International Journal of Engineering & Technology, 7 (2.32) (2018) 269-274

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Review on the Security Issues in Human Sensor Networks for Healthcare Applications

Radhika Rani Chintala[1], Narasinga Rao M R[2], Somu Venkateswarlu[3]

[1,2]Department of CSE, KLEF, Vaddeswaram, Guntur, Andhra Pradesh, India
[3]Sreyas Institute of Engineering and Technology, Hyderabad, Andhra Pradesh, India
**Corresponding author E-mail: radhikarani_cse@kluniversity.in*

Abstract

Human Sensor Network (HSN) is an emerging technology that allows to remotely monitor, gather and maintain the information of patient’s health parameters using bio-sensors. The bio-sensors are either implantable or wearable or may be stitched on the clothes of a patient.The collected health information is processed and maintained in a database server. The information from the database can be accessed by the users such as doctors, health servants, government, insurance agencies and by the patient or his relatives. Since, the information collected is related to thepatient’s private health record, it is required to be safely stored and protected from an unauthorized access. Thus, Security and Privacy are the key issues in HSNs.In this paper, the infrastructure-based and adhoc-based communication architecture of HSN and challenges and measures of security and privacy issues have been reviewed.

Keywords: *Human Sensor Network (HSN), Security, Privacy, Healthcare systems.*

1. Introduction

As per the survey conducted by World Health Organization (WHO), Heart related Disease (HRD) is the major reason for the loss of human life. It is assessed that the HRD related deaths will reach up to nearly 240 lakhs by 2030. Other than this, more than 25 crores of individuals will experience the ill effects of diabetes and the rateof HRD patients or diabetics will rise. The number of people whose age is greater than 60 will raise in future [1].HSN is a procedure that observes, remotely, the status of patient health and collects the data from the sensors kept in patient body. All these sensors and actuators will create a wireless network.The biosensors are either implantable or wearable or may be stitched on the clothes of a patient to record certain body parameters, for example, heart rate, electro cardio gram (ECG), Plasmon Biosensor, electroencephalogram (EEG), blood pressure (BP), body dynamics, breath rate levels, temperature, blood glucose [2] etc. These sensors are specifically used for exclusive purposes to meet the prerequisites of user community. The IEEE 802.15.6 has proposed scientific categorization for HSNnodes as per their work inside the human body [3]. The node can be categorized in the way they are used:

Implant Node: The node that is kept below the skin or inside the body tissue.
Body Surface Node: It is placed either on body surface or two centimeters far from the human body.
External Node: It is the node that is placed atleast500 cm far from the human body.

Three types of nodes are generally used in HSNs.

Coordinator: This node communicates the data to the outside world securely. The Personal Digital Assistant (PDA) is the coordinator of a HSN in which all the nodes can communicate among themselves.
End Nodes: These nodes are confined to execute the embedded application. Theycan't transmit messages among the nodes.
Relay: The relay node comprises of a parent and childnodes and relay messages. These nodes sense the message communicated by other nodes and relays the same further to longer distances.
Actuators follow up on the data received from the sensor nodes and act as per the directions. The actuator is set up with built in repository and regulates legitimate dosages of hypoglycemic agent to help the glucose level estimations,for example patients with diabetes [4]. It can be additionally utilized in a few different fields and applications, like, observing contamination levels, physiological and therapeutic checking, human PC collaboration and training. Fig. 1 shows the placement of different sensors that can communicate through a HSN.

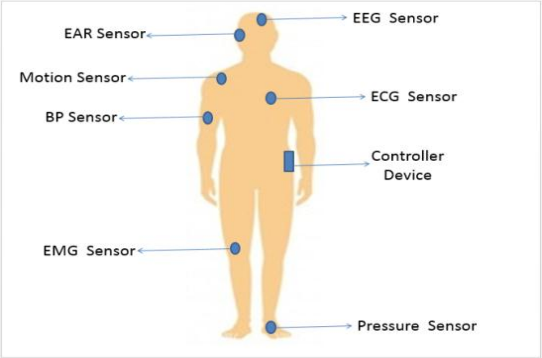


Fig.1 Placement of sensors that communicate by the means of a HSN.

Anysmart device can remotely read the data sensed by the sensors or a PDA between the patient and a medical staff. The decisions taken by the medical staff must be secured and should not be accessed by unauthorized persons as it may be pose a threat to the patient's life [5], for example change of drug's dosage or treatment methods, if received by the wrong person [6]. Hence, stringent security mechanisms are compulsory to ensure confidentiality, authentication, secure group management, integrityand reliability.

Several benefits as well as challenges are offered by HSN application to healthcare division. These advantages allow us to monitor day to day medical status of patient round the clock without restrictions. The challenges include providing security and privacy to the patient's vital health information. [7,8].

The data sensed and send by these sensors to the hospital data center server may get attacked by the adversary. The adversary may alter the data and pass the modified data to the doctor or server. These changes may endanger the life of the patient. Given the weakness of patient privacy, security ought to be foremost important than the usage of technology in healthcare [9].

2. HSN Applications

HSN applications can be categorized into Medical, Military, Environmental, Home, Sports and other business application areas.

2.1Medical Applications

HSNs are used in medical applications for various purposes like offering interfaces to diagnostics, remotely monitoring the physiological information of a person, drugs administration in medical care centres or hospitals and as a guide to recovery. In upcoming days, HSN will be feasible to screen the patients regularly and suggest the required medication whether they are in hospital, or at home or somewhere else. There will be no need for the patients to get connected with heavy machines to monitor the health status.

2.2 Military Applications

There are various benefits of HSNs when being used in military system. Few military applications of HSN include sensing of the hydration levels, temperature and locality. A soldier's uniform incorporated with a HSN can act as a wearable electronic system that interfaces gadgets such as life care sensors, health observing GPS, and communicate data along soldier's wearable device. The quick positioning, adaptation to non-critical failure and self- association qualities of sensor systems makes them an extremely encouraging detecting method for military. As the HSN is based on the deployment of low cost and one-use throwaway sensors, damage of few nodes by unreceptive activities do not influence the military applications when compared to the traditional sensor, which gives an improved advantages of HSN in the battlefield.

2.3 Environmental Applications

Few HSN applications regarding environment include observing the environmental changes that may show influence on crops and domestic animals; tracing the movements of insects, birds and small animals; fire detection in forests; checking water system; planetary investigation; pollution reading; atmospheric and geophysical study; biochemical and flood detection.

2.4 Home Applications

There are many benefits of using HSNs in Home applications. A few of them include managing the home appliances such as ovens, vacuum cleaners, freezers, geezers and lighting systems. The sensors within these domestic appliances can communicate among themselves and with outer network by using satellite or internet. The HSNs permits the end-users to efficiently control the home appliances remotely or locally.

2.5 Lifestyle & Sports Applications

HSNs provide new facilities for remote body network systems that include providing support for navigation in cars and while doing walking, gallery or city control, entertaining system that is wearable, newborn child observing, heart rate and performance observing in sports, remote cash card that is used to show the recent cash transactions, balance checking, etc.

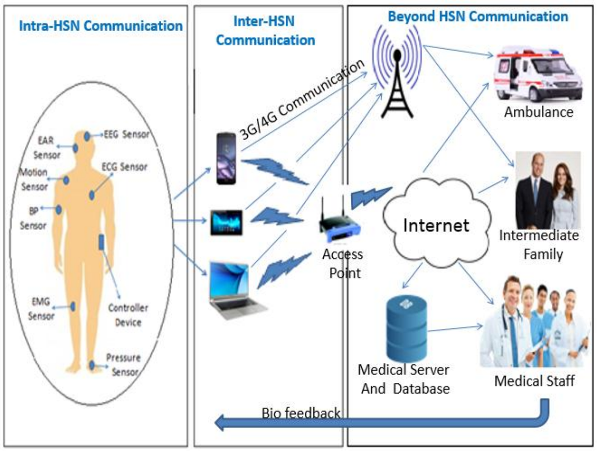
2.6 Other Business Applications

Few business applications include building virtual consoles, checking material exhaustion, building virtual consoles, supervising stock, observing item quality, developing keen office spaces, ecological control in office structures, Controlling robots, manufacturing plant process control and mechanization, machine analysis, transportation, production line instrumentation, vehicle identification and following and instrumentation of semiconductor handling chambers.

3. HSNCommunication Architecture

Inorder to employ the security mechanisms in HSN, the communication structure/organization/configuration within and out of the networks must primarily be understood. This section deals with the communication architecture of HSN.

Fig. 2 portrays that the electronic gadgets are spread all through in a network, with the area of the gadget being attached to a specific application. As the human being moves constantly, so the position of sensors is dynamic. So HSNs are not fixed area networks [2]. In the majority of the HSNs framework, the architectural design contains three different levels as given:



=**Fig**.2 Communication levels in HSN.

i. Level-1: Intra-HSN communication: In this level, the communication among the sensors is limitedwithin the patient's body. The signals inside the coverage area of the sensor travel till the access point available in level 2, through smart devices.

ii. Level-2: Inter-HSN communication: Basically, communication at this level endeavors to associate HSNs with different systems or networks, hence data can be effortlessly be recovered through different media, for example, the web [9].

iii Level 3: Beyond-HSN Communication: This level of Communication is suitable for city areas [6]. A medical server and database is important in level 3 communication, as it stores the medical history of the patient along with his profile. Medical staff as well as patients can be cautioned to anemergency circumstance through Internet or Short Message Service (SMS). Level 3 additionally takes care of rebuilding of important patient data that can be vital to get ready for suitable treatment [10].

In HSNs, the poor Signal to Noise Ratio (SNR) and limited resources (Energy, computational ability and memory space) of sensors increases the vulnerability to security attacks [9]. The large noise signal present in the channel may cause the loss of data packet. This vulnerability can be utilized by the attacker forharmingHSN network and may affect the operation of entire system. Hence a high level privacy and security system has to be used in HSNs.

4. Security and Privacy requirements of HSNs

HSN systems must maintain particular security methods to assure privacy, confidentiality, security and data integrity of patient's medical information 24*7 [11]. In order to guarantee the security features, HSN framework should apply certain security procedures. Security as well as privacy are the most important features in HSN system. Security indicates that patient's information is secured from unauthorized access while being exchanged, gathered, processing and being stored securely. Privacy is defined as the process that authoritatively controls and monitors the usage of patient's data. Thus, more importance has to be given to shield patient critical data from unauthorized users [12].

Fig. 3 shows a protected component of the information gathering and different purposes of the systems administration including the last where the information can be recovered by just the approved individual and through individual ID methods for unscrambling [13].

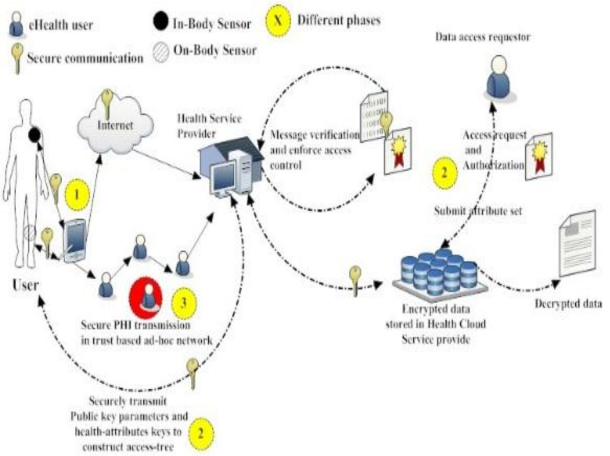

eHealth user
Secure communication
In-Body Sensor
On-Body Sensor
X
Different phases
Data access requestor
Internet
Health Service Provider
Message verification and enforce access control
Access request and Authorization
2
1
User
Submit attribute set
3
Secure PHI transmission in trust based ad-hoc network
Encrypted data stored in Health Cloud Service provide
Decrypted data
Securely transmit Public key parameters and health-attributes keys to construct access-tree
2

Figure 3.Security and privacy in a HSN system.

The privacy and security requirements to ensure the safety of a HSN system and its extensive acceptance by its users are explained below.

Data Confidentiality: Confidentiality of data indicates the security of important information from being exposed, is considered as the primary issue in HSN [13-15].

Data Integrity: Integrity of data refers to the procedures adopted to secure the message, its consistency and correctness. It applies to both single messages and in addition multiple messages [9]. It is important that the data not be available and changed by a potential enemy by usingauthentication protocols [16].

Data Freshness: Either by replaying or by recording the enemy can't affect the confidentiality and integrity of patient information, if proper Data Freshness techniques are employed.

a. Strong freshness guarantees order of the frames and delay.
b. Weak freshness guarantees order of the frames only [14].

Accessibility of the network: It suggests a medicalconsultant with effective access to a patient's data. It also ensures that the network is up and live always [9,11]. HSN operations may be switched if the network failure occurs.

Data Authentication: Nodes inside a HSN must be able to confirm that the data is sent or received from a known server.

Secure Management: To deliverdistribution of key to a HSN, the decoding and encoding operation requires need to be controlled securely by the organizer. The organizer is responsible to include and expel HSNnodes in secureway.

Trustworthiness: The data of the patient stored in the server must be safe and secure. For this one can use Error-Correcting Codes while storing the data in the server. Thus there won't be any failure in retrieving the correct information, and thus a critical issue can be avoided [7].

Secure Localization: Most of the HSN applications require exact location of the patient. Else possibility of replaying to a fake signal is fair [13].

Accountability: Medicalserver and database administrator should take the accountability of securing the patient data in the server [17].

Flexibility: The patient should have the flexibility on transferring his access controls within or outside HSN (whenever he changes the doctor or hospital) [16].

Protection guidelines and consistence prerequisite: At present there are distinctive sets of polices for security throughout the world. The American Health Insurance Portability and Accountability Act (HIPAA)is a set of directions for medical staff and hospitals. It is designed to confirm that a patient's medical records are secure [18].

The Health Information Technology for Economic and Clinical Health (HITECH) Act, develops how data innovation can securely be utilized to gather, store, offer and utilize delicate patient data. The Act takes note of that the individuals who are protectors of health information of patient must contact the individual influenced if a security issue emerges [19]. This is a decent case of how such principles and controls ought to be authorized at a bigger extension if any nation receives the HSN innovation. There are scarce conditions, for instance a medicinal crisis that may require the unveiling of patient wellbeing data to specialists on call [20]. Table1 demonstrates the significant security dangers, security necessities and the conceivable security arrangements when utilizing a WBAN.

Table 1. Security threats and possible security solutions in WBAN.

Security threats	Security requirements	Possible security solutions
Unauthorized access	Key establishment and trust setup	Random key distribution and Public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption and Access control
Message modification	Integrity and authenticity	Keyed secure hash function and Digital signature
Denial of Service (DOS)	Availability	Intrusion detection systems & redundancy
Compromised node	Resilience to node compromise	Inconsistency detection and node revocation and Tamper proofing
Routing attacks	Secure routing	Secure routing protocols
Intrusions and malicious activities	Secure group management, Intrusion detection Systems and secure data aggregation	Secure group communication, Intrusion detection systems

4.1. HSN Security Threats

HSNs are exposed against an immense number of threats and attacks which could hack into the system. Therefore privacy

&security measures have to be taken seriously.Attackers may focus on the accessibility of a HSN by catching or disabling a specific node, this sometimes brings about loss of a patient's life. An enemy can likewise utilize tampering and jamming for blocking the entire HSN [21] which can lead to packet loss.It is feasible that an attacker may physically damage, intrude into HSN to obtain a patient's health data. It can likewise utilize a flooding strategy to debilitate the memory by over and again sending additional superfluous packets, which the HSN can't deal with. This makes the authentic clients not to get access to theirservices [22]. It should be possible through Denial of Service (DoS) attack lessen the system's ability of giving the important services. Table 1 demonstrates the security dangers and conceivable security solutions that can be utilized as a part of HSN.

4.2. The Current Security Measures

A few security solutions for HSN have been proposed and they are discussed here.

4.2.1. TinySec:

TinySec is a solution to achieve link layer encoding and data authentication in Biomedical Sensors Networks (BSNs). This technique is part of TinyOS release. It relies on a single key by default thatis programmed into sensor nodes before being deployed. This technique provides a certain level ofsecurity. But is can’t protect against physical capture of node as it is shared [2].

4.2.2. Biometrics:

This strategy is broadly used to secure communication in biomedical sensor systems utilizing biometrics [23].

4.2.3. IEEE 802.15.4 and IEEE 802.15.6 Security Protocols:

The security suites are arranged into two fundamental modes: secured and unsecured mode. Unsecured mode implies that no security suite has chosen. The standard characterizes 8 exclusive security suites. The first is the Null suite that gives no security, while the others are arranged by the distinctive security tiers. A definite depiction of this standard is available in [24]. Further, in 2012, the better form, standard IEEE 802.15.6 had been endorsed [25]. This most current standard endeavors to give a universal consistent low power, small distance wireless communication around a human. It encourages an extensive variety of rates fluctuating from narrow band (75.9 Kbps) to ultra wide band (15.6 Mbps), contingent upon need [26].

4.2.4. Zigbee Security Services:

ZigBee has given a new meaning to ultra-low power wireless communication. The ZigBee network layer characterizes additional security services including forms for validation and key-exchange and IEEE802.15.4. The ZigBee standard distinguishes a reliable center that controls allowing the nodes to join or leave the network [24].

4.2.5. Bluetooth Security Protocols:

It contains of several protocols such as Baseband, Link Manager Protocol (LMP) andLogical Link Control and Adaptation (L2CAP)[27].

4.2.6. Wireless Security Protocols:

Numerous security protocols are developed to protect the wireless network such as Wired Equivalent Privacy (WEP), Wi–Fi Protected Access (WPA) and Wi–Fi Protected Access version 2 (WPA-2).

4.2.7. Hardware Encryption:

Hardware encryption is implemented by use of a ChipCon 2420 ZigBee compliant RF Transceiver. The CC2420 is capable of executing IEEE 802.15.4 security operations with AES encryption by utilizing 128-bit keys. The operations utilize a counter called, CTR, mode of decryption and encryption [25].

4.2.8. Elliptic Curve Cryptography (ECC):

This technique is a choice for public key cryptography in HSN. The main use of Elliptic Curve Cryptography (ECC) lies in its elements offering high computation, reduced key-size, andsignatures which are compact [28].

4.2.9. Encryption Techniques:

HSN provides the required security by deigning the network to encode the entire data with different keys. It offers high form of security by three different mechanisms Symmetric key encryption, Conventional Public Key Encryption and Identity Based Encryption [29].

5. Research in HSN Security and Privacy

Because of severe resource constraints in HSN, initial security schemes are symmetric cryptosystems which provide weak security. The sensor's nodemaindrawback is its restricted computation energy, communication rate and memory space [30].

Much research has been led to think about the security issues in HSNs [31–35]. Research directed by Lee et al. [36] proposed encryption methodbased on Elliptic Curve Cryptography (ECC) in medical systems. This method was separated into three primary stages: Registration, Verification and key-exchange. The conclusions said that the method accomplishes greater reliability and gives better security to the method. Zhao [37] proposed ID (identity) based effective and covert verification method(no certificate is demanded while communicating) for HSNs utilizing ECC. It provides mutual authentication between client and server. The findings demonstrated that the execution examination of the validation plot is enhanced by 50.58% in the client side and 3.87% in the server side.

An approach for securing communication in HSNs can be obtained by means of the utilization of biometrics; the body of patient is used to direct cryptographic keys for the nodes secured to the body itself [38]. This defends the patient’s information security and privacy of patient’s data. Mana et al. [39] proposed a biometric approach utilizing the information from heartbeat. This strategy depends on symmetric key dispersion design. The detections demonstrated that the proposed approach could be utilized to protect cipher key distribution among e-health communications of HSNs. The outcomes demonstrated that utilizing exclusive biometric properties is useful for the purpose of identification.

Salem et al. [40] proposed a method for anomaly identification in HSN. The proposed design links machine learning (ML)& data mining algorithms with latest sensors. It can recognize sporadic variations and the defective sensor information in the physiological parameters of the patient. This empowers the systems to guarantee trustworthy operations and ongoing global checking from smartelectronics devices. Scientists have also analyzed protection of patient's information in HSN and different strategies made to secure it from outside interruptions [41].Mana et al. [39] set forth procedures to guarantee location security in HSN. The establishment of theprotocol is transitory aliases. Accordingly, both the destination and source in the HSNs are secured on mobiledevices. Barua et al. [41] recommended patient-centric control (PEACE) plan to get the personal health information proficiently and safely. This approach secures privacy by utilizing digital signature and pseudo-identity schemes. Their discoveries demonstrate that the approach gives a truly necessary security prerequisite.

6. Discussion and Recommendations

HSNs have turned out to be an incredible resource in the healthcare services. For any healthcare application, security and protection issues must be settled immediately to stop a disaster in the public. Authentication and security measures must be applied to manage the security threats.

Authentication schemes can be advantageous in deciding the origin of information, whether it is from the authorized individual. A centralized controller is required in HSNs, for transmission of data, generated by various sensors the patient is wearing. Authentication, firewalls, routers and other types of security devices can be used as security measures and to monitor the network traffic.Beside concerns in the design of sensors, focus should also be on their cost and size. They must be able to transfer the data to a couple of meters. And should also support multiple frequency of operation, should support patient requirements in context of reliability, power usage and data rate.

With the feasibility in ECCof HSN, it is fundamental to explore the usage of Okamoto's identification protocol.

One more method, which is still under development, to avoid intrusion is Intrusion Detection Systems(IDS). This technique is simulated by the biological insusceptible system that makes use of Negative Selection Algorithm(NSA). This application improves the execution of a HSN to operate regardless of the presence of negotiatednode. IDS in HSNs represents a testing issue, particularly when proactive defense components need to acquire assaults.Digital forensics is the way toward researching to distinguish, follow and investigate illicit and deceitful events and give proof to implement laws against such occasions. Interruption Detection and Prevention Systems (IDPS) can be utilized to give the data expected to identify suspicious early activities and may even prompt aversion of severe damage. An IDPS can be considered as a helpful tool for gathering digital confirmations that might be utilized as a part of a court and law and thus, the systems activities can be effortlessly observed.

One more vitalprivacy and security measure is to educatepublic about HSN's security and make them to know the after effects.

7. Conclusion

Now a days sensors are often implanted on human body in order to enhance quality of their life. The work presented in this paper, reviewed the organization of HSNs by considering privacy and security. It has discussed about communication architecture of HSN, the privacy &security in HSN and the threats to the actuators and sensors.Also discussed about the attacks in HSN. Digital Forensics and IDPS and other safety measures are also discussed for ensuring compliance with the law and the moral behaviour of medical staff& system operators who have access to the patient's information and records.The health care and public personnel have to be aware of the challenges that are present in the usage of HSN, to guarantee the secured delivery of patient's health information at all the levels.

References

[1] C.D. Mathers and D. Loncar, "Updated projections of global mortality and burden of disease, 2002–2030: data sources, methods and results",PLos Med (World Health Org), pp.1-8, 2006.

[2] D.A. Sharma, "Wireless health care monitoring system with data security and privacy",Int J Res ComputEng Electron, Vol.2, No.2, 2013.

[3] Yazdandoost KY andSayrafian-Pour K., "Channel model for body area network (BAN)", IEEE P802, 15, 08-0780; 2009.

[4] P.G. Naranjo, M. Shojafar, H. Mostafaei, Z. Pooranian and E. Baccarelli, "P-SEP: a prolong stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks", J Supercomput, 1–23, 2016.

[5] J. Wang, Z. Zhang, K. Xu, Y. Yin and P. Guo, "A research on security and privacy issues for patient related data in medical organization system", Int J Security Appl, Vol. 7, No. 4, pp. 287-298, 2013.

[6] G.V. Crosby, T. Ghosh, R. Murimi and C.A. Chin, "Wireless body area networks for healthcare: a survey", Int J Ad Hoc, Sensor Ubiquitous Comput, Vol. 3, No.3, pp. 1-26, 2012.

[7] O.U. Rehman, N. Javaid, A. Bibi and Z.A. Khan, "Performance study of localization techniques in wireless body area sensor networks", 11th IEEE international conference on trust, security and privacy in computing and communications, pp. 1968-1975, 2012.

[8] S. Pathania and N. Bilandi, "Security issues in wireless body area network", Int J ComputSci Mobile Comput, Vol. 3, No.4, pp. 1171-1178, 2014.

[9] M. Al Ameen, J. Liu and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications", J Med Syst, Vol. 36, No.1, pp. 93-101, 2012.

[10] Radhika Rani Chintala, Nunna Krishna Chaitanya and DheerajDevanaboina, "Medical Virtual Physical Structures Using Homomorphic Encryption Techniques", International Journal of Pure and Applied Mathematics, Vol. 116, No. 5, pp. 87-92, 2017.

[11] R. Kumar and R. Mukesh, "State of the art: security in wireless body area networks", Int J ComputSciEngTechnol (IJCSET), Vol. 4, No.5, pp. 622-630, 2013.

[12] Radhika Rani Chintala, MR NarasingaRao, S. Venkateswarlu, "Design of a Secure System for Reading Patient's Data Using Medical Sensor Networks", Journal of Chemical and Pharmaceutical Sciences(JCHPS), Vol. 10, No.1, 673-679, 2017.

[13] M.J. Kargar, S. Ghasemi, O. Rahimi, "Wireless body area network: from electronic health security perspective", Int J Reliable Quality E-Healthcare (IJRQEH), Vol. 2, No. 4, pp. 38-47, 2013.

[14] N.D. Han, L. Han, D.M. Tuan, H.P. In, M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks", InfSci, 284, pp. 157-166, 2014.

[15] Tewari, P. Verma, "Security and privacy in E-healthcare monitoring with WBAN: a critical review", Int J ComputAppl, Vol. 136, No. 11, 2016.

[16] N. Fatema, R. Brad, "Security requirements, counterattacks and projects in healthcare applications using WSNs – a review", Int J ComputNetwork Commun (IJCNAC), Vol. 2, No. 2, 2014.

[17] S.S. Javadi, M.A. Razzaque, "Security and privacy in wireless body area networks for health care applicationsWireless networks and security", Springer, Berlin Heidelberg, pp. 165-187, 2013.

[18] Office for Civil Rights, United State Department of Health and Human Services. Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>

[19] Health Information Technology for Economic and Clinical Health Act HITECH. Ways And Means and Science Technology <http://waysandmeans.house.gov/media/pdf/110/hit2.pdf> [accessed 10.11.15].

[20] K.J. Kim, S.P. Hong, "Privacy care architecture in wireless sensor networks", Int J DistribSensNetw, pp. 1-8, 2013, ArticlePDF (463KB)

[21] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, K.S. Kwak, "A comprehensive survey of wireless body area networks", J Med Syst, Vol. 36, No. 3, pp. 1065-1094, 2012.

[22] R. Latif, H. Abbas, S. Assar, "Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review", J Med Syst, Vol. 38, No. 11, pp. 1, 2014.

[23] S.N. Ramli, R. Ahmad, M.F. Abdollah, E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)", 15th international conference on advanced communication technology (ICACT), pp. 998-1001, 2013.

[24] S. Saleem, S. Ullah, K.S. Kwak, “A study of IEEE 802.15.4 security framework for wireless body area networks”, Sensors, Vol. 11, No. 2, pp. 1383-1395, 2011.

[25] G.V. Crosby, T. Ghosh, R. Murimi, C.A. Chin, “Wireless body area networks for healthcare: a survey”, In J Ad Hoc, Sensor Ubiquitous Comput, Vol. 3, No. 3, pp. 1, 2012.

[26] S. Ullah, M. Mohaisen, M.A. Alnuem, “A review of IEEE 802.15.6 MAC, PHY, and security specifications”, Int J Distrib-SensNetw, pp. 24, 2013.

[27] Ahmadi, M. Shojafar, S.F. Hajeforosh, M. Dehghan, M. Singhal, “An efficient routing algorithm to preserve k-coverage in wireless sensor networks”, J Supercomput, Vol. 68, No. 2, pp. 599-623, 2014.

[28] Z. Zhao, “An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem”, J Med Syst, Vol. 38, No. 2, pp. 1-7, 2014.

[29] S.H. Ali, “Novel approach for generating the key of stream cipher system using random forest data mining algorithm” Sixth IEEE international conference on developments in eSystemsEngineering (DeSE), pp. 259-269, 2013.

[30] Y. Tian, Y. Peng, X. Peng, H. Li, “An attribute-based encryption scheme with revocation for fine-grained access control in wireless body area networks”, Int J DistribSensNetw, Vol. 11 ,2014.

[31] J. Liu, Z. Zhang, R. Sun, K.S. Kwak, “An efficient certificateless remote anonymous authentication scheme for wireless body area networks”, IEEE international conference on communications (ICC), pp. 3404-3408, 2012.

[32] Lee YS, Alasaarela E, Lee H., “Efficient Encryption Scheme based on Elliptic Curve Cryptography (ECC) and Symmetric algorithm in Wireless Body Area Networks (WBANs)”, pp. 36–9, 2013.

[33] T. Kovačević, T. Perković, M. Čagalj, “LIRA: a new key deployment scheme for wireless body area networks”, IEEE international conference on software tele-communications and computer networks (SoftCOM), pp.1-6, 2013.

[34] H. Xiong, “Cost-effective scalable and anonymous certificateless remote authentication protocol”, IEEE Trans Inf Forensics Secur, pp. 2327-2339, 2014.

[35] X. Liang, M. Barua, R. Lu, X. Lin, X.S. Shen, “HealthShare: achieving secure and privacy-preserving health information sharing through health social networks”, ComputCommun, Vol. 35, No. 15, pp. 1910-1920, 2012.

[36] Lee YS, Alasaarela E, Lee H, “Secure key management scheme based on ECC algorithm for patient’s medical information in healthcare system”, The IEEE international conference on information networking 2014 (ICOIN2014), pp. 453-457, 2014.

[37] Z. Zhao,” An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem”, J Med Syst, Vol. 38, No. 2, pp. 1-7, 2014.

[38] J. Zhou, Z. Cao, X. Dong, N. Xiong, A.V. Vasilakos, “4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks”, InfSci, 314, pp. 255-276, 2015.

[39] M. Mana, M. Feham, B.A. Bensaber, “Trust key management scheme for wireless body area networks”, IJ Network Security, Vol. 12, No. 2, pp. 75-83, 2011.

[40] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, B. Furht, “Anomaly detection in medical wireless sensor networks using SVM and linear regression models”, Int J E-Health Med Commun (IJEHMC), Vol. 5, No. 1, pp. 20-45, 2014.

[41] M. Barua, X. Liang, R. Lu, X. Shen, “PEACE: an efficient and secure patient-centric access control scheme for eHealth care system”, IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp. 970-975, 2011.