IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Private and Secure Healthcare Data Transmission and Analysis for Medical Wireless Sensing System

Buddesab[1*], Thriveni J [2], Venugopal K R [3]

[1,2,3]Department of Computer Science and Engineering, University of Visvesvaraya College of Engineering, Bangalore University, Bangalore-560001 India

[*]*Corresponding Author: tonnur21@gmail.com, Tel.: +919945258825*

DOI: https://doi.org/10.26438/ijcse/v7i2.519527 | Available online at: www.ijcseonline.org

Accepted: 19/Feb/2019, Published: 28/Feb/2019

***Abstract*—** The merging of Internet of Things (IoT), Wireless Body Area Network (WBAN), and Cloud Computing (CC) has greatly influenced the Electronic Medical (E/M) Healthcare system. As the use of E/M healthcare increases, the chances of privacy and security violation increases. To address this, a Healthcare system framework is designed which collects medical data from WBAN, transmits them through Wireless Sensor Network (WSN) and publish them through Wireless Personal Area Network (WPANs). WSN allows more number of nodes to transmit the packets from source to destination. It involves three techniques 1) Packet Scheduler where there can be multiple source and destination which prevents collision. 2) Multiple selection method based upon monitor node which provides multiple routes. The monitor node optimizes the selected node. 3) Node to Node compression and Load Balancing Technique which compress the packets sent from source to destination and to decrease the delay. The data collected from WBAN will be aggregated and stored in a file. The file is uploaded to cloud and is accessed by Hospital authorities whenever required. Simulation results shows that the proposed system perform better than existing system with respect to Packet delivery ratio, Transmission time and Energy consumption.

***Keywords*——** Cloud computing, healthcare system, Internet of thing, WBAN, WSN.

I. INTRODUCTION

The Rapid growth of IoT, Cloud Computing, Wireless Body Area Networks (WBAN) and Wireless Personal Area Network (WPAN) has made tremendous impact on Medical care system. Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Wireless Body Area Network allows checking the real time health updates. The sensor will be embedded in the human body which will collect all the physiological changes so that it will be easy to monitor, the health changes irrespective of the places. Applications involve people suffering from diabetic, heart attack, Asthma etc.

Wireless personal area network (WPANs) is a personal short distance wireless area network for interconnecting devices. Bluetooth, Code Division Multiple Access (CDMA) etc are some of the WPANs devices. The existing e/m (electronic/mobile) healthcare system mainly focuses on security and privacy of the system with the help of GSRM (Group Send Receive Model) and HEBM (Homomorphic Encryption Based on Matrix) respectively. In existing system, packets are transmitted from source to destination. During the transmission of packets, sensors will collect the medical data and all the medical data gets aggregated and will be stored in one file. That file will be uploaded to cloud for processing the data. Later the Hospital staffs searches the status of the sensor node information and its collected medical data.

A. Motivation

In this paper we have proposed a privacy and security for healthcare system by Implementing Enhanced Homomorphic Encryption Based on Matrix in WSN and with more number of nodes to transmit the packets from source to destination, which includes packet scheduler with multi-path selection based upon monitor node with node to node compression and provide authentication (user authentication process) to improve the security performance.

B. Research Contribution

The important contribution of this paper is

1. Proposed Healthcare System with more number of nodes to transmit the packets from source to destination with multipath selection with node to node compression.
2. Authentication is provided to increase the performance of security so that intruder cannot enter into the system.

3. If there are multiple source and destination in HEBM, it leads to the collision. In EHEBM, we use packet scheduler where there can be multiple source and destination.
4. In HEBM, packets are delivered from source to destination through neighboring nodes. In EHEBM, multipath selection method, provides multiple routes. The monitor node optimizes the selected route.
5. If large amount of packets are to be transmitted in HEBM, then there will be delay whereas in EHEBM, node to node compression technique compress the packets and there by decreases the delay.

C. Problem Definition

In the existing system, privacy of individual information has been violated where the hackers can enter into the network easily without any authentication. To overcome this, the Healthcare system framework is designed which collects the medical data from WBAN, transmits through WSN which includes packet scheduling and Load Balancing to decrease the delay time and authentication has been included to enhance the security where it becomes difficult for the hackers to enter the network easily.

D. Organization of this paper

The organization of the paper is as follows. Section II provides information about the related work. Section III and Section IV describes the System Model and algorithm. Performance Evaluation is done in Section V and finally the conclusion is summarized in Section VI.

II. RELATED WORK

Sawand *et al*., [1] have proposed the technology of wireless body area networks (WBANs) that has been growing tremendously in health and real time body monitoring system. Wang *et al*., [2] have planned a privacy-aware cloud-assisted healthcare observation system via compressive detecting for resource-efficient data acquisition and to collect medical information. Amirbekyan *et al.,* [3] have projected the efficiency of secure scalar products, is very important as a result of they will cause overhead in communication value, but real operations additionally function one among the fundamental various secure protocols, but the security is semi honest and data are often leaked.

Reid *et al*., [4] have discussed the Role Based Access Control (RBAC), as a hopeful access control system. for effectiveness and unambiguousness, get to strategies that allow access to an expansive scope of substances while explicitly denying it to subgroups from securing those elements should be upheld in health info networks. The System exhibits an adjustment of RBAC that supports general consent with specific denial. In Attribute Based Encryption, framework gives a proof-of-idea mobile application that enables patients to get to the encrypted records on their iPhone disconnected and safely send out those records to other cloud-based EMR Suppliers [5].

Shin *et al*., [6] have proposed the Extended RBAC security that model observe security necessities associated with privacy protection in u-HealthCare Service Integration Platform (u-HCSIP). The framework is a protected solution for mobile access to Electronic Health Record (EHR) system. The HER system resolution allows secure authentication and communication between a mobile device and a healthcare service supplier through usage of a two-factor authentication technique on a cell phone [7].

Guo *et al*., [8] have proposed the Electronic social insurance (eHealth) frameworks which supplanted the paper-based medicinal frameworks because of the attractive highlights features such as universal accessibility, high accuracy, and low cost. As a important component of eHealth frameworks, mobile healthcare (mHealth) applies mobile devices, for example, smart phone and tablets. Financial and regulatory related has provided strong incentives to institute better disease prevention, enhanced patient checking, and push U.S. medicinal services into the advanced period. This progress necessitates that information protection is guaranteed for computerized digital data in three individual stages: I. procurement, II. Capacity and III. Calculation [9].

Cherkaoui *et al*., [10] have proposed the framework to enhance the Quality of Service (QoS) of e-health applications to guarantee well-organized and constant remote observing of patients and elderly. Optimizing Homomorphic Encryption for streaming Algorithm which presents a technique that expands effectiveness and parallelism for specific calculations under Fully Homomorphic Encryption (FHE) yet some genuine security issues remain [11].

Marwan *et al*., [12] have provided an approach based on Secure Multi-Party Computation (SMC) protocols to ensure privacy-preserving in the collaborative systems. This technique adopts the collaborative method to improve medical quality. Suitable cryptographic tools are presented for permitting fractional visibility and valid protection on approved parts for various levelled security insurance of eHealth information [13]. M-Health can be characterized as mobile computing, medical sensor and communication technology for healthcare. The goal is to supply a set of papers that will mirror the spectrum of the ongoing advances in m-Health innovations and the job of the developing mobile and network technology in m-Health frameworks and applications [14].

Simplicio *et al.,* [15] have presented SecourHealth, a lightweight security system concentrated on highly sensitive information gathering applications however the main

drawback is it keeps the outside attack but fails to keep inside attack. A review publication designed at enhancing security and protection in IMDs and health- related BANs provided that clear definitions and an extensive summary of the matter area. They analyse regular topics, arrange applicable outcomes, and distinguish patterns and headings for future research [16].

Chan *et al*., [17] have proposed the system that mechanism on Security homomorphism which permits encrypted information to be worked on two added substances homomorphic schemes, to be Iterated Hill Cipher (IHC) and Modified Rivets Scheme (MRS). The framework gives a structure of Multi-agent design which handles the security and Protection of sensitive medical information. The Remote Patient Monitoring setting engineering will be utilized for approval. The proposed framework utilizes various types of operators to deal with delicate restorative data, for instance, Monitoring Agent, Policy Agent, Data Collector Agent, Access Control Agent, Ontology Store Agent, and Physician Agent [18].

Lin *et al*., [19] have proposed the framework gives vehicle mounted medicinal sensors to social insurance applications. It is a joint power and confirmation control algorithm to plan the clients' transmission of medical information. The target of this algorithm is to limit the number of clients who are disconnecting from the network whereas keeping the EMI on medical sensors at a appropriate level. The system proposed an expense and energy effective three level models for healthcare dependent on WSN to remove restrictions of wired system and to utilize wireless technology efficiently [20].

Pintilie *et al.,* [21] have an efficient storage solution by analyzing and taking into consideration the requirements of e-Health applications (such as computational time, storage, processing time, costs) and important aspects of data replication strategies (such as data priority, price, data size). Hybrid deduplication method is also used in this system.

Guerrero *et al*., [22] have proposed a system which is a flexible, event-driven, user consent-revocation mechanism and includes the dimensioning of the network event-based model. The system aims at explaining in detail the technology drivers behind the IoT and health care with the information on data modelling of medical devices, data validation of critical incident data, data mapping of existing IoT data into different other associated system data [23].

Abinaya *et al.,* [24] have introduced the Information Retrieval R-Tree that Algorithm is used for fetching data with spatial, textual filtering and document ranking from bulky database or network. The system effectively aggregate the data of patients in the various network segments to remove the communication overhead of headers and acknowledgements. The performance of the system is assessed based on aggregation efficiency, total transmission time and end-to-end delay using MATLAB simulations [25].

III. SYSTEM MODEL

A. Proposed Architecture

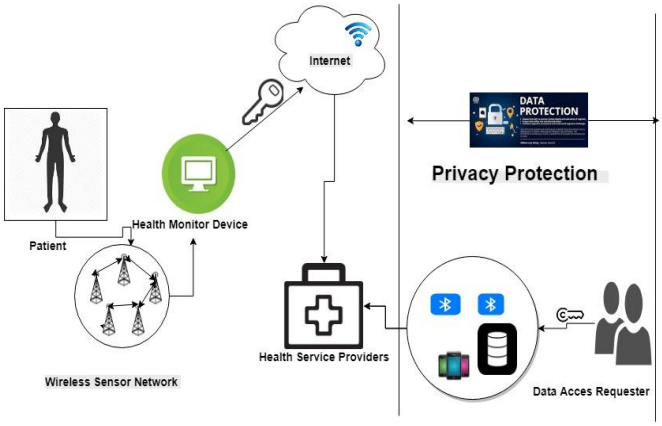

Figure 1. Proposed Architecture

The Figure.1 shows the proposed architecture where the user's biological and physiological information are collected by a healthcare monitor device and through WSN, sensor nodes collect the data and the data is uploaded to the cloud. Later the information has been stored in the database of the health service provider. Data access requestor who needs to access the particular user data can access the details through their smart devices. They collect the information through health service provider.

The proposed system provides the privacy and security for Healthcare system. The existing system provides the security and privacy by using GSRM and HEBM methods respectively. In this system, we have included node to node compression and security authentication for the existing system. In Wireless Sensor Network (WSN), numbers of nodes have been increased to transmit the packets from Source to Destination which includes Packet Scheduler with multipath selection based upon monitor node with node to node compression. Before transmitting the packets, we need to check the quality of the node through Packet Scheduler. Here node encrypts the data and compress the file for security purpose.

Quality means the transmission power, receiving power, ideal power and sensing power and we also check the characteristics of the node. Based on that we assign the packets to the node. Node to Node compression is to compress the packet which is also a data compression which reduces the size of the packets. By applying Packet scheduler and node to node compression technique provides High

Throughput, Avoids Latency, Packet Loss and provides High Accuracy as well as Energy consumption is reduced as compressed data requires less energy for transmission and receiving power when compared to the existing system.

Next we enhance the security system by providing first Level Authentication which means every node has information regarding user id and password. All nodes information will be stored in the database. So, every time Database is verified, if the authentication matches the node will be allowed inside the network.

B. Block Diagram of EHEBM

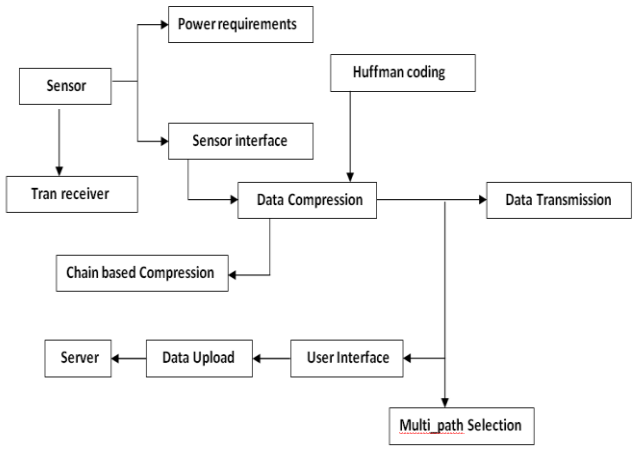

Figure 2.Block Diagram of EHEBM

The Figure 2 shows the Block diagram of EHEBM which includes trans receiver, power requirements , sensors for the transmission of the data , before transmission of data , the data is compressed using Chain based compression method and Huffman coding Algorithm. A *Huffman code* is a particular type of optimal prefix code which is used for data compression without losing the packets. Data is sent from source to destination based on packet scheduler with multipath selection and node to node compression with is Sensor collects the medical data and all the data will be aggregated till it reaches the destination and compressed data later will be uploaded to the server and later authorized hospital staff searches the status information.

C. Techniques used in the proposed system

Techniques used in this proposed system are

1. Multipath selection based upon monitor node.
2. Node to Node Compression.
3. Packet Scheduler.
4. Load Balancing.

1. Multipath Selection based upon monitor node

This technique helps to optimize the route which helps to transmit the packets from source to destination. The quality of the node is been checked first and later the transmission of the packet to that node takes place. This technique reduces the packet loss.

2. Node to Node Compression .

In our proposed system, we use node to node compression technique where the data packets are compressed first and transmitted from source to destination. This technique reduces the size of the packets to half of its original size which increases the storage capacity and reduces the Energy Consumption.

3. Packet Scheduler

It is a queuing discipline which manages the sequence of the network packets transmission in the network interface. Since multiple source and destinations, packet scheduler helps to transmit the packets in a sequence order. As the packets are transmitted in sequence order reordering of the packets in later stage is avoided thus reducing the consumed time. High Packet Delivery Ratio has been achieved using this technique.

4. Load Balancing

Load Balancing is used to check the quality of the node before transmitting the packets. It helps to avoid the packet loss, latency and increases the throughput. The lifetime of the network does not depend only on the lifetime of weak node but depends on the life all nodes in the network which helps to extend the lifetime of the network.

IV. ALGORITHM

A. Algorithm for EHEBM

Step 1: Each node sends a broadcast message to nearb Nodes.
Step 2: Node status defines whether the node is in active Mode or wake up Mode (nid).
nid->neighbour_id.
Step 3: After checking bandwidth and frequency the Nearest node send the ACK message.
Step 4: Admin node authenticates the member node by getting the user id and password.
A-node->uid, pwd
Step 5: After getting the user id and password, node cheeks the database entry from the user credentials.
A-node ->uid_table
A-node->info_status
Step 6: Multiple paths should be selected based upon the source and destination
nb->link_routes
Step 7: Then it optimize the path based upon the packet Scheduling technique.
Step 8: Chain based Compression takes place while the Message is in transit.

Step 9: Node encrypts the data and compress the file
Msg_i=ci(msg1)+ci(msg2)+……ci(msgn)
Step 10: Receiver node only compresses the data by using the key.

In the given algorithm EHEBM, node sends broadcasting message to all nearby nodes and checks the node status whether it is in active mode or not. The nearest node sends the acknowledgement message checking the bandwidth and frequency and the admin node authenticates the member node by getting its user id and password. Admin node checks the user id and password in the database, if the credentials are present the member is acknowledged as authenticated member node and is allowed inside the network for packet transmission. If the credentials are not valid, the steps are repeated to find the node with valid or authenticated user id and password. Later with multipath selection, packet scheduler and node to node compression, the packets are transmitted. Chain based transmission method is used when the message is transmitted, then the node encrypt the data and compress the file. Here to compress the data Huffman Coding technique is used to avoid packet loss. Later the data is uploaded to the virtual cloud and Hospital staff can search the status information. The table shows the example of status information.

Table 1. Status Information Table

ID no	Min_Th	Max_Th	Value	Level
1	21	25	23	Medium
2	21	25	18	Lower
3	21	25	26	Higher
4	21	25	7	Lower
4	21	25	7	Lower
5	21	25	30	Higher
6	21	25	20	Lower
7	21	25	22	Medium
8	21	25	35	Higher

The Table 1 shows the status information table where in practical the min and max threshold will be the range of sugar, BP, asthma etc and the value will be patient's value and accordingly treatment can be done. Here the Id number is considered ID of the person and all the details of them have been stored in the database. Minimum and Maximum Threshold values have been given. In this case it is 21 and 25 respectively and the person value is collected and if the value is within the min and max threshold it is medium or said to be normal. If the value is below the min threshold value then it said to be lower and if the value is above the max threshold value then it is said to be higher.

Homomorphic Encryption Based Matrix (HEBM) is used for privacy purpose. It provides user id and password based upon matrix calculation which provides privacy to the network.

V. PERFORMANCE EVALUTION

A. QoS parameters used to evaluate HEBM and EHEBM algorithms are

1.Packet Delivery Ratio
2.Energy Consumption
3.Transmission Time
4.Network Lifetime
5.Average Storage Capacity
6.Routing Load
7.Packet Loss
8.Throughput

B. Simulation Setup

Simulation in Conducted using NS2 to evaluate the performance of EHEBM. The sensors are setup where the environmental condition needs to be matched. The user can store the data in the cloud over the internet. The hard disk is 40GB and RAM is 3GB. The operating system is ubuntu and coding language is C++, Java/J2EE. The IDE is Net beans 6.9.1 with MYSQL database. The visual interface is set to command line prompt

C. Performance Analysis

1. Packet Delivery Ratio

Packet Delivery Ratio is the number of packets which has been transmitted from source to destination excluding the packets which has been lost or not transmitted to the destination. A Packet Delivery Ratio can be defined as the number of packets received by number of packets sent.

$$\text{Packet Delivery Ratio} = \frac{Received\ Packets}{Sent\ Packets} \text{ X } 100$$

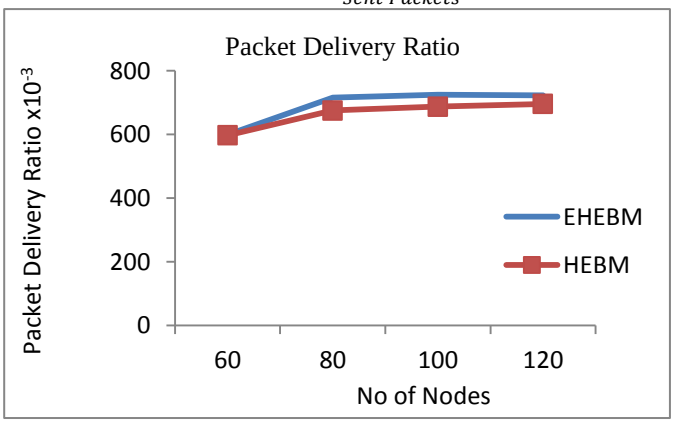

Figure.3 Comparison of Packet Delivery Ratio between HEBM and EHEBM

Figure 3 shows Packet Delivery Ratio of HEBM and EHEBM. Since there is less packet loss and more number of packets have been transmitted from source to destination in EHEBM. The quality of the node has been checked by load balancing technique and then the packet are transmitted which avoids packet loss. So, Packet Delivery Ratio of EHEBM is higher as compared to HEBM.

2. Energy Consumption

Energy consumption is defined as the amount of energy consumed in the network.

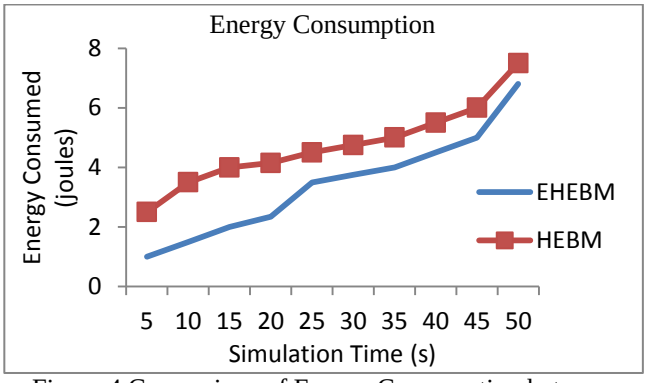

Figure.4 Comparison of Energy Consumption between HEBM and EHEBM

Figure 4 shows the comparison of Energy consumption between HEBM and EHEBM. Energy consumed in EHEBM is less than HEBM because of packet scheduling multi path selection which helps to optimize the route by checking the quality of the node and node to node compression. Since the data is compressed, energy consumed will be less in EHEBM.

3. Transmission Time

Transmission Time is the overall consumption of time in the network. If there are n nodes and there is a n to n delay, the time transmitted for that delay will be calculated. If the delay is high, transmission time will be more and vice versa.

Transmission Time = n_to_n_delay * 1000 ms

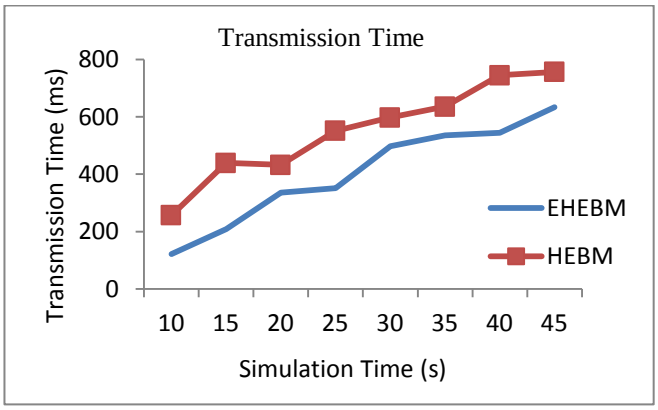

Figure 5. Comparison of transmission time between HEBM and EHEBM

Figure 5 shows the comparison of transmission time between HEBM and EHEBM where the time consumption of EHEBM is less than HEBM because there is no waiting time and delay is less when compared to HEBM. The routing time is less as we are using multipath selection in EHEBM.

4. Network Lifetime

Network Lifetime checks how long the network can have the connectivity. It depends network connectivity is network reliability and time taken to transmit the packets from source to destination and the energy consumed.

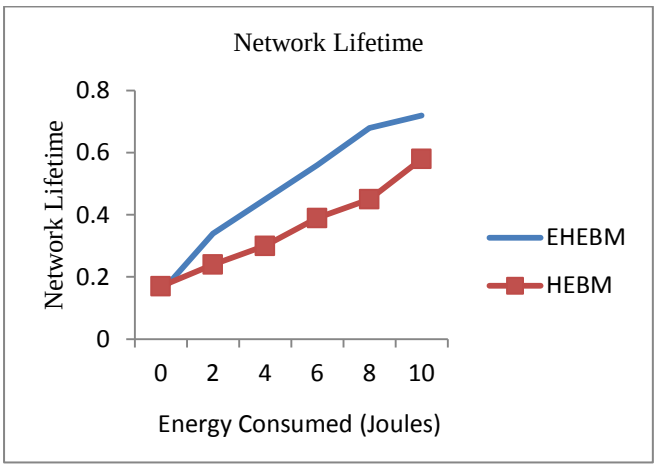

Figure.6 Comparison of Network Lifetime between HEBM and EHEBM

Figure 6 shows the comparison of network lifetime between HEBM and EHEBM where network lifetime of EHEBM is high as compared to HEBM because the packet loss and delay is less and Multipath selection increases the throughput and there is no congestion as compared to HEBM and also the energy consumed is less, there is no depletion in the network. So the network Lifetime is high in EHEBM.

5. Average Storage Capacity

The storage capacity can be defined as the capacity to store the packets in the database.

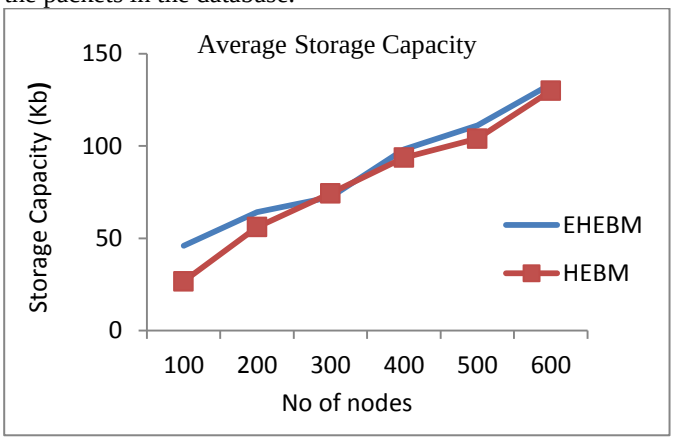

Figure.7 Comparison of Average storage cost between HEBM and EHEBM

Here the average storage capacity is compared between existing system (HEBM) and proposed system (EHEBM). Since the data is compressed, it occupies less space and

capacity to store more number of packets is increased when compared to the existing system. Comparison of average storage capacity between HEBM and EHEBM is as shown in the Figure 7. In HEBM some unwanted or duplicate packets will be stored but in EHEBM data redundancy is achieved and unwanted packets are not stored thus increasing the storage capacity.

6. Routing Load

Routing Load can be defined as the number of packets transmitted across the network from one node to another node.

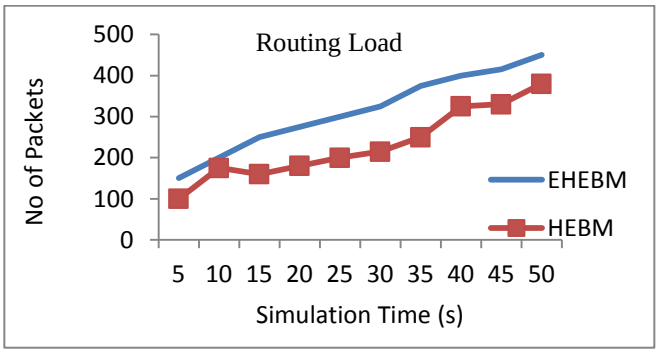

Figure 8. Comparison of Routing Load between HEBM and EHEBM

Figure 8 shows the comparison of the Routing Load between HEBM and EHEBM. Routing load is increased in EHEBM as compared to HEBM because of Packet scheduler and Load Balancing so that there will be no latency, no waiting time, delay will be reduced, also the quality of the node is checked with respect to the power consumption. So, the number of packets transmitted across the network is high in EHEBM than HEBM.

7. Packet Loss

The loss of packets when transmitted from source to destination can be defined as Packet Loss.

Packet Loss = Sent Packets – Received Packets

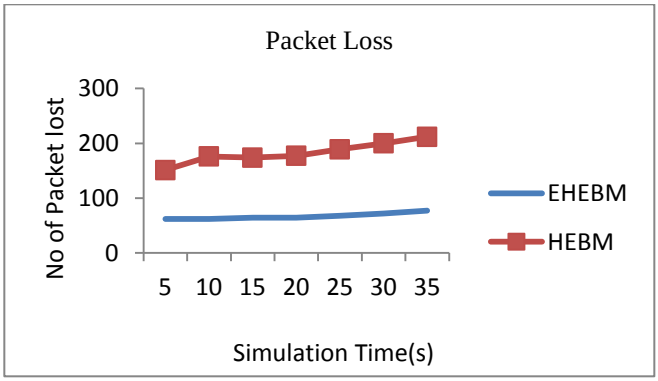

Figure 9. Comparison of Packet Loss between HEBM and EHEBM

Figure 8 shows the comparison of Packet Loss between HEBM and EHEBM where the packet loss in EHEBM is comparatively low as compared to HEBM because of using Load balancing to transmit the packets to the destination

8. Throughput

Throughput is defined as overall packet delivered in a period over the transmission medium.

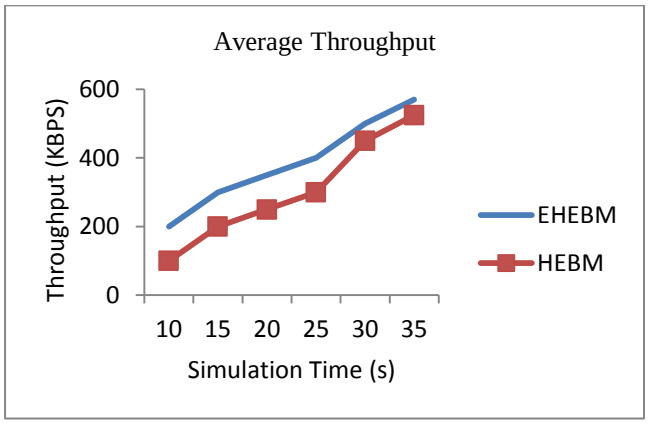

Figure 10. Comparison of Average Throughput between HEBM and EHEBM

Figure 10 shows the Comparison of Average Throughput between HEBM and EHEBM. The information shared in given amount of time is high as the packet loss and delay is decreased in EHEBM also there is no congestion as we are using packet scheduler technique. So, the average Throughput is high in EHEBM as compared with HEBM.

VI. CONCLUSIONS

The proposed system in Wireless Sensor Network (WSN) allows more number of nodes to transmit the packets from source to destination which includes the following techniques 1) packet scheduler with multipath selection based upon monitor node and 2) Node to Node compression which reduces the delay, energy consumption and increases the throughput, storage capacity. 3) Load Balancing method to check the quality of nodes before sending the packets which in turn increases the lifetime of the network.

Security is enhanced by providing First Level Authentication, where the member node needs to produce its user id and password to the Admin node. If the credentials are available in the database server, then the member node is allowed inside the network.

REFERENCES

[1] A. Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System," *China Communications for Journal*, Vol. **12**, No. **1**, pp. **46-65**, Jan. **2015**.

[2] 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 *IEEE INFOCOM Proceedings*, pp. **2130-2138**, **2014**

[3] A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," *in Proceeding of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07*), pp. **209-214**, **2007**.

[4] J. Reid, I. Cheong, M. Henrickson, and J. Smith, "A novel use of RBAC to Protect Privacy in Distributed Health Care Information *Systems*," *in Proceeding of 8th Australasian Conference on Information Security and Privacy*, pp. **403-415**, **2014**.

[5] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing Electronic Medical Records using Attribute-based Encryption on mobile devices," *in Proceeding of 1st ACM Workshop Security Privacy Smart Phones Mobile Devices*, pp. **75-86**, **2011**.

[6] Moon Sun Shin, Heung Seok Jeon, Yong Wan Ju, Bum Ju Lee and Seon-Phil Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," *The Scientific World Journal*, **2015**.

[7] Jelena Mirkovic, Haakon Bryhni, Cornelia M. Ruland, "Secure Solutions for Mobile Access to Patients Health Care Record," *in IEEE International Conference on E-health Networking,Application and Service*s, pp. **296-303**, **2011**.

[8] Linke Guo, Chi Zhang, Jinyuan Sun, Yuguang Fang, "A Privacy Preserving Attribute Based Authentication system for Mobile Health Network", *IEEE Transactions on Mobile Computing*, Vol **13**, No. **9**, pp. **1927--1941** , **2014**.

[9] Ovunc Kocabas, Tolga Soyata, Jean-Philippe Couderc , " Asessement of Cloud Based Health Monitoring using Homomorphic Encryption",*in IEEE 31st International Conference on Computer Design (ICCD),* pp . **443-446**, **2013**.

[10] El Hadi Cherkaoui, Nazim Agoulmine, "Context Aware Mobility Management with Wifi/3G Offloading for Ehealth WBANs" *in IEEE 16th International Conference on e-Health Networking, Applications and Services,* pp **472-476**, **2014**.

[11] Alex Page, Ovunc Kocabas, Scott Ames, Muthuramakrishnan Venkitasubramaniam and Tolga Soyata, "Cloud Based Secure Health Monitoring: Optimizing Fully Homomorphic Encryption for streaming Algorithm", *in IEEE Globecom Workshop-Cloud Computing System*. pp. 48-52, 2014.

[12] Mbarek Marwan, Ali Kartit and Hassan Ouahmane ,"Applying Secure Multi-Party Computation to Improve Collaboration in Health care Cloud ", *IEEE International Conference on Systems of Collaboration (SysCo),* pp**. 1--6**, **2016**.

[13] Alexandru Soceanu, Alexandru Egner and Traian Muntean, "Managing the Privacy and Security of eHealth Data", *20th International Conference on Control Systems and Science*, pp. **439-446**, **2015.**

[14] R. Istepanian, E. Jovanov, and Y. Zhang, "Guest Editorial Introduction to the Special Section on m-Health: Beyond Seamless Mobility and Global Wireless Health-care Connectivity," *in IEEE Transactions on Information Technology in Biomedicine* , Vol. **8**, No. **4**, pp. **405--414**, **2004**.

[15] Marcos A. Simplicio Jr., Leonardo H. Iwaya, Bruno M. Barros, Tereza C. M. B. Carvalho, and Mats Naslund , " Secour Health : A Delay Tolerant Security Framework for Mobile Health Data Collection*", in IEEE Journal of Biomedical and Health Informatics*, Vol. **19**, No. **02**, pp. **761--772**,**2015**.

[16] Michael Rushanan, Aviel D. Rubin, and Denis Foo Kune , " SoK: Security and Privacy in Inplantable Medical Devices and Body Area Networks*", in IEEE Symposium on Security and Privacy (SP),* pp. **524--539**, **2014**.

[17] Aldar C-F. Chan, "Symmetric Key Homomorphic Encryption for Encrypted Data Processing" *IEEE International Conference on Communications ICC'09*, pp. **1--5**, **2009**.

[18] Todor Ivas¸cu, Marc Frıncu and Viorel Negru , " Considerations Towards Security and Privacy in IoT based E-health Applications" *in IEEE 14th International Symposium on Intelligent Systems and Informatics,* pp. **275—280**, **2016**.

[19] Di Lin, Fabrice Labeau, Yuanzhe Yao, Athanasios V. Vasilakos, and Yu Tang, "Admission Control over Internet of Vehicles Attached with Medical Sensors for Ubiquitous Health Care Applications" *in IEEE Journal of Biomedical and Health Informatics*, Vol. **20**, No. **4**, pp **1195-1204**, July **2015**.

[20] Uttara Gogate and Jagdish W. Bakal ," Smart Health Care Monitoring System Based on Wireless Sensor Network", *International Conference on Computing, Analytics and Security Trends (CAST*), pp. **594-599 , 2016.**

[21] Andreea Pintilie, Elena Apostol and Ciprian Dobre, "Efficient Storage and Replication Solutions for Health Care Applications", *IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*,**2016**.

[22] Rosa Sanchez-Guerrero, Florina Almenarez, Daniel Dıaz-Sanchez, Patricia Arias and Andres Marın, "A Model for Dimensioning a Secure Event Driven Health Care System" *IEEE Transaction*, pp **30-37**, **2012.**

[23] Muthuraman Thangaraj, Pichaiah Punitha Ponmalar and Subramanian Anuradha, "Internet of Things (IOT) Enabled Smart Autonomous Hospital Management System – A Real World Health Care Use Case with the Technology Drivers" *IEEE International Conference on Computational Intelligence and Computing Research*,**2015**.

[24] Abinaya.M and Ganesan. R, "Effective Search Mechanism for Finding Nearest Healthcare Facilities", *Proceedings Global Conference on Communication Technologies (GCCT 2015)* , pp **534-538**,**2015**.

[25] Roopali and Raj Kumari, "An Efficient Data Offloading to Cloud Mechanism for Smart Healthcare Sensors",*1st International Conference on Next Generation Computing Technologies (NGCT-2015)* , pp **90-96**,**2015**.

Authors Profile

Mr. Buddesab received the Bachelor of Engineering degree in Information Science and Engineering form The National Institute of Engineering Mysore, in 2009, and the Master of Technology in Computer Science and Engineering from M.S. Ramaiah Institute of Technology Bangalore, in 2013, both Visvesvaraya Technological University, Belgaum, India. He is currently working toward the PhD degree from Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, Bangalore University, India. His research interests include cloud computing, scheduling and resource management, data security and Wireless sensor networks. He is a member of IEEE since 2014. He has published research papers in reputed international journals and conference. He has one years of teaching experience and 4 years of Research Experience.

Dr.Thriveni J has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 23 years of teaching experience. Currently she is Professor in the Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore. She has over 90 research papers to her credit. She has produced four doctorate students and guiding 07 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.

Dr.K. R. Venugopal is currently the Vice Chancellor Bangalore University, Bengaluru. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bengaluru. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Micro-processor Programming, Mastering C?? and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE, ACM and ISTE.

