Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

BIOMETRIC SECURITY IN WBAN

M.Infant angel*[1],R.sudha*2

*Research Scholar, Dept. of Computer Science,
PSG College of Arts & Science, Coimbatore, India[1]

*Asst. Professor, Dept. of Computer Science,
PSG College of Arts &Science, Coimbatore, India[2].

Abstract: *Remote body zone network(WBAN) is another pattern in the innovation that gives remote instrument to screen and gather patient's wellbeing record information utilizing wearable sensors.It is generally perceived that an abnormal state of a framework security and security assume a key part in ensuring these information while being utilized by the human services experts and amid capacity to guarantee that patients record are remained careful from interloper's danger.It is consequently of awesome enthusiasm to talk about security and protection issues in WBAN.This paper likewise covers the condition of-workmanship safety efforts and research in WBAN.The remote body region arrange (WBAN) is a framework that encourage to clients for giving programmed wellbeing monitoring,which sends critical wellbeing related information to the specialists with the assistance of body sensors.*
The exploration infers that:

- *Security necessities of electronic medicinal services are for the most part focused around;data confidentiality,data authenticity,data integrity,and client/element validation.*
- *Biometrics offer viable and helpful technique for accomplishing the above security necessities however biometric encryption and biometric validation.*
- *Biometrics has wide arrangements in medicinal services industry because of their capacity to offer solid.*

Keywords*: biometrics,healthcare,privacy,security,confidentiality*

Introduction

Wireless body area networks (WBANs) consist of small wearable or implantable sensors on, near, or in a human body. By collecting vital sign parameters and activities from a human body, WBANs can enable continuous health monitoring and provide portable, real-time and ubiquitous healthcare services, and offer numerous practical and innovative applications to improve healthcare quality [1-9]. The security of WBANs is critical for those healthcare applications because the sensitive biometric data have to be exchanged over insecure networks. Moreover, medical management is an important issue for all the healthcare applications. Therefore, the design of effective medical management mechanisms for WBANs is also indispensable.

In medical management, patient information authentication, healthcare operation verification and doctor liability identification are the important areas in need of research. The applications of WBANs can draw lessons from the existing approaches [24-27] for medical image applications, in which the electronic medical record (EMR) containing prime healthcare information is directly embedded into a medical image by watermarking schemes for patient authentication and data integrity check. However, the watermarking schemes cannot be directly applied to the healthcare applications over the WBANs for two reasons. Firstly, most of those schemes [24, 26-27] will unavoidably modify the watermark carriers in order to embed the EMR. However, as the watermark carriers in WBANs are sensitive biometric data and must not be modified, the lossless watermarking scheme has to be used for WBANs. Secondly, because the sizes of typical biometric data are much smaller than those of medical images, the watermark embedding capacity would be insufficient for hiding the EMR.

Applications of wban

(a) **WBANs working as a Virtual Doctor**: As explained by Ganesh Borse and Himangi Pande [3] WBAN based system can be developed and used as a virtual doctor. It supports various healthcare services to its dependents having abnormalities related to cancer, diabetes, high blood pressure, cardiovascular disease, etc. Here a server is designed to keep information about the patient (e.g. his/her medical history). The server also sends daily tips and suggestions. Moreover, in case of emergency it provides the patient with the medical aid by informing the concerned hospital and also patient's family and relatives. Its key point is SVM (Support Vector Machine) used to keep track of physiological data about patient then take decision on its basis.

(b) **WBANs used as death Intimation Device**: This application of WBAN is mainly developed for unfit elderly people, paralyzed or immobile patients. Nowadays in various countries people live alone in the last span of their lives. Timely Information about their death must be delivered to right authority. Here a TinyOS software based MEMS are used in sensor nodes for generating swift alerts. This wearable biocompatible feeler detects movements of patient body and their

pulse-rate or heart-beat. Accordingly this sensor updates information about user within server and triggers are generated and sent to doctor (as a SMS) using cellular network.

(c) **E-Healthcare monitoring systems for Homely Elders[8]:** In this application of WBAN wellness of elders living independently in their residence is being accomplished. An intelligent home monitoring system based on ZIGBEE-WSN has been designed and developed to observe and evaluate the fitness of old person in home environment. MEMS sensors are used here to analyze the gestures and EPIC. Temperature sensors and other body sensors are used to find any irregularity for elders during their routine activities as sleeping, walking, eating, bathing or even car driving. If any abnormality occurs it is immediately informed to network coordinator and such collected information is handed over to medical personals.

(d) **Cloud-based Healthcare systems** [9], [10]: Here usage of WBAN based healthcare system is developed with the help of immensely powerful and currently hot concept of cloud-computing. By this distributed service based concept healthcare objectives has become highly promising to take care of human life-style.

Secure Medical Information Management System (SMIMS)

Assumption:

1.The deployment of sensors with the pre-stored information to the patient is secure. There is no error of pre-stored information.

2) We are primarily concerned with the three threats resulting from the wireless channel, which are data eavesdropping, data modification and impersonation attack.

3) The symmetric keys have been previously distributed, and we mainly focus on the processes after the key management and establishment.

4) As another reference for security in WBANs [17], there is a secure storage in the sensor mote and the critical information stored in the storage will not leak even if it is physically captured by an unauthorized person.

MECHANISMS USED TO INCULCATE SECURITY AND PRIVACY IN WBAN

A lot of research has been taken place and still in progress to solve this safety problem within WBANs. Safety and network security solutions developed and used in wired sensor networks and general wireless sensor networks are simply futile in WBAN scenario due to following 3 reasons

- WBAN is directly related to human beings so hit and trial or any hypothesis is useless
- Hostile environmental conditions.
- Openness of network.

Few recent papers are covered here which emphasize on solving security and privacy facets of healthcare arrangements using WBANs.

a) **Security and privacy preserved healthcare systems based on Cloud-computing concept**:

Cloud computing is the latest area in which splendid projects are being developed for information processing and resource (availability) scheduling in a ubiquitous and fully automated but less expensive way. E-healthcare is one of those projects that flourished under the umbrella of cloud computing in a glorious manner. Security and privacy are exceptionally noteworthy properties in E-healthcare systems within WBANs. A cloud based framework using WBANS as its backbone implemented security and privacy techniques [9], [11] is one of its own kinds. This skeleton has 2 steps to apply security as- International Journal of Computer Applications (0975 – 8887) Volume 136 – No.11, February 2016 41 (i) Any pair of sensors can talk to each other safely by using multi-biometric key generation scheme within WBANs. (ii) Patient's data stored on cloud has been made confidential and safe by using dynamic reconstruction of metadata. This framework has attached a personal server to a patient, a client interface/ data-reader, RBS (Remote base station) and a hospital community cloud. This structure supports both indoor (within hospital) and outdoor (away from hospital) patients. Main technique used to secure communication is based on combination of 2 biometric values as values taken from ECG and EEG devices. It raises length of keys using key-gen algorithm. This raised length keys are used to encrypt and decrypt the private data and in this way randomness and unpredictability are introduced for attackers. Patient's data is parameterized as per the degree of sensitivity. By this approach a ubiquitous mobile healthcare service is devised in this framework. Testing of security has been tested by DIEHARDER software on UBUNTU machine.

b) b) Multidisciplinary approaches used to develop secure WBANs in healthcare: Since WBANs are directly related to human health, so different human body generated or contained values/information can be made used to grow security within systems. By following above idea, robustness property of human body is used as an inspiration [19] which is evolved from biology to develop secure systems. An approach to secure WBAN using BIO-Inspiration developed by Rathore et al. is revolutionary idea in recent scenario. In this research security is implemented by using human immune system as it base and inspiration along with machine learning techniques have been applied here. Here malicious nodes are detected by machine learning module. Antigen and antibody concept of human immune system is used as a different module for removal of malicious nodes from communication network. According to another research new improved encryption mechanisms are developed on the basis of two conceptsDNA computation and Chaos Theory [22]. It targets secure data communication by using a concept- only encrypted information will be transmitted. DNA based cryptography is not a new method but doing this along with

chaos theory of non-linear mathematical model brings a broad and unpredictable encryption scheme in to picture. Unauthorized user will feel this chaotic encrypted data as a noise. So chaos is used as a key generator and it proved as a strong pseudorandom generator. By this concept safe, collision-free and efficient MAC protocol could be developed here.

c) Protocol-redesigning and development based mechanism to implement security in WBANs in healthcare:

In these mechanisms, many existing routing and transmission control protocols are redesigned and developed again in order to make secure and privacy preserving WBANs. Another area of development consists of many new security protocols to defeat evil intensions of cryptanalysts. Zhang et al. developed a secure and lightweight admission and transmission protocol for WBSNs and WBANs [21].

In this protocol PWH (Personal Wireless Hub) and PHI (Personal Health Information) are utilized as basic terms. PWH is local processing unit of WBANs and data collected by sensors is termed as PHI. Data is forwarded from PWH to remote healthcare centre for necessary actions. In this research both- security of transmission of PHI and preserving privacy of PHI are handled properly. A polynomial based authentication scheme is explored and used to fulfill above required security and privacy implementation. Eavesdropping is controlled and prevented here by applying pair wise key generation and usage by two non-malicious nodes. Security while transmitting the data is applied by devising a protocol along with symmetric encryption and sub-keyed hash function. By applying this methodology few major security aspects as- confidentiality, authentication and integrity are accomplished. This protocol was implemented on optimally numbered systems having TinyOS version 2.x. Energy consumption by each component is also controlled here. Another development of security protocol is enriched by enabling the proper usage of Different PAKE (pair-wise acknowledgement key exchange) based idea. A detailed analysis of PAKE protocols [18] provides a transparent view of secure WBANs. Various limitations in PAKE protocols such as forward secrecy, impersonation attacks, dictionary, and replay attacks are also analyzed here thoroughly. Hence, these researches are definitely giving a path to move ahead and create few more security protocols to strengthen security of data and communication channels within WBANs. Other trust based schemes and anomaly detection systems [2] are also being developed to make E-healthcare observatory systems more reliable

Biometric identificationin health care

Biometric identification refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics [7], [17]. Many physiological and behavioral characteristics are unique to an individual. This makes biometric identifiers inherently more reliable and capable than knowledge-based and token-based techniques in distinguishing an authorized person from an imposter [7]. The identification mode is concerned with the task of comparing a user's biometric sample with all the template set of users enrolled in the database to output the identity of the user [15]. As a result, it is referred to as one-to-many (one-to-N) task [18]. The output is normally a sorted list of candidate models based on the degree of match of the test sample [18]. Identification is an important component in negative recognition and might be employed in positive recognition as well [12]. Positive recognition systems prevent multiple users of single identity while negative recognition systems prevent multiple identities of a single user.

Biometric authentication in health care

Biometric authentication is often generally referred to as 'biometrics' in practice [19]. The term 'biometrics' is also used synonymously with Biometric recognition [15], [18]. In fact, authors in [15], [19] recognize the fact that, the term 'biometrics' has been used to refer to the statistical analysis of biological data historically. The three terms would thus be used interchangeably in this work. Biometrics, as stated earlier, is concerned with the use of physiological characteristics (e.g. fingerprint, iris) or behavioral traits (e.g. keystroke dynamics, signature) to verify the identity of an individual [15], [20]. Biometrics process is mostly done automatically by the use of computers [15], [19] hence could also be defined as the automated method of recognizing or verifying the identity of individuals based on their physiological or behavioral traits [15], [19]. Biometric authentication is basically a pattern recognition system [21], [22]. It operates by comparing extracted feature set which is obtained from the biometric data collected from individuals to the template set stored in the database [22]. Authentication is mostly considered to involve two modes; identification and verification [20].

Electronic healthcare (E-health)

Advancements made in the field of telemedicine around the twentieth century paved the way for e-Health. Following that came developments in computerization, digitization of data, and digital networks which led to multiplicity of e-Health applications [24]. Currently, e-Health comprises of a whole range of services or systems at the edge of healthcare and information technology: telemedicine (remote health care delivery using telecommunication and information technology); electronic health records (electronic health information about a patient or individual); consumer health informatics (use of medical informatics to analyze consumer needs for information); health knowledge management (capturing, describing, organizing, sharing, and effectively using healthcare knowledge); medical decision support systems (interactive expert systems that assists health professionals

with decision making tasks); mHealth (mobile health i.e. use of mobile devices for different applications in healthcare) [24]. The underlying factor in all these technologies is the digitization of data. Without the data digitization, all these technologies and for that matter e-Health would not have been possible. In that regard, the term (e-Health) suggests digital health information in contrast to the paper-based health information. The term 'health' does not solely refer to medicine, disease, or healthcare but also comprises of public health and healthcare [25]. Public health is geared towards preventing and responding to diseases in populations by governments; healthcare is geared towards individual patients and the treatment of disease [25]. This indicates that e-Health involves all facets of health and not only healthcare

Biometrics in healthcare

Biometrics is yet to make the expected impact within the healthcare environment [39]. The adoption of biometric technology in health care is gaining ground within the industry as pressure increases on healthcare providers to reduce fraud, to provide secure access to medical records and facilities, to reduce costs, and to facilitate easier access to medical records [39], [40]. The adoption of biometrics in health care goes along with the adoption of electronic health record (EHR) system; as EHR makes the use of biometrics more efficient and effective [9]. As a consequence of the adoption of EHR, it is now easy for health professionals to view or tamper with a patient's record [41]. A secure authentication system in the form of biometric technology is as a result adopted by most health care organizations to meet governmental regulations [41]. Biometrics is concerned with automated authentication of individuals based on their distinguishing physiological or behavioral characteristics [12], [42]–[44]. The current nature of biometric technology adopted within the health industry is based on physiological characteristics and multi-biometric systems [35]. The use of fingerprint technology to authenticate and protect medical records against unauthorized users is mentioned in [45]. The authors make use of fingerprint verification among other technologies to ensure that access to Picture Archiving and Communication System (PACS) or Radiology Information System (RIS) is done by authorized users [45]. PACS are computers or networks concerned with the storage, retrieval, distribution and presentation of medical images [45]. Fingerprint biometrics in this case, provides the needed security measure to properly authenticate users who access the storage or network, thus ensuring the privacy and safekeeping of medical images. The authors of [46] proposed a framework that consists of four types of biometric identifiers (i.e. fingerprint, iris, retina, DNA). The framework makes use of these biometric characteristics of the patient that distinctively identifies them to their complete electronic health record. In [47], authors integrate fingerprint biometrics in smart card as an authentication measure to reduce impersonation attacks. The aim is to address privacy issues within medical smart cards. The fingerprint helps in E-Health Security Requirements Data Confidentiality Data Integrity Data Authenticity Authentication Encryption Figure 2: Model of e-health security requirements 15 authenticating users' access to medical information that is stored in patients' medical smart cards. Again, in [41], voice biometrics combined with on-line signature is used as authentication mechanism and also improve authentication performance. The biometric-based system provides the necessary security for access to patients' records and ensures patients' privacy in the process. The trend seen within the biometric industry has been continuous biometrics and by which the state- of-the-art of continuous biometrics has traditionally been known to employ unimodal or bi-modal techniques [35]. However, other potential biometric modalities are been researched into within the health care industry based on biosignals. Within the medical settings, the biosignals can be easily captured by biomedical devices in homes, ambulances, or medical centers as part of patient monitoring. Some of the biosignals that is receiving a lot of attention in terms of research are; electrocardiogram (ECG), photoplethysmography (PPG), and electroencephalography (EEG) [48]– [50]. ECG is a diagnostic tool that measures and records the electrical activity of the heart in detail [51]. The EEG is a signal that is represents the sum of the electrical activity of the functioning human brain [48]. Photoplethysmography (PPG) is a simple and low-cost optical technique that can be used to detect blood volume changes in microvascular bed of tissue [52]. In [53], ECG signal is employed in data authentication approach to reduce key exchange overhead. The ECG biometric signal is used as a security scheme to provide secure communication inside body area network (BAN). In their approach, sensors within a BAN also employ the biometric authentication to differentiate which person they belong to. Additionally, in [35], the authors present a biometric framework based on ECG signals. Their approach is for continuous identity verification using ECG signals to enhance security of health information systems. In [50], the authors presents a key agreement protocol which allows sensors to agree on symmetric cryptographic key for securing communication in sensor network. The authors use physiological features i.e. PPG to encrypt and decrypt cryptographic keys communicated within the network thereby ensuring security. The development of mobile health (m-Health) technologies in the form of wearable medical devices and body sensor network (BSN) technologies have paved the way for the increase use of biometrics in health care services. The health industry is receiving a lot of attention in the use of wearable biometric sensors for monitoring various health related issues.

Biometric user authentication and encryption

A biometric system for user authentication measures biometric features of individuals to form a database of biometric templates for subsequent recognition process based on comparison. As such an unencrypted biometric

data or template presents the same vulnerabilities as unencrypted password based system. This could give an opportunity to an adversary who gains access and obtains information to attack the system thereby compromising the security of the system. In terms of algorithms or methods used for user authentication purposes, column 2 of table 8 in Appendix A gives a summary in that regard as reported by selected studies. Our review shows that a number of the reviewed papers apply hash function operations to the biometric data for user authentication purposes. In this, some studies apply biohashing techniques data whiles others apply one-way hash functions to the biometric before authenticating users. Biohashing is a technique of encrypting biometric data by using one-way cryptographic hash function such as SHA-256. It generates a random vector of bits from a user/patient's biometric features to produce user specific biocode [82]. In other words, it maps a user's biometric features randomly onto binary strings with user specific tokenized random numbers [97]. Biohashing is one-way and non-invertible transformation in that there is no way to get the user specific code without having both token and user biometric data [98]. Application of biohashing algorithm ensures the anonymity of users' biometric data.

Conclusion

Electronic healthcare leverages on Information and Communications Technology (ICT) to improve on the efficiency of health service, reduce cost, ensures safety, and help reach out to thousands of patients or healthcare consumers outside the confines of health care establishments. The pervasiveness of ICT makes it indispensable in healthcare especially in the face of developments in internet technologies, computer and telecommunication systems. These developments introduce privacy and security concerns in healthcare systems. Maintaining security and privacy in healthcare systems therefore becomes extremely important as when patients' sensitive information get disclosed could have serious damaging effect. Information security with respect to healthcare data security and patients' privacy is an essential requirement in the healthcare sector. Traditional authentication mechanism such as passwords and access cards may not be very appropriate for addressing the current electronic health care security and privacy challenges. Providing efficient and convenient authentication mechanism as well as providing security to data communication goes a long way to address security requirements posed by electronic healthcare. In this context, biometrics has proven to address the issue effectively. Generally, traditional forms of biometric technology have been applied in several health applications or systems ranging from unimodal to multimodal systems, continuous and unobtrusive authentication approaches, and in wireless sensor networks to secure data communication.

References

1.G. Bai and Y. Guo, "A general architecture for developing a sustainable elderly care e-health system," in 2011 8th International Conference on Service Systems and Service Management (ICSSSM), 2011, pp. 1–6.
2. S. Y. Kwankam, "What e-Health can offer," Bull. World Health Organ., vol. 82, no. 10, pp. 800– 802, Oct. 2004.
3.G. Eysenbach, "What is e-health?," J. Med. Internet Res., vol. 3, no. 2, Jun. 2001.
4.S. K. Sharma, H. Xu, N. Wickramasinghe, and N. Ahmed, "Electronic healthcare: issues and challenges," Int. J. Electron. Healthc., vol. 2, no. 1, pp. 50–65, Jan. 2006.
5.A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," Int. J. Internet Enterp. Manag., vol. 6, no. 4, pp. 279–314, Jan. 2010.
6.K. S, L. J, and P. G, "The challenge for security and privacy services in distributed health settings.," Stud. Health Technol. Inform., vol. 134, pp. 113–125, Dec. 2007.
7.K. S. Kwak, S. Ullah, N. Ullah, An Overview of IEEE 802.15.6 standard, Invited paper for presentation in ISABEL 2010
8. R. Cavallari, F. Martelli, R. Rosini, C. Buratti and R. Verdone, A survey on Wireless Body Area Networks: Technologies and Design Challenges, vol.16, no. 3, pp. 1635-1656,Oct. 2014 [4] P.Kumar and H-J Lee, Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, 12, pp.55-91,(www.mdpi.org/sensors), Sensors 2012
9. A. Sawand, S. Djahel, Z. Zhang, F. Nait-Abdesselam, Towards Energy-Efficient and Trustworthy eHealth Monitoring System, Selected Paper from IEEE/CIC ICCC(China Communications)January 2014
10.Ganesh Borse and Himangi Pande, The Role of Virtual Doctor Server on Wireless Body Area Network, pp. 1-6, Fourth Post Graduate Conference:iPGCON-2015 [7] O.M.Ayoub, I.Aleem,. Utilization of Body Sensor Networks to receive Death Intimation of Residents Registered with Local National Health Services, Extensive Journal of Applied Sciences, EJAS Journal2014-2-1,1-5 [8] K.R. Pragnya,J.K.Chaitanya, Wireless Sensor Network Based Healthcare Monitoring System for Homely Elders, doi:10.7323/ijaet/v6_iss5_14, International Journal of Advances in Engineering & Technology, Nov.2013 [9] F.A.Khan,A.Ali,H.Abbas,N.A.H.Haldar
11.R.sudha,M.devipriya.,2017.CiiT International Journal of Biometrics and Bioinformatimcs,,vol 9,No 7.
12.R.sudha,M.devipriya.,Enchanced bio-trusted anonymous authentication routing technique of wireless body area network,Sep.2017.Biometric Research 2016;Special issue:S276-S282.