ISSN (ONLINE):2456-5717
International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.4, Issue.5, May 2018

Integrated Wireless Sensor Network for Medical Data Transmission Using GSRM and HEBM

[1] G.Thiviya Bharathy, [2] T.SheikYousuf

[1] II M.E CSE, Mohamed Sathak Engineering College, Kilakarai – 623 806.

[2] Associate Professor, CSE Dept., Mohamed Sathak Engineering College, Kilakarai – 623 806.

Abstract— **Wireless Sensor Networks (WSN) is widely used in medical data transmission which collects the real time medical data information from the patients by using wireless sensor. In hospitals, medical sensor monitors the large volume of real time data from the patients. The transmission of this medical data through wireless network is the biggest problem because the medical information of the patients is highly sensitive. To provide private and secured medical data transmission, we propose the wireless sensing healthcare system in this paper. In our health care system, the medical data are collected from Wireless Body Area Network (WBAN) and that is transmitted through Wireless Sensor Infrastructure Network, finally the data are scattered in Wireless Personal Area Network (WPAN).**

Keywords: **Medical Data Transmission, WPAN, WBAN**

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensor to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to other locations. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

Sensor to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to other locations. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The sensor networks for medical applications can be of several types: implanted, wearable, and environment-embedded. The implantable medical devices are those that are inserted inside human body. Wearable devices are used on the body surface of a human or just at close proximity of the user. Environment-embedded systems employ sensors contained in the environment. Possible applications include body position measurement, location of persons, overall monitoring of ill patients in hospitals and at homes. Devices embedded in the environment track the physical state of a person for continuous health diagnosis, using as input the data from a network of depth cameras, a sensing floor or other similar devices. Body-area networks can collect information about an individual's health, fitness, and energy expenditure. In health care applications the privacy and authenticity of user data has prime importance. Especially due to the integration of sensor networks, with IoT, the authentication of user become more challenging; however, a solution is presented in recent work.

Body sensor network systems can help people by providing healthcare services such as medical monitoring, memory enhancement, medical data access, and communication with the healthcare provider in emergency situations through the SMS or GPRS. Continuous health monitoring with wearable or clothing-embedded transducers and implantable body sensor networks will increase detection of emergency conditions in at risk patients. Not only the patient, but also their families will benefit from these. Also, these systems provide useful methods to remotely acquire and monitor the physiological signals without the need of interruption of the patient’s normal life, thus improving life quality.

Many hospitals rely on wireless communication to monitor patients and alert doctors about their status. As hospitals grow in size and become more densely populated, the density of data transmitted through the hospital’s wireless network grows proportionally. Furthermore, different types of data originating from patients with different medical conditions present a range

of criticality, and also permit a range of acceptable latency for medical attention. Consequently, scheduling data transmission throughout the hospital network becomes a problem of great importance.

Hospitals increasingly rely on body area networks (BANs) of wireless sensors to monitor the status of patients. These cyber-physical sensor networks must schedule the transmission of sensory data to a BAN controller node that aggregates and makes sense of the data gathered by the sensors. The BAN controller can then detect whether a significant event, like a heart attack or stroke, has occurred in the patient. Once an event has been detected, the hospital relies on a second layer of networking that allows the BAN controllers to alert a headquarters about the potentially life-threatening status of the patient. In this paper, we focus on this problem and provide a prioritized queue management and greedy scheduling scheme based on the criticality and deadline of patients' sensory data.

Driven by technology advances in low-power networked systems and medical sensors, we have witnessed in recent years the emergence of wireless sensor networks (WSNs) in healthcare. These WSNs carry the promise of drastically improving and expanding the quality of care across a wide variety of settings and for different segments of the population. For example, early system prototypes have demonstrated the potential of WSNs to enable early detection of clinical deterioration through real-time patient monitoring in hospital, enhance first responders' capability to provide emergency care in large disasters through automatic electronic triage improve the life quality of the elderly through smart environments, and enable large-scale field studies of human behavior and chronic diseases. At the same time, meeting the potential of WSNs in healthcare requires addressing a multitude of technical challenges. These challenges reach above and beyond the resource limitations that all WSNs face in terms of limited network capacity, processing and memory constraints, as well as scarce energy reserves. Specifically, unlike applications in other domains, healthcare applications impose stringent requirements on system reliability, quality of service, and particularly privacy and security.

There is a long history of using sensors in medicine and public health. Embedded in a variety of medical instruments for use at hospitals, clinics, and homes, sensors provide patients and their healthcare providers' insight into physiological and physical health states that are critical to the detection, diagnosis, treatment, and management of ailments. Much of modern medicine would simply not be possible nor be cost effective without sensors such as

thermometers, blood pressure monitors, glucose monitors, electrocardiography (EKG), photoplethysmogram (PPG), electroencephalography (EEG), and various forms of imaging sensors.

The ability to measure physiological state is also essential for interventional devices such as pacemakers and insulin pumps. Medical sensors combine transducers for detecting electrical, thermal, optical, chemical, genetic, and other signals with physiological origin with signal processing algorithms to estimate features indicative of a person's health status. Sensors beyond those that directly measure health state have also found use in the practice of medicine. For example, location and proximity sensing technologies are being used for improving the delivery of patient care and workflow efficiency in hospitals, tracking the spread of diseases by public health agencies, and monitoring people's health related behaviors (e.g., activity levels) and exposure to negative environmental factors, such as pollution.

Goal:

The goal of our project is,

- To provide efficient medical data delivery without attacks
- To ensure the privacy of the healthcare system

Existing System:

In existing system, the author designed the system which provides close relationship between patient's medical records and a sequence attribute such as existing symptoms and undergoing treatments. These attributes were preserved in decentralized health care system that authenticates the information for security concern. Due to the decentralized manner of health care system, the network connectivity between the wireless body area network and wireless personal area network is very poor. Authentication process performed by Homomorphic encryption which ensures the privacy by transforms the plaintext into ciphertext to resist cipher text attack but it took more time for encrypt the information.

Issues:

- Higher time consumption
- Poor network connectivity

Problem Statement:

One of the developing networks is that Wireless Sensor Network which is promising technology due to their wide range of application in health care system. However the healthcare system still faces many challenges like poor network connectivity due to the decentralized manner of healthcare system. The healthcare system also suffered by the privacy breach violation of sensitive medical information due to poor encryption process.

Need for System:

To solve this problem, a new solution is prepared by combining Wireless Body Area Network, Wireless Sensor Infrastructure network and Wireless Personal Area Network, which provides efficient and secured medical data transmission with better network connectivity.

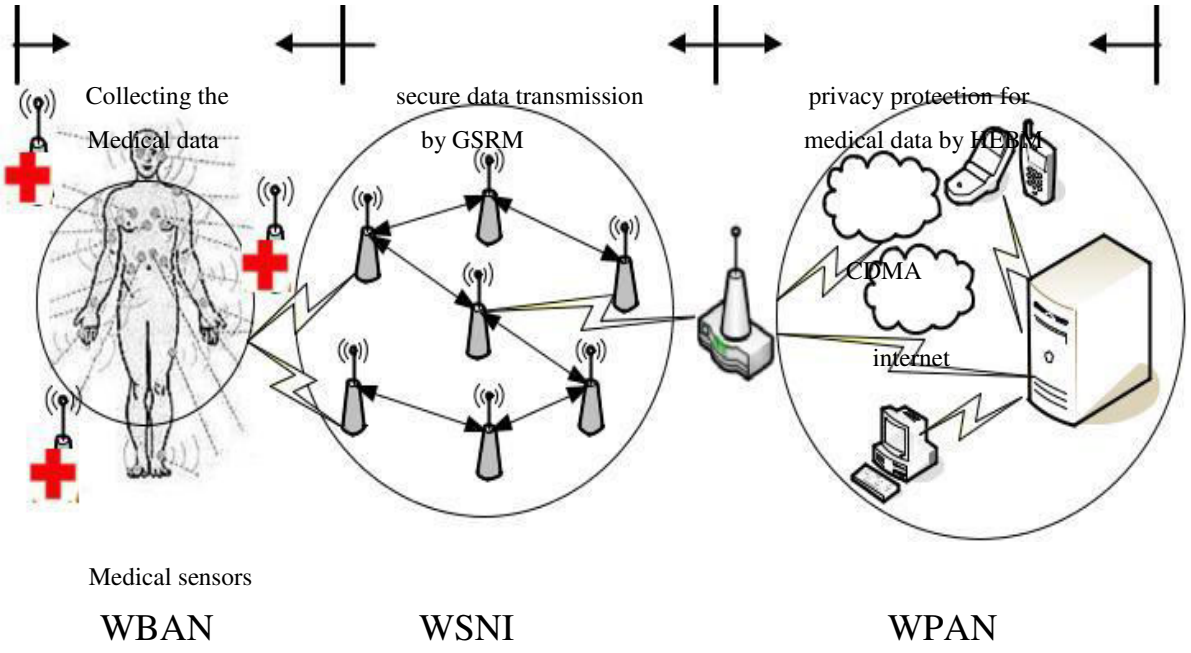
Proposed System:

The healthcare system which provides secured and private medical data transmission. The Wireless Body Area Network (WBAN) collects the medical information by using medical sensors. The medical data transmitted through the Groups of Send Receive Model (GSRM) and the medical data are published in Wireless Personal Area Network (WPAN) which is handled by authorized family of patient.GSRM provides key distribution and secure data transmission using HEBM. Homomorphic Encryption Based on Matrix ensures the privacy of medical data. Key distribution minimizes the resource consumption of memory, computation and communication of sensor to improve the efficiency.

Advantages of Proposed System:

- Improves the network connectivity
- Minimize the delay

II. System Architecture and Result Analysis



The rapid technological convergence between Internet of Things (IoT), Wireless Body Area Networks (WBANs) and cloud computing has made e-healthcare emerge as a promising application domain, which has significant potential to improve the quality of medical care. In particular, patient-centric health monitoring plays a vital role in e-healthcare service, involving a set of important operations ranging from medical data collection and aggregation, data transmission and segregation, to data analytics. This survey paper firstly presents an architectural framework to describe the entire monitoring life cycle and highlight the essential service components. More detailed discussions are then devoted to {\em data collection} at patient side, which we argue that it serves as fundamental basis in achieving robust, efficient, and secure health monitoring. Subsequently, a profound discussion of the security threats targeting eHealth monitoring systems is presented, and the major limitations of the existing solutions are analyzed and extensively discussed.

Our proposed healthcare system involves the Group of Send Receive Model scheme to provide key distribution and secure data transmission. To ensure the security of transmitted medical data, we introduce the key distribution scheme. The key distmproves the efficiency of the healthcare system by decreasing the resource consumption of memory, computation and communication of sensor. In nodes are acts as sender nodes and other group nodes are acts as

receiver nodes. If a node is acts as middle node of two adjacent groups, it can send (receive) the message from one group to other group

Wireless Body Area Network (WBAN):

The technical convergence of Internet of Things (IoT), Wireless Body Area Network (WBAN) and cloud computing provides promising information intensive model which significantly improves the quality of medical care. In our proposed healthcare system, Wireless Body Area Network (WBAN) collects the medical information from patients by using medical sensor. The medical sensing data from a wireless body-area network relayed via extended wireless sensor network infrastructure and then published in wireless personal area network. Due to energy exhaustion or node breakdown, some nodes will be dead after a period of running of WSNs. If the dead node is not a leader, the leader will mark this node a "virtual node" and no keys in the group will be changed. However, other nodes in the group no longer send messages to the dead node. If the dead node is a leader, the election algorithm (Algorithm 1) in the group will be conducted and the new leader will mark the dead leader a "virtual node". If the number of virtual nodes exceeds one-half of the total members in the group, the leader node will delete them and re-distribute the keys in the group. However, if the alive nodes are too few (below a certain threshold) to maintain communications in the group, the group will be destroyed and all alive nodes will rejoin the network by seeking other groups. Specifically, if the dead node is a GSRM-Middle node, the node nearest to it within the communication range of the group will be searched and will replace it; otherwise, if an appropriate neighbor node cannot be found, the group will be destroyed and all living nodes will rejoin the network. If one node leaves the network unconventionally (for example, a capture attack occurs), the leader launches the key updating, generates a random number *rd*, then sends it confidentially to all other nodes.

Group construction and key distribution:

In wireless sensor network infrastructure, the medical data are transmitted to wireless personal area network by relay sensors. Groups of Send Receive Model provide key distribution scheme encryption scheme to improve the security of the medical data from the wireless body area network.

The key distribution scheme improves the efficiency of the system by reducing the resource consumption of sensors. Homomorphic Encryption Based on Matrix (HEBM) provides data privacy protection by transform the plaintext data to ciphertext data.

Wireless Personal Area Network (WPAN):

In our healthcare system, the secured medical data released via gateway to Wireless Personal Area Network through CDMA. It permits authorized families and guardians to obtain patient's health information anytime and anywhere via mobile handheld devices.

Expert System:

Expert system designed to achieve an automatic analysis of scrambled medical data. The medical data from the WBAN is transmitted through wireless sensor infrastructure network to WPAN. The results are obtained through the expert system in WPAN. It only feeds the results back, based on three cases such as normal, relatively low and high.

Algorithm Description

(i) Group of Send Receive Model (GSRM)

Our proposed healthcare system involves the Group of Send Receive Model scheme to provide key distribution and secure data transmission. To ensure the security of transmitted medical data, we introduce the key distribution scheme. The key distribution scheme improves the efficiency of the healthcare system by decreasing the resource consumption of memory, computation and communication of sensor. In GSRM all sensor nodes are included within a circle with radius R. The count of the nodes in a group should be even number. One half of the group nodes are acts as sender nodes and other group nodes are acts as receiver nodes. If a node is acts as middle node of two adjacent groups, it can send (receive) the message from one group to other group. In GSRM, a leader node sends sessionkeys for each member node in the group. When a node acquires its session key between itself and another node in the same group, it is allowed to send the message using the key.

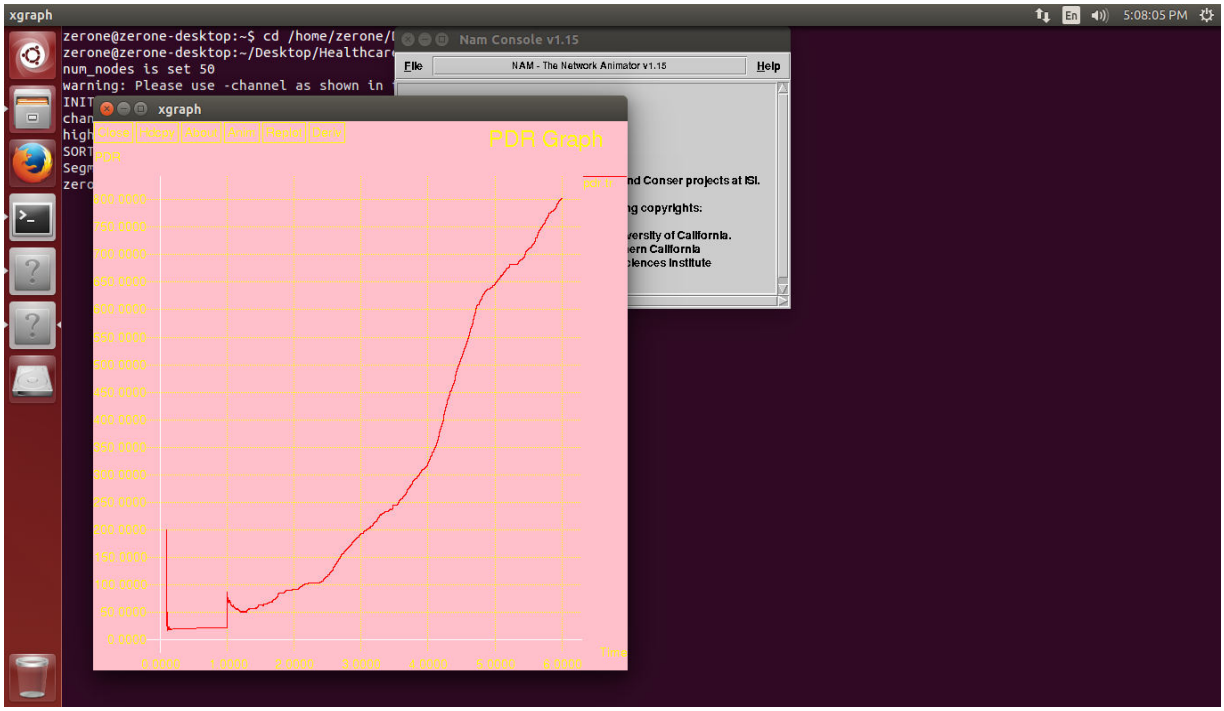
(ii) Homomorphic Encryption Based on Matrix

To provide better privacy preserving characteristics, we proposed Homomorphic Encryption Based on Matrix in our healthcare system. Users of HES submit 'n' number of

medical data from WBAN via Wireless Sensor Infrastructure Network to WPAN represented as min and max.

To verify preliminarily the reliability and feasibility of the expert system, we tested 78 patients using HES (only body temperature, heart rate and blood oxygen) for a duration of one week. Note that one important feature of HES is that it is available for the families and guardians to access health status information of these 78 patients via their mobile phones' whicalso caters to the scenario of remote healthcare for old people. The analysis of questionnaires of their . Three situations are possible: satisfied with the results provided by the expert system, unsatisfied and no response. We see a relatively high approval of results provided by the expert system.Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems. For resource-efficient data acquisition, one major trend today is to utilize compressive sensing, for it unifies traditional data sampling and compression. Despite the increasing popularity, how to effectively process the ever-growing healthcare data and simultaneously protect data privacy, while maintaining low overhead at sensors, remains challenging. To address the problem, we propose a privacy-aware cloud-assisted healthcare monitoring system via compressive sensing, which integrates different domain techniques with following benefits. By design, acquired sensitive data samples never leave sensors in unprotected form. Protected samples are later sent to cloud, for storage, processing, and disseminating reconstructed data to receivers. The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise. Theoretical and empirical evaluations demonstrate the system achieves privacy-assurance, efficiency, effectiveness, and resource-savings simultaneously

Result Analysis:



After completion of expert system it is allowed to the graph generation process. Since graph generation is the final module of our proposed system. During a graph generation process shows an automatic analysis of medical data with our proposed system. It also measures how well our proposed system is better when compared to an existing system. Finally we generate a graph for the PDR vs simulation time we chosen for our concept.

This proposal fulfills the simulation time then the key distribution is performed by Groups of Send Receive Model (GSRM) and the privacy protection is provides by Homomorphic Encryption Based on Matrix. Finally the users obtained the secure information via gateway in wireless personal area network.

REFERENCES

[1] A.Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System, " China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.

[2] M.S.Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.

[3] C.Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.

[4] M.Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area

[5] Networks," in Proc. of 35th IEEE Symp.on Security and Privacy, 2014, pp. 524-539.

[6] C.Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[7] P.T.Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.

AUTHOR(S) BIOGRAPHY

G.Thiviya Bharathy received the BE degree in Computer Science and Engineering from Anna University Chennai. Now she is studying in II ME CSE in Mohamed Sathak Engineering College at Kilakarai, Ramanathapuram.

T.Sheik Yousuf received the PhD degree in Computer Science and Engineering from Anna University Chennai. He received the ME(CSE) and M.Tech(IT) degree with Distinction from the Anna University Chennai. Now working as an Associate Professor in CSE department at Mohamed Sathak Engineering College, Kilakarai, Ramanathapuram. His current research focuses on frequent pattern mining for data mining with single scanning. He has published 2 technical papers in reputed international journals and 30 papers published in National conferences. He is a lifetime member of ISTE.