a fixed position in the body or even carried at different positions in clothing if wearable-like sensors are used. In e-health applications, a WBAN aims to provide an efficient and reliable communication infrastructure to all implanted, non implanted and wearable sensor devices for the human body [1]. In this regard, because health data transmitted through a WBAN could be exposed to unauthorized parties, or even malicious adversaries, it is critical to ensure security services through the entire data stream (data life cycle), which involves data acquisition, data transmission to a storage system, and the data accessed by authorized users. From an architectural viewpoint, the data cycle can be decomposed into a three-layer network architecture in terms of data collection (sensory stage), transmission (communication network) and storage (application).

The provision of security services over the entire data life cycle in a WBAN is of paramount importance to prevent attacks such as tampering, falsication, or data capture by a third party. The development of security and privacy services for IoT healthcare architectures is an important research area [2]. Two core challenging issues related to the design and development of secure WBANs have been addressed thus far. On the one hand, since a standardized system architecture is not well defined, data restriction and preservation of its integrity and the robustness of the WBAN system, in general, are not achieved [3]. On the other hand, the design of computational and energy efficient security mechanisms is essential because WBAN sensors are resource-constrained devices. As in other systems, WBANs require security services at three architectural layers that provide confidentiality (C), integrity (I), authentication (A) and access control (AC) [4], [5]. Each of these services can be guaranteed when using cryptography algorithms and, in this particular case, by lightweight cryptography algorithms [6], [7]. Unfortunately, few studies have investigated these security services (C, I, A, and AC) at a time when e-health services are relying on a WBAN. Specifically, most existing research regarding secure WBANs primarily investigated the design of lightweight security services for data collection (e.g., those produced in the sensor nodes and delivered to a base station) [8][10]. Other studies reported custom security protocols that address some but not all of the required security services [11][14], or practical deployments with experimental evaluation of security mechanisms are missing [15][17]. It is worth noting that custom protocols usually only address one single security service, and only for two actors in the WBAN (sensor node and base station, or sensor node and cloud server). However, an integrated approach that can provide security services to protect the entire data life cycle in a WBAN has not yet been proposed for all recommended security services, since data is produced in the sensor nodes, when data is transmitted to the base station then to the cloud

server, and until data is ally accessed by end users (nurse, pharmacy, doctors, etc).

2. LITERATURE REVIEW

Security and privacy in E-healthcare monitoring with WBAN: A critical review:

In the current scenario Wireless Body Area network (WBAN) has made its prominent place among technological advancements to improve human health. Since WBAN uses a wireless technique for communication, it has various positive & striking features such as its unattended nature, unobtrusiveness, mobility and cost effectiveness. These WBANs are extremely essential for people with severe diseases. For example, Heart patients, pregnant women, mentally challenged people, etc. need a continuous observation. Thus, WBAN, on the one hand, is working as a virtual safeguard for its users. WBAN, on the other hand, exploits wireless media during its realization. All the constraints specially related to insecurity (openness) have also been elaborated here. Since health related information is tremendously crucial and confidential and also liable to the patient's life. Therefore, we need to take care of mechanisms applied to WBANs to overcome all the issues and drawbacks related to security and privacy. This paper focuses on various limitations and their possible solutions available within WBANs in order to provide secure and private information management to its dependents and users.

Security and privacy issues in wireless sensor and body area networks:

Advancements in wireless communication and availability of miniaturized, battery powered micro electronics devices have revolutionized the trend of computation and communication activities to the generation of smart computing where spatially distributed autonomous devices with sensors forming wireless sensor network (WSN) are utilized to measure physical or environmental conditions. WSNs have emerged as one of the most interesting areas of research due to its diverse application areas such as healthcare, utilities, remote monitoring, smart cities, and smart home which not only perform effective monitoring but also improve quality of living. Even the sensor nodes can be strategically placed in, on, or around human body to measure vital physiological parameters as well. Such sensor network which is formed over human body is termed as wireless body area network (WBAN) which could be beneficial for numerous applications such as eldercare, detection of chronic diseases, sports, and military. Hence, both network applications deal with sensitive data which requires utmost security and privacy. Thus, the security and privacy issues and challenges related to WSN and WBAN along with the defense measures in place should be studied in detail which not only is beneficial for effective application but also will motivate the researcher to find their own path for exercising better protection/defense. Accordingly, in this chapter a brief overview of both networks is presented along with their inherent characteristics, and the need for security and privacy in either networks is illustrated as well. Besides, study has been made regarding potential threats to security and privacy in both networks and existing measures to

handle these issues. Finally the open research challenges are identified to draw the attention of the researcher to investigate further in this field.

Internet of Things: A survey of enabling technologies in healthcare and its applications:

Internet of Things (IoT) on the Wireless Body Area Network (WBAN) for healthcare applications is an operative scenario for IoT devices that has gained attention from vast research fields in recent years. The IoT connects all subjects and the healthcare system seamlessly. This paper describes the WBAN based IoT healthcare system and reviews the state-of-the-art of the network architecture topology and applications in the IoT based healthcare solutions. Moreover, this paper analyzes the security and the privacy features consisting of privacy, authentication, energy, power, resource management, Quality of Services and the real-time wireless health monitoring that are quite problematic in many IoT healthcare architectures. Because, system architecture is not well-defined, data restriction and its integrity preservation is still a challenge. At present 90% of the information available is acquired in the recent two years. This survey mainly aims at analyzing healthcare purpose which is based on digital healthcare system. Further, it reports many IoT and the e-healthcare policies and systems that decide how to ease all bearable development. Thus, the overall system provides large possibilities for future research based on IoT healthcare system. Finally, research gaps are reviewed and the possible future aspects have been discussed.

Security and privacy in remote healthcare: Issues, solutions, and standards:

Remote healthcare machinery such as telemedicine and remote monitoring are the potential solution to the problems of rural health care which suffers from the lack of medical infrastructure and medical professionals. This chapter re-establishes the need for remote healthcare. The two approaches of remote health care: telemedicine and remote monitoring are discussed, supported by illustrating general architectures. The primary focus of this chapter is the issue of security and privacy in remote healthcare. Since healthcare data are sensitive and critical, and mishandling of which may have severe consequences, ensuring the security, privacy, and confidentiality of patients' data is of utmost importance. The privacy and security threats, requirements, solutions, and standards are examined and explained meticulously. The challenges and the trade-offs in ensuring privacy and security in remote healthcare are identified and justified. A special discussion on the latest happenings and the future of remote healthcare security is also presented.

A survey of lightweight cryptographic algorithms for iot-based applications:

Lightweight crypstographic algorithms are powerful and secure algorithms which are equipped with leading-edge innovation like RFID or Wireless Sensor Networks (WSN) or quickly developing Internet of Things (IoT). They are lightweight in terms of power utilization, clock cycles, and speed, etc., and are easy to implement on constraint or ultra-

constraint hardware devices like FPGA's or RFID labels. This paper indicates a concise knowledge of IoT, and lightweight and implemented algorithms compare the performed cryptographic algorithms and yield a proficient conclusion in terms of security, reliance, speed, memory and throughput, applications, and so forth. Thus, optimized algorithms relying upon the platform utilized can search through the scrutinized list.

3. METHODOLOGY

Specifically, most existing research regarding secure WBANs primarily investigated the design of lightweight security services for data collection (e.g., those produced in the sensor nodes and delivered to a base station).

In proposed a three-tier security architecture that is different from that presented in this study. Security is addressed by a custom method that is based on key management (one for each tier, comprised of sensor nodes, base stations, and network connection nodes) and hash functions. The proposed prototype allows us to evaluate the costs of providing security services over the entire data life cycle in WBAN deployments with resource-constrained devices. The proposed method prevents these attacks by ensuring confidentiality, integrity, authentication and access control over data.

An embedded system can be defined as a computing device that does a specific focused job. Appliances such as the air-conditioner, VCD player, DVD player, printer, fax machine, mobile phone etc. are examples of embedded systems. Each of these appliances will have a processor and special hardware to meet the specific requirement of the application along with the embedded software that is executed by the processor for meeting that specific requirement. The embedded software is also called "firm ware". The desktop/laptop computer is a general-purpose computer. You can use it for a variety of applications such as playing games, word processing, accounting, software development and so on. In contrast, the software in the embedded systems is always fixed listed below: • Embedded systems do a very specific task, they cannot be programmed to do different things. . Embedded systems have very limited resources, particularly the memory. Generally, they do not have secondary storage devices such as the CDROM or the floppy disk. Embedded systems have to work against some deadlines. A specific job has to be completed within a specific time. In some embedded systems, called real-time systems, the deadlines are stringent. Missing a deadline may cause a catastrophe-loss of life or damage to property. Embedded systems are constrained for power. As many embedded systems operate through a battery, the power consumption has to be very low. • Some embedded systems have to operate in extreme environmental conditions such as very high temperatures and humidity.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

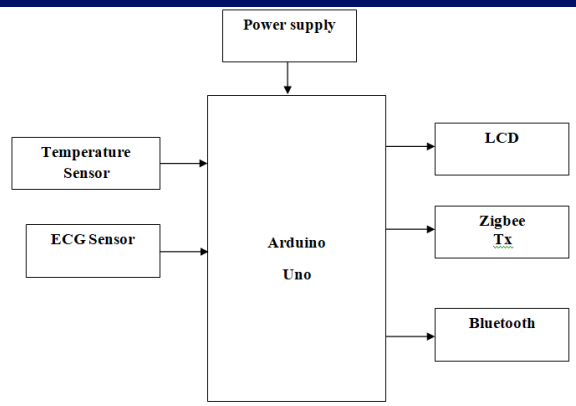


Fig.1: Block diagram

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.

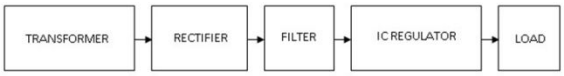


Fig.2: Power supply

Transformer:

Transformers convert AC electricity from one voltage to another with little loss of power. Transformers work only with AC and this is one of the reasons why mains electricity is AC. Step-up transformers increase voltage, step-down transformers reduce voltage. Most power supplies use a step-down transformer to reduce the dangerously high mains voltage (230V in India) to a safer low voltage. The input coil is called the primary and the output coil is called the secondary. There is no electrical connection between the two coils; instead they are linked by an alternating magnetic field created in the soft-iron core of the transformer. Transformers waste very little power so the power out is (almost) equal to the power in. Note that as voltage is stepped down current is stepped up. The transformer will step down the power supply voltage (0-230V) to (0- 6V) level. Then the secondary of the potential transformer will be connected to the bridge rectifier, which is constructed with the help of PN junction diodes. The advantages of using bridge rectifier are it will give peak voltage output as DC.

Voltage Regulators:

Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustably set voltage. The regulators can be selected for operation with load currents from hundreds of milli amperes to tens of amperes, corresponding to power ratings from milli watts totens of watts. A fixed three-terminal voltage regulator has an unregulated dc input voltage, Vi, applied to one input terminal, a regulated dc output voltage, Vo, from a second terminal, with the third terminal connected to ground. The series 78

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

regulators provide fixed positive regulated voltages from 5 to 24 volts. Similarly, the series 79 regulators provide fixed negative regulated voltages from 5 to 24 volts. Voltage regulator ICs are available with fixed (typically 5, 12 and 15V) or variable output voltages. They are also rated by the maximum current they can pass. Negative voltage regulators are available, mainly for use in dual supplies. Most regulators include some automatic protection from excessive current ('overload protection') and overheating ('thermal protection'). Many of the fixed voltage regulator ICs has 3 leads and look like power transistors, such as the 7805 +5V 1Amp regulator. They include a hole for attaching a heat sink if necessary.

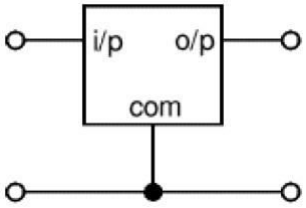


Fig.3: Regulator

ZIGBEE TECHNOLOGY:

ZigBee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power, wireless sensor networks. The standard takes full advantage of the IEEE 802.15.4 physical radio specification and operates in unlicensed bands worldwide at the following frequencies: 2.400–2.484 GHz, 902-928 MHz and 868.0–868.6 MHz 1.

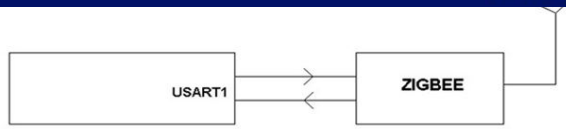


Fig.4: Zigbee

5. EXPERIMENTAL RESULTS

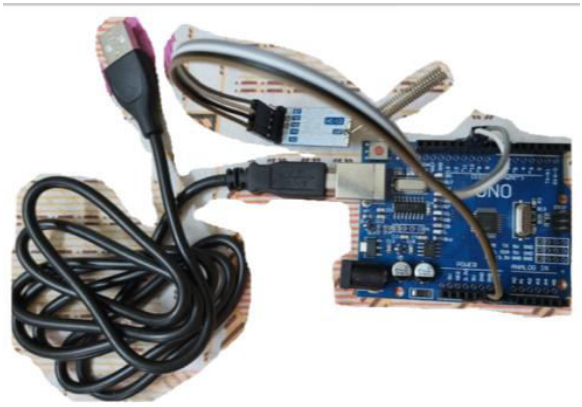


Fig.5: Output

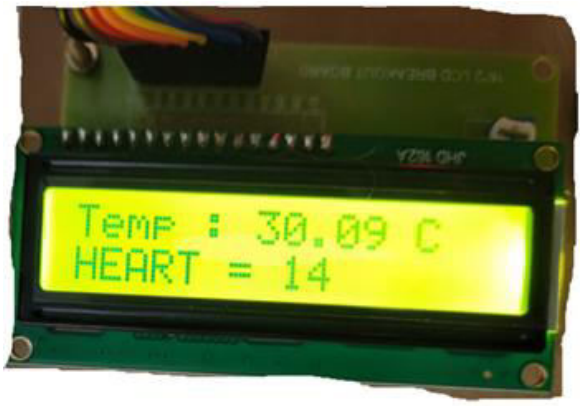


Fig.6: Output

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

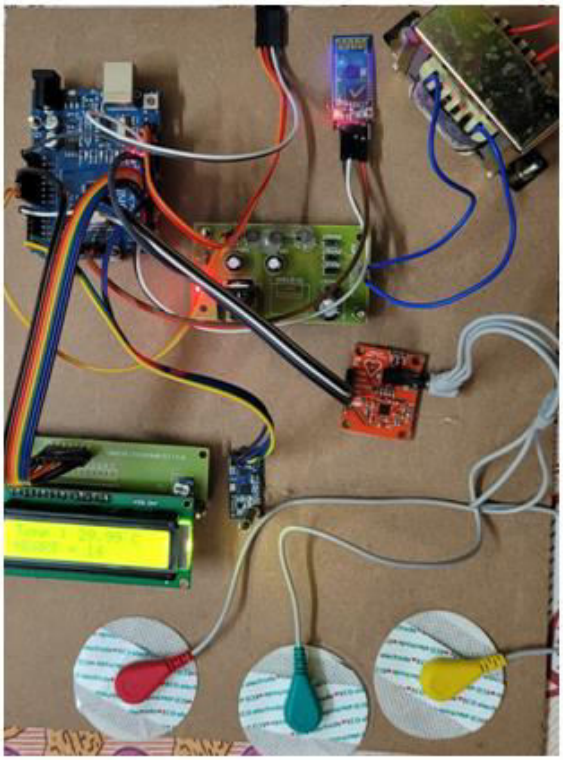


Fig.7: Output

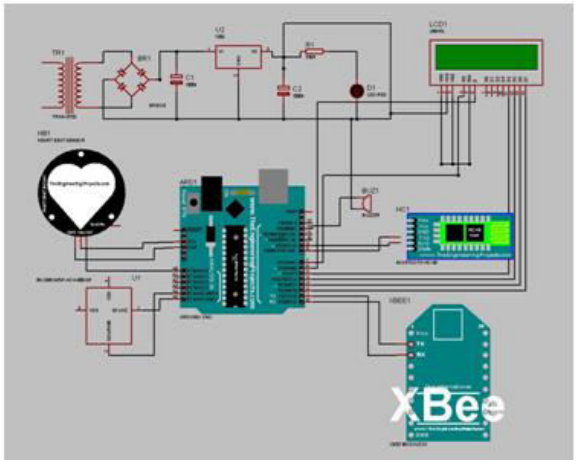


Fig.8: Output

6. CONCLUSION

In this study, we proposed a three-tier security model for WBAN systems suitable for e-health applications that relies on the use of lightweight cryptography to provide security services in the entire data cycle. As a proof of concept, a prototype was deployed based on the three-layer model to determine the performance of the proposed method in terms of execution time, memory and energy consumption. We first provided extensive experimental evaluations to determine the most appropriate cipher suites to ensure specific security services in a real WBAN deployment. Conversely, we observed that the cost of crypto-algorithms in terms of computational resources is acceptable. Specifically, the penalty in performance due to the computational processing of cryptographic layers can be tolerated by end-users while still meeting the expected data rate of sensed data.

REFERENCES

[1] A. Tewari and P. Verma, ``Security and privacy in E-healthcare monitoring with WBAN: A critical review," *Int. J. Comput. Appl.*, vol. 136, no. 11, pp. 37_42, Feb. 2016.

[2] M. Roy, C. Chowdhury, and N. Aslam, ``Security and privacy issues in wireless sensor and body area networks," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. Cham, Switzerland: Springer, 2019, pp. 173_200.

[3] M. M. Dhanvijay and S. C. Patil, ``Internet of Things: A survey of enabling technologies in

healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113_131, Apr. 2019.

[4] H. D. Jude and V. E. Balas, Eds., ``Security and privacy in remote healthcare: Issues, solutions, and standards," in *Telemedicine Technologies*. London, U.K.: Academic, 2019, pp. 201_225. [5] K. R. Siva and R. Venkateswari, ``Security challenges and solutions for wireless body area networks," in *Computing, Communication and Signal Processing*. Singapore: Springer, 2019, pp. 275_283.

[6] A. Shah and M. Engineer, ``A survey of lightweight cryptographic algorithms for iot-based applications," in *Proc. ICCS*, 2019, pp. 283_293.

[7] S. B. Sadkhan and A. O. Salman, ``A survey on lightweight-cryptography status and future challenges," in *Proc. Int. Conf. Advance Sustain. Eng. Appl. (ICASEA)*, Mar. 2018, pp. 105_108.

[8] [8] J. Shen, Z. Gui, X. Chen, J. Zhang, and Y. Xiang, ``Lightweight andcertificatelessmultireceiver secure data transmission protocol for wireless body area networks," *IEEE Trans. Dependable Secure Comput.*, early access, Sep. 21, 2020, doi: 10.1109/TDSC.2020.3025288.

[9] M. Ali, M.-R. Sadeghi, and X. Liu, ``Lightweight _ne-grained access control for wireless body area networks," *Sensors*, vol. 20, no. 4, p. 1088, Feb. 2020.

[10] C. Meshram, C.-C. Lee, S. G. Meshram, R. J. Ramteke, and A. Meshram, ``An efficient mobile-healthcare emergency framework," *J. Med. Syst.*, vol. 44, no. 3, pp. 1_14, Mar. 2020.