Security and Privacy in E-Healthcare Monitoring with WBAN: A Critical Review

Anurag Tewari
Computer Science and Engg. Department, PSIT College of Engineering, Kanpur, Uttar Pradesh, India

Prabhat Verma
Computer Science and Engg. Department, Harcourt Butler Technological Institute, Kanpur, Uttar Pradesh,India

ABSTRACT
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.

General Terms
Sensors, Safety Mechanisms, Wireless Body Area Network.

Keywords
WBANs, Security, Privacy, Healthcare, Sensors, Features, Applications**,** Cloud Computing.

1. INTRODUCTION
In current scenario of technological advancement it is the duty of humans to develop & provide better life-style to all human-beings irrespective of their age, gender or geographical location. As HEALTH IS WEALTH is well known and true forever. So taking care of sickness sensitive people while without disturbing them from their regular routines is must. In technically ancient era of communication only wired media was present. It lacked mobility & required big expense related to maintenance of large cables. Now everything in communication technology has become wireless same is true for healthcare systems also.

As Science and Technology has been evolved to create a human like machine means a machine which can sense, think and behave more or less like a human. During this technical advancement creation of artificial but intelligent sensing system (sensors) is the most prominent and challenging invention. These sensors have also attempted to bridge the gap between human and machine interaction. At the present time since last decade these sensors are utilized in the fields of human society in two major areas- Medical and Non-Medical.

These sensing devices (sensors) and their interconnected arrangements are designed to behave interactively but in distributed manner and termed as sensor networks. Due to invention of wireless technology these sensor networks are also developed as wireless sensor networks (WSNs). As humans are able to move everywhere along with its all natural sensors (eyes, nose, ears etc.) in different environmental conditions similarly WSNS are also evolved to behave. A complete new group of sensors are dedicated for the well-being of human body and its network is called as Wireless Body Area Network (WBAN).

In below figure Fig.1 layer L1 contains a user (human-being) along with many sensors (encircled as s) attached. In layer L2 a personal server/ gateway device exists to collect different data sensed by sensors in L1. In layer L3 Internet based clouds/ services exist .This L3 layer also connects user with hospital/medical help by healthcare based cloud.
The main contribution of this paper is to draw attention towards most sensitive and less explored and less solved area of WBAN technology – Information security and data privacy of physiological knowledge of patient and user. This review paper provides collected information from few important researches, survey & review papers on WSN, (Wireless Medical Sensor Network) WMSN & WBAN over a period of 2011 to 2014. Here all the applications, features, limitations of WBAN systems along with their future research possibilities are covered and disclosed. This paper is structured in to 6 sections. II section contains distinguished features of WBANs. In section III few latest applications are discussed. Section IV elaborates Requirement and necessity of Security and Privacy aspects against possible attacks within WBANs. Section V provides an analytic view of recent mechanisms applied to preserve security and privacy within WBANs. Finally section VI concludes this review performed in all previous sections along with future possibilities to make WBAN secure, private as well as efficient.

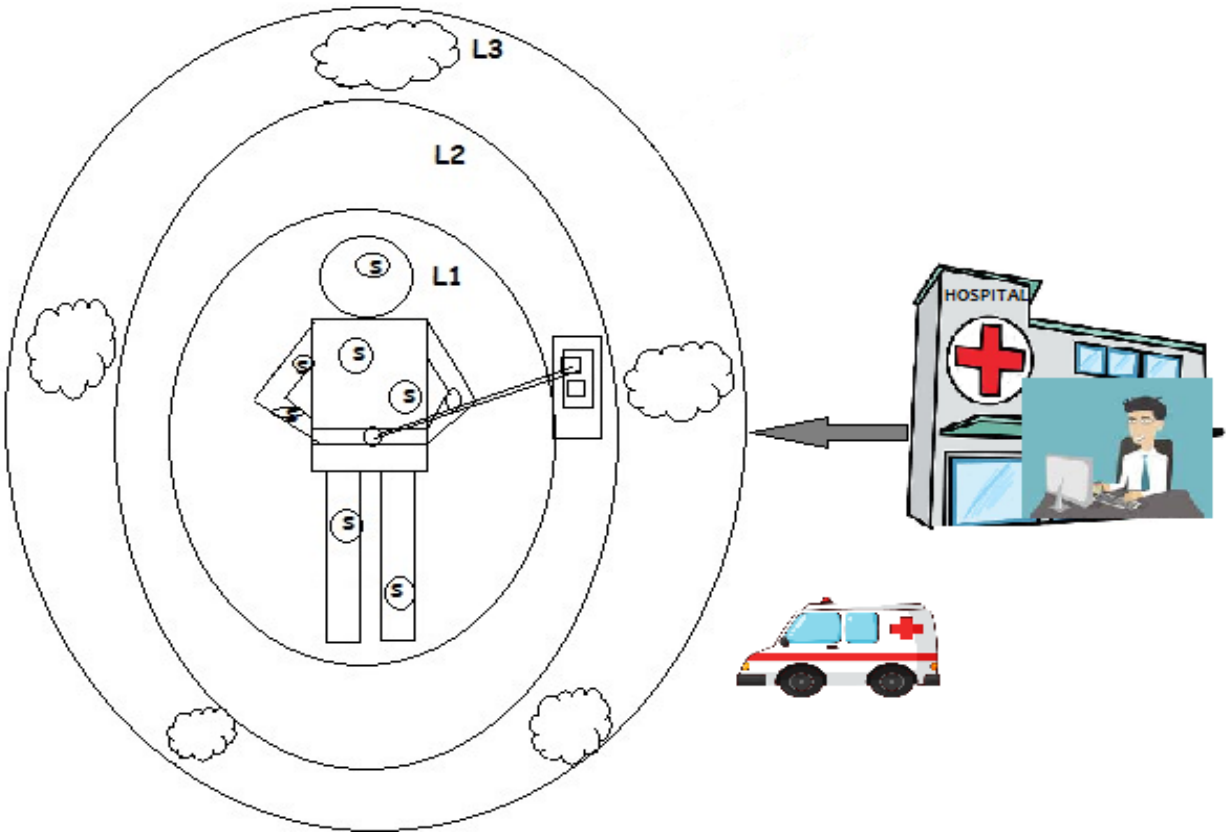

Fig.1 Functional Layer-based architecture of WBAN

2. FEATURES OF WBAN

In this section some unique features of WBAN are covered which give a distinguished shape to WBAN from MANET (Mobile Ad-Hoc Network) & WSN. Interconnected Devices developed and used on, in or around the body of human users generally come under the umbrella of WBANs. Medically Implanted and wearable sensor are extremely popular components of WBAN in E-Healthcare perspectives [1]. WBAN has been standardized by a task group established by IEEE 802 and it is named as IEEE 802.15.6 [1], [2].

Few Important but Unique features who characterize WBAN can be defined as [4]:

1. Human Centric Interactions (Activation): WBANs are directly attached to human body parts to collect data as a collection of sensed information. Human body is very much sensitive as well as reactive to these sensors. So these sensors must be harmless and easily acceptable to human body.
2. Scalability: WBANs are scalable for small scale arrangements. Their size contains at most 10-15 sensors attached in, on or around the body of user. Range of sensors used here in WBANs mainly exists around some 30 to 50 meters.
3. Mobility: It is the most significant feature which made WBANs extremely popular. One can do his/her daily routine work along under supervision of medical helpers.
4. Reliability: This property has values of sampling data-rates of sensing devices used within WBANs. These are comparatively many, stable and high than general sensor networks.
5. Deployment: These networks consist of many sensors connected directly to exit points and gateways. Sensors are localized to form a dense network.
6. Battery Replacement: Battery replacement can be easily performed within sensing devices used in WBANs. But extra care of those sensors which are medically implanted in the body of patient should be taken.
7. Properties of data within sensor: Information collected by sensing device is related to life or death of a dependent human being so it should be secure (encoded), private and permanent as far as possible.
8. Acceptance to Human Body: Sensor devices are machines which are directly fastened to human body so these devise have been made harmless in their functioning for human body.
9. Network Topology: In WBANs generally star, mesh, hybrid or cluster network topologies are used effectively.
10. Others: Bandwidth utilization, technical standardization and other features are defined and utilized within WBANs as per IEEE 802.15.4[3], and a detailed nomenclature gives a well defined functional overview of this special purpose sensor networks.

3. APPLICATIONS OF WBANS IN HEALTHCARE

In human body important organs as well as diseases related to them are covered by WBAN. Many non-intrusive sensors are

medically important inside the body of patients. Remote care of patients is the main feature to explore to the fullest in WBANs supported system. Few recent applications of WBANs to improve the lifestyle of mentally and physically challenged people, people with certain diseases, pregnant women, etc. are developed and used.

The detailed list of applications utilizing WBANs extensively consists of [3] ECG, EEG, ENG, Pulse-Oximeter (SPO^2), drugs delivery, post operative and temperature monitoring, glucose level, toxins status, blood pressure, etc.

(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.
So, paralyzed and immobile patients are monitored remotely without any regular human intervention. On their death occurrence this system also informs the responsible authorities to make necessary arrangements to collect and dispose dead-bodies from specific locations.

(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. It helps in remote health monitoring and performs magnificent health observation of soldiers in battle field. By joining hands with clouds efficiency, scalability and overall performance of WBAN has been raised manifolds.
In this application sensing devices used within WBAN measure values related to biological study of physiology and then these observed measurements are sent to different servers located at the cloud of hospital community. Now clinicians can get this information for proper required treatment. Patients, physicians and medical staff are connected to the cloud to access information and resources with proper privileges.

(e) Other applications and projects:

Major applications under the umbrella of WBAN are [15]:- Treatment of cardiovascular abnormalities, cancer detection, asthma monitoring, developing telemedicine systems, artificial retina, fitness monitoring in sports and battle field etc..

As per the survey done on healthcare some applications/projects using WBANs are listed as[4],[12],[13]:

(i) CodeBlue: ZIGBEE enabled radio transactions are used to connect sensing devices within WBAN to communicate with access points (AP). Its architecture is Ad-Hoc based and the structure is self-organizing.

(ii) AID –N: group casualty happenings are targeted in this application. It is similar to CodeBlue but here wireless repeaters are used along with APs and a GPS module is also attached for localization.

(iii) CareNet: In this project remote health monitoring and controlling is executed by using web-enabled methodologies. It has a 2-tier architecture which makes it scalable, reliable and secure.

(iv) Alarm Net: This project has a combination of WBAN and environmental sensor network. Its architecture is 3-tier based. 1st tier has WBAN devices, 2nd tier has environmental sensors and 3rd tier has Alarm-Gate which is a network based on Internet Protocol (IP). So its goal is patient health monitoring in home environment.

(v) UbiMon: It consists of ad-hoc network of wearable and implantable sensors to create a WBAN. Goal of project is to capture physiological status regularly and detect any life-threatening symptom present in patient.

(vi) Others: many other application based projects are as: Mobicare, MediSN, STAIRE, Vital-Jacket, Bike-Net, eWatch [14].

Hence there are various applications and projects developed to enrich the pervasiveness of WBAN in healthcare.

4. REQUIREMENTS OF SECURITY AND PRIVACY ASPECTS IN WBAN

In case of money it is well known that earning and collection of money is important but more important is to keep it safe and secure, so that nobody could ever steal it and a lot of hard work could go in vain. Similar case is applied to information or physiological data collected by various sensors within WBAN about health status of a human user.

Three main points in which security must be applied within WBAN are-

1. On sensors attached in, on or around user's body.
2. On personal servers (where aggregated information is kept and to be sent out side for further processing).
3. On Communication channels & various entry/exit points or gateways.
4. On Internet (to connect medical community outside the WBAN).
5. On Devices used by Clinicians or medical helpers.

There are few stringent reasons for the requirement of security; some of them are as follows:

I. Elderly and non-tech-savvy user's lives could be endangered if any attacker obtains and misuses their current health information.

II. Pregnant woman want to hide her current status but somebody hacks it & makes it public so it may harm social status of pregnant lady and even life of mother and would be child may be under threat.

III. Some Insurance persons can modify (to reduce benefits) their policy for user by getting private current status of patient.

IV. Wrong information could be intentionally entered thru (insecure) channel trespassing. On the basis of this modified information inappropriate medical treatment could be provided. So life of patient as well as reputation and goodwill of hospital and doctor could be ruined.

V. Project development under WBAN will be negatively influenced and it would be defamed among target customers/users. Fallen Trust on technology could de-motivate and prevent researchers for further progress.

So, accurate, reliable, secure and trustworthy remote healthcare observant systems are greatly required to be developed using WBANs.

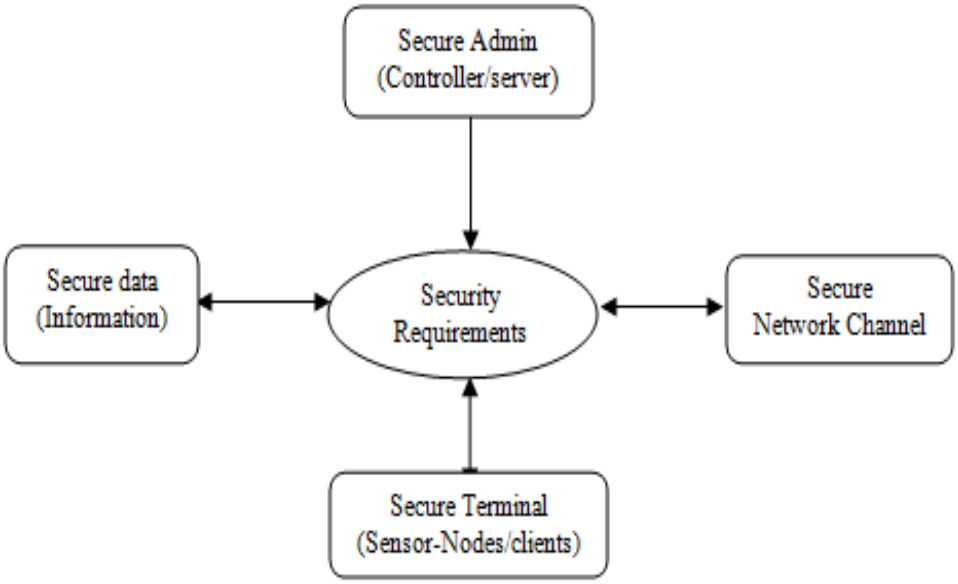

Fig.2 Areas where need and urgency of security exists within WBAN

So, accurate, reliable, secure and trustworthy remote healthcare observant systems are greatly required to be developed using WBANs.

5. 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:

1. WBAN is directly related to human beings so hit and trial or any hypothesis is useless.
2. Hostile environmental conditions.
3. 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-

(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.

Thus, confidentiality, authenticity and integrity are conserved here and a new area of future research has also been initiated. But this framework is not putting sufficient focus to protect against physical tampering and jamming of sensing devices.

One more research paper by Han, In & Jo [10] has presented a better scheme for data confidentiality in cloud-based WBANs. In this paper authors have proposed a multi-valued and ambiguous scheme to confine data confidentiality. Data communication between cloud and WBANs is attempted to be secured efficiently. It is based on the association of complexity theory to cryptography. Authors have compared their results with standard AES, DES encryption techniques and shown their supremacy on these contemporary methods.

In another research presented by Muhannad and Yaser [16] efficient information collection in WBANs is implemented by introducing cloudlet concept. Reliability and trust worthiness is maintained here up to some limit. Hence, integrity of large data collected by different machines attached to patients and users is also aimed to be kept.

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 concepts- DNA 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.

6. CONCLUSION

This paper provides an assessment of current state-of-art methods to design a completely new dimension of efficient and secure remote e-healthcare monitoring systems using WBANs. Nowadays technical advancements are equally worried about the health of our ageing society. This review paper is the first step to find and solve existing problems in E-healthcare arrangements. Our future research must be in the direction of multidisciplinary attachments to obtain better, promising and unexplored area of WBAN based e-healthcare arrangements. As IOT (Interenet Of Things) has become recent area of development for efficient service providing. But a lot of research work is required to enhance security and privacy within applications based on IOT. So the future scope of this review paper is pervasive development of security enabled system along with sufficiently high availability of resources. In future, developers must raise trust of technology among society. Security and privacy are the only two basic

requirements to win this trust. The research and development in data security and privacy within WBANs is still in its primary stage. Thus, further research and methodical designing is required in this area so that various new applications could serve the humanity.

7. ACKNOWLEDGMENTS

We sincerely acknowledge all the cited scholars who have contributed towards development of the review paper by providing strong ideas in this field. We would like to thank Prof. A.K. Pandey for his valuable suggestions to inspire our research in this area.

8. REFERENCES

[1] Ramesh Kumar, R. Mukesh, State Of The Art : Security In Wireless Body Area Networks (IJCSET) International journal of Computer Science & Technology,Vol.4 No. 05 May 2013

[2] K. S. Kwak, S. Ullah, N. Ullah, An Overview of IEEE 802.15.6 standard, Invited paper for presentation in ISABEL 2010

[3] 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

[5] 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

[6] 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 Journal-2014-2-1,1-5

[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, A cloud based healthcare framework for security and patients' data privacy using wireless body area networks, Elsevier, Procedia Computer Science vol.34 (2014)pp.511-517, Nov 2014

[10] N.D.Han, L. Han, D.M.Tuan, H.O. In, M. Jo, A Scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks, Elsevier, Journal of Information Science 284 (2014) pp.157-166, April 2014

[11] Hutchinson, C., Ward, J. < Castilon, K. Navigating the next-generation application architecture. IT Professional, 1(2), pp. 18-22, 2009

[12] Bruno, Rodrigues, Diez, Lopez-Coronado, Mobile-Healt: A review of current state in 2015, Elsevier, Journal of Biomedical Informatics vol.56 (2015) pp.265-272, Jun 2015

[13] M. Chen, J. Wan, X. Liao, V.C.M. Leung, A Survey of Recent Developments in Home M2M Networks, IEEE Communications survey and tutorials, Vol. 16, No. 1, First Quarter 2014

[14] N. Fatema, R.Brad, Security Requirements, Counterattacks and Projects in Healthcare Applications Using WSNs- A Review, International Journal of Computer Networking and Communication (IJCNAC) Vol. 2, No. 2 (May 2014)

[15] Ullah, Higgins, Braem, Latre, Blondia, Moerman, Saleem, Rahman, Kwak, A Comprehensive Survey of Wireless Body Area Networks, DOI 10.1007/s10916-010-9571-3, Springer 2010

[16] S.S. Javadi and M.A. Razzaque, Security and Privacy In Wireless Body Area Networks for Healthcare Applications, DOI 10.1007/978-3-642-36169-2_6, Springer-Verilag Berlin Heidelberg 2013

[17] Lu, Lin, Shen, SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency, IEEE Transactions On Parallel and Distributed Systems Vol. 24 No.3 Year 2013

[18] M.Toorani, Cryptanalysis of Two PAKE Protocols for Body Area networks and Smart Environments, International Journal of Network Security, Vol. 17, No.5, pp. 629-636, Sept. 2015

[19] H. Rathore, V. Badarla, S.Jha, A. Gupta, Novel Approach for Security in Wireless Sensor Network using Bio-Inspirations, IEEE (2014)978-1-4799-3635-9/14

[20] O. Salem, Y. Liu, A. Mehaoua, R. Boutaba, Online Anamoly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring, IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 5, September 2014

[21] D.He, C. Chen, S. Chan, J. Bu, P Zhang, Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks, selected paper for IEEE journal 2011.

[22] A. F. Marhoon, A. H. Hamad, Chaos Theory and DNA Computation Based Data Encryption System for E-Healthcare Monitoring System, Vol. 5 No. 5 Journal of Information Engineering and Applications, 2015.