A Secured Patients Monitoring System Using Sensor Nodes in Health Care Institutions

Pabitra Mohan Khilar[1], Swasti Sadhan Khatua[2], Rakesh Ranjan Swain[3]
Department of Computer Science and Engineering
National Institute of Technology
Rourkela-769008, Odisha, India
Email: [1]pmkhilar@nitrkl.ac.in, [2]sadhanswasti@gmail.com, [3]rakeshswain89@gmail.com

***Abstract*—Telemedicine is one of the hot research topics which provides health-care solutions to remote areas. There are various situations, where telemedicine plays a vital role. Nowadays psychiatrist use cloud computing to come across their patients from remote places, which makes their job easier. This is called tell the psychiatrist. As the patients maintaining many numbers of queues, the urgent patients have to wait in the same queue with normal patients, and they wait for their respective time. This situation is undesirable. Then the collection of real-time monitoring of patients vital data becomes a tedious job. A model is proposed in our paper where a single doctor is taken into consideration. A micro-controller model is being used here which consists of various smart sensors inside it. The smart sensors are kept intact with the patient's body. A support staff (named as ward boy) attaches the particular smart sensors to the particular patient's body. Then the sensors start recording the patient's vital data and they send it to the central database system. The model is strictly concerned about the minimization of the traffic intensity and the maximization of the throughput. As the proposed model works on WSN environment possibility of various attacks increases. One of the most important attack is considered, Black hole attack. To make our Model robust, a security algorithm is added in this model, which eradicates the complications from the sensors. The salient features of the security algorithm are also described.**

***Index Terms*—Telemedicine; Smart Sensors; Blackhole Attack; Backup Time.**

I. Introduction

Telemedicine has become a boon for mankind since years. Patient's vital data is recorded by the support staff and sent to the central database by using cloud environment [1]. The data is fetched by an authorized doctor. The doctor observes patients condition via a web-cam [2]. With the advent of cloud computing, sensor networks, and automation of health care institution, these technologies are feasible for implementation. Considering the recent World bank survey, 70% of the world's population lives in rural area [3]. As most of the doctors prefer urban areas, the rural area patients get neglected [4]. In order to overcome this situation, a telemedicine solution is proposed here, so that patients from rural (remote) areas can be benefited. Apart from the rural area, various remote area patients will also be benefited using telemedicine [5]. In our proposed model patients are diagnosed through a web-cam by a physician. The proposed model includes heterogeneous smart sensors (micro controller integrated with smart sensors) which are attached to patients bodies by a ward boy. Thereafter ward boy collects the data from smart sensors and transfers them to a central database situated in the server [1], [6]. The objective of this work is to propose a patients servicing system for remote areas and evaluate it using the generic parameters and to reduce the traffic intensity. While performing the work on telemedicine most of the researchers face the following challenges, such as: infrastructure, flexibility (platform), & acceptance.

As the patients gathering increases the diagnoses time also increase. As a result, lots of delays occur. Computationally, the traffic intensity increases. As the patients have to maintain many numbers of queues, the time taken for individual patient's diagnosis will take a lot of time. This situation is undesirable for critical patients. Then the collection of real-time monitoring of patient's vital data becomes a tedious job. Our model reduces the traffic intensity by categorizing the patients into three types. They are; (i)emergency patients,(ii)on-demand patients, and(iii)normal patients. Then the patients are prioritized and they are arranged in a queuing fashion. The model reduces the traffic intensity by using the above three sub models. After the model the security area related to the proposed model is concerned.

We are using various heterogeneous sensors modules inside the micro controller. When the data from patients body is recorded through various smart-sensors, the sensitive information of patients is sent to the server. During the transmission process, some sensors show wrong data or won't send any data due to packet drop. This situation tells that some sensors are corrupted or faulty [7]. Under WNS infrastructure there is a higher possibility of security threats like black hole attack, DoS (denial of service) attack, spoofing etc. But as all the sensors sending their individual recorded information to the server, therefore the possibility of black hole attack increases. There exist no efficient solution so far in the detection of black hole attack, and no efficient algorithms proposed. To make our model robust, a black hole prevention model is also proposed.

II. Related Works

To eliminate the barrier between distant patients and doctor, telemedicine has been introduced since years. The developed countries like US, UK, Canada etc are already succeeded in telemedicine programs and regularly adding new features to this technology. There exist few works which are having

similar solutions. The analysis falls into two categories: (i) solutions for telemedicine and automated information gathering, & (ii) solutions for data gathering on WSN (wireless sensor networks [8]).

In the work [2], UbiMon (also known as Ubiquitous monitoring environment for wearable and implantable sensors) is used. The author proposed a model for patient's monitoring system. The interface ready to process, store and acquire the tasks but this platform fails to record the on-demand vital data about the patients. In work [9], the author proposes a multiuser, collaborative environment with multi-modal human and computer communication by considering the vision, sound, and sensitivity. The communication is done by eye-tracking, cognition system, and micro-beam pen. Though noise in the channel is a primary factor in the method, the author's explanation is not satisfactory. The work in [10] introduced a monitoring model for various significant signs, which is based on mobile gadgets and remote maintenance. It used wearable sensors to collect critical messages (signals). The WBS (wearable bio-sensors) are used for the cardiovascular monitoring system. It addressed both scientific and clinical concerns about WBS but the model fails if a large scale medical environment is concerned. The work in [11], says about wireless sensor networks to patient's data gathering. The work utilized micro-controllers for the collection of patient's information. This result is not concerned with distribution and big scale maintenance. The work in [1], says that it eradicates the manual note making and information recording through sensors. This work doesn't consider any delay when a lot of patients are trying to access the treatment. The work in [6], says there exist a solution, based on web accessing is done in wireless manner. The mobile devices processed the cloud to parse HTML components for web pages. As our primary objective is to reduce the traffic intensity for the queues and to make our model a secured one, we can conclude that none of the analyzed solutions are satisfying our requirements completely.

In many papers, authors neglected the security issues in their respective works. This is the major loophole if a practical approach is considered. In many papers, authors are keeping all the patients within the same group without giving any priority to urgent patients irrespective of our model. In the proposed model, we grouped the patients into three category which eradicates the unwanted time delay for urgent patience.

III. Proposed Work

We have assumed that, there are various remote areas having individual health care institutions (or hospitals having medicine stores) [5]. There is a single doctor who is working on the entire model. A micro-controller (having various smart sensors attached within) is taken, which is attached to the patients bodies. As the patients have to maintain many numbers of queues, the time taken for individual patient's diagnosis will take a lot of time. This situation is undesirable. Then the collection of real-time monitoring of patient's vital data becomes a tedious job. To reduce the traffic intensity is

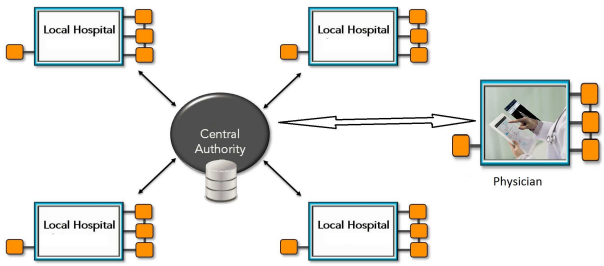

Fig. 1: Proposed solution

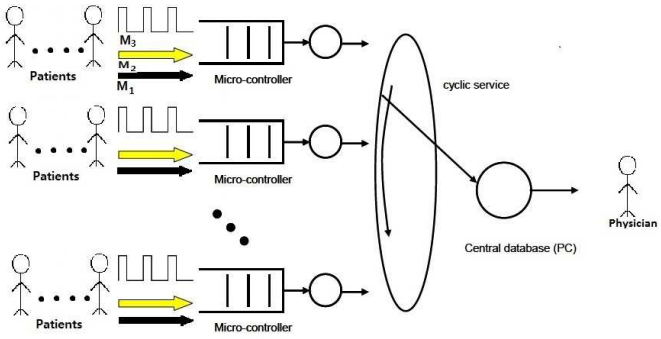

Fig. 2: Model of proposed work

our objective. Therefore to minimize the traffic intensity, the patients are categorized into three groups such as:

1) Emergency patients: These patients are given the first priority. For these patients the support staff collects data and saves the messages as M_1 type message. Severe injuries related to nervous system, BP etc are the examples.
2) On-Demand patients: These patients are given the second priority. Seasonal diseases like influenza, allergy, chickenpox, flu etc are the examples. For these patients the support staff collects data and saves the messages as M_2 type message.
3) Normal patients: These patients are given least priority compared to the above two. Examples are cold, fever etc.

Also the data of various medicines (i.e. low cost and high cost medicines) are stored to database. It is accessible to medical staffs and an authorized physician. If a particular medicine is not available, then the staff member will communicate to the nearest remote hospital. He will message to the central database, then the physician decides to send the required medicine, and after then the database will be updated.

A. Implementation (Model For Patient's Servicing System)

The proposed model consists of various patient's queues, which will be categorized by the support staff.

This model assumes that, the micro-controllers to be operated as queuing servers. The central server polls the group of M micro-controllers for traffic, with respect to the current situation.

B. Assumptions

1) The i^{th} $(1 \leq i \leq M)$ micro-controller is connected to N_i different sensors. P number of patients are attached to the i^{th} micro-controller, having N_i different body sensors.
2) The resultant messages for the j^{th} $(1 \leq j \leq N_i)$ sensor are categorized as three types:
   a) Type 1: Emergency messages (for emergency/critical patients written as M_E):- As any number of patients comes randomly Poisson distribution is considered for these messages. These messages have higher priority over type 2 and type 3 messages. According to Poisson rate m_{1j} bytes generated for λ_{1j} message per second.
   b) Type 2: On-demand messages (on-demand patients symbolizes as M_O):- The On-demand patients suffer from seasonal diseases. This model is concerned about uniform random distribution with certain time interval. According to uniform distribution m_{2j} bytes generated for α_{2j} message per second. These messages have higher priority over type 3 and lesser priority than type 1 messages.
   c) Type 3: Normal or Periodic messages (for normal patients written as M_N). This will be done by FCFS (first come first serve) basis, m_{3j} bytes every T_j seconds.
3) The micro-controller serves at the rate of C_m bytes per second.
4) M number of micro-controllers are connected to the central system using IEEE 802.15.4.
5) The central system polls each message and processes at the rate of C_c bytes per second.

C. Time complexity Calculation

The Algorithm 1 takes $\mathcal{O}(N \log N)$ time with N number of smart sensor nodes and M number of micro controllers.

Line number: (1),(2),(3) run on $\mathcal{O}(1)$ of time, (4) runs on $\mathcal{O}(MN)$ of time=$\mathcal{O}(N)$, (5) runs on $\mathcal{O}(N \log N)$ of time, (6) runs on $\mathcal{O}(N \log N)$ of time, (7) runs on $\mathcal{O}(R)$=$\mathcal{O}(MN)$=$\mathcal{O}(N)$ of time, (8) runs on $\mathcal{O}(R)$=$\mathcal{O}(MN)$=$\mathcal{O}(N)$ of time. Hence the time complexity becomes $\mathcal{O}(N \log N)$

Algorithm 1 Algorithm for Patient's Servicing System

1: Initialize: M number of Micro-controller & N number of smart sensor;
2: Initialize: 3 types of messages (Emergency message=M_E, On-demand message=M_O, & Normal message=M_N);
3: Set the priority of messages (lower is the value priority is more, i.e. M_E=1, M_O=2, & M_N=3);
4: **for** Each micro-controller, $i = 1$ to M **do**
5: **for** Each sensor node, $j = 1$ to N **do**
6: Calculate the arrival time (AT) of message X_{ij};
7: **end for**
8: **end for**
9: Sort the messages with respect to the arrival time (AT) and end time (τ), where AT=0 to τ;
10: Sort the messages w.r.t its priority;
11: **for** Each message R, where $R = M \times N$ **do**
12: **if** Priority($X_{i,j}$)=1 **then**
13: $\overrightarrow{R_E} \leftarrow X_{ij}$;
14: **else**
15: **if** Priority($X_{i,j}$)=2 **then**
16: $\overrightarrow{R_O} \leftarrow X_{ij}$;
17: **else**
18: $\overrightarrow{R_N} \leftarrow X_{ij}$;
19: **end if**
20: **end if**
21: **end for**
22: **for** Each time instance, $j = 0$ to τ **do**
23: Process the messages $\overrightarrow{R_E}$, $\overrightarrow{R_O}$, & $\overrightarrow{R_N}$ respectively with first come first serve.
24: **end for**
25: Fetch the Patient's data from the central database by the Physician;

IV. Security in Patient's Servicing System

The proposed model considers various heterogeneous medical sensors inside the micro-controller. We are taking various smart sensors inside the micro-controller. As the proposed model is made for remote area again we have considered low computational power, low energy and low bandwidth. When the data from patients body is recorded through various smart-sensors, the sensitive information of patients is sent to the server. During the transmission process some sensors show wrong data or won't send any data due to packet drop. This situation tells that some sensors are corrupted or faulty [12], [13]. Because of this, the patients will suffer a lot in future.

The black holes are also called as sink holes [14]. Back hole attack is one type of Denial of Service attack, where a malicious node is present inside the network. That malicious node pretends to be a normal node and it gives false REP message to source node [15]. Due to which source node sends the data packets through that path but the malicious node drops them fully or partially. To make our model robust, a black hole prevention model is proposed. the security feature we have considered is made to prevent the black-hole attack in the micro-controller.

A. Proposed Model for Prevention Black Hole Attack

In the proposed model a source node and a destination node is considered, where the micro-controller works as source node and the server works as destination node. In this model, some formula have been discussed. They are: (i) Source node: From where the message packet starts traveling, here the smart sensors are the source nodes, (ii) Destination node: Here the central server works as destination node, (iii) REQ: Read as "Request Message", (iv) REP: Read as "Reply Message", (v) Average Delay: Delay can be defined as the time taken for a message packet to reach the destination, and the average delay can be calculated by taking the mean of all delays for

every message packets sent, (vi) PDR (Packet Delivery Ratio): It is the ratio between total number of packets received and total number of packets sent, (vii) Backup Time(BT): BT= $2 \times propagationtime$ + transmission time + queuing time. It is also considered as $2 \times propagationtime$, by neglecting transmission time and queuing time. Generally within an BT all the packets must be received [16]. But in case of traffic delay, sometimes congestion occurs in the network. So this causes packet loss. Thats why in this model considers a limiting time (ending time) named as backup time. In this model backup time is considered as double of reply time ($2 \times REP$).

Algorithm 2 Algorithm For Prevention of Black Hole Attack

1: Initialize $MaxTh = \theta_1$, $MinTh = \theta_2$;
2: Broadcast REQ message to server;
3: Wait for REP message;
4: Set Back up time $(BT) = REQ + 2 \times REP$;
5: **for** $i = 1$ to N **do**
6: Each node $n_i \in N$;
7: **if** $WT(n_i) > BT(n_i)$ **then**
8: Then n_i declared as Malicious node;
9: **else**
10: Then send the correct message to the server;
11: **end if**
12: **end for**
13: **for** $i = 1$ to N **do**
14: **for** $j = 1$ to T **do**
15: Calculate the sensor value x_{ij} for sensor node $n_i \in N$ at j^th time instance;
16: **end for**
17: **end for**
18: **for** $i = 1$ to N **do**
19: **for** $j = 1$ to T **do**
20: **if** $x_{ij} < \theta_1$ or $x_{ij} > \theta_2$ **then**
21: Then x_{ij} is a faulty value;
22: **else**
23: x_{ij} is a fault free value;
24: **end if**
25: **end for**
26: **end for**

Minimum threshold (θ_1) and Maximum threshold (θ_2) are set already. If the threshold value is not recorded within the range by the sensor, then the sensor is identified as corrupted. The threshold value varies for different parameters and different conditions. Eg. for temperature the threshold value varies from 97.7^0F to 99.5^0F. For blood pressure the threshold value varies from 90 mmHg to 250 mmHg etc.

B. Time complexity for Prevention Algorithm Calculation

The Algorithm 2 takes $\mathcal{O}(N)$ time with N number of smart sensors (nodes).

Line no: (1),(2),(3),(4) run on $\mathcal{O}(1)$ of time, (5) runs on $\mathcal{O}(N)$ of time, (6) runs on $\mathcal{O}(N)$ of time, (13) runs on $\mathcal{O}(N)$ of time, (18) runs on $\mathcal{O}(NT)$=$\mathcal{O}(N)$ of time, as $N >> T$. Hence the time complexity becomes $\mathcal{O}(N)$.

V. Simulation and Result

The total traffic intensity is given by $\rho = \frac{MN}{C_s}(\lambda_s m_1 + \alpha_s m_2 + m_3/T)$.

The simulation algorithm ran on NS2 environment of version 2.35. The simulation environment depends on some specific parameters. The values and ranges of those specific parameters are given below in the Table I.

TABLE I: Simulation Parameters

Parameter(s)	Value(s)
Number of smart sensor nodes	50
Simulator	NS2,Version 2.35
Simulation time	200 Seconds
Simulation area	$400 \times 400\ Meter^2$
Transmission Range	250 Meters
Carrier sense range	350 Meters
Packet size	512 Bytes
MAC protocol	IEEE 802.15.4
Traffic type	CBR(Constant Bit Rate)
Agent(connection protocol)	UDP(User Datagram Protocol)
Data rate	5 Mbps
REP Waiting Time	2 Seconds
Black hole node	2

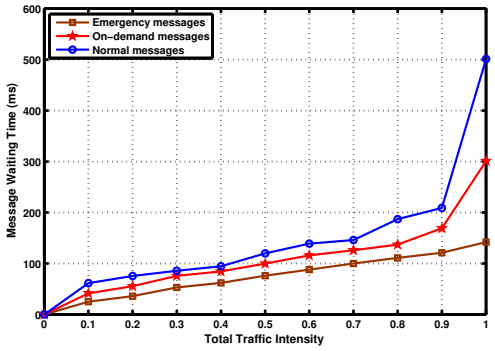

Fig. 3: Traffic intensity vs Message waiting time

Figure 3 depicts the message waiting time (for three types of messages) versus network traffic intensity. The emergency messages shows lesser waiting time with respect to both on-demand and normal messages. According to our model.

Figure 4 depicts typically message loss rate for 3 types of messages vs network traffic intensity. It is clearly observed that emergency messages experience less message loss rate with respect to both on-demand and normal messages. In our proposed scheme emergency message's priority is higher as compared to other messages, so the sensors in the micro-controller processes prioritized messages first. Therefore the message loss rate i.e. the ratio between the drop messages and the total number of sent messages of emergency messages is lesser than the rest two messages.

Figure 5 depicts the average throughput for 3 types of messages vs network traffic intensity. In this figure, the throughput

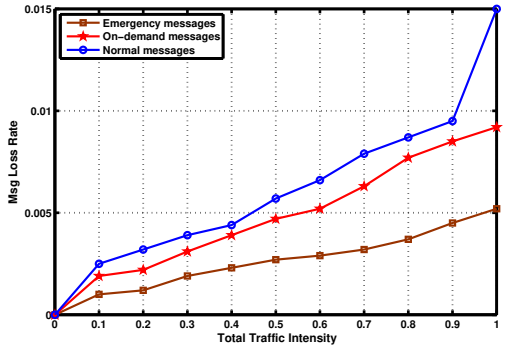

Fig. 4: Traffic intensity vs Message Loss Rate

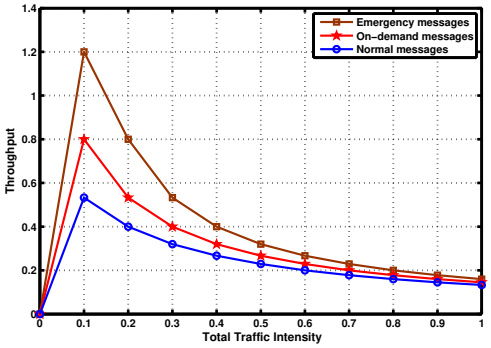

Fig. 5: Traffic intensity vs throughput

of the emergency messages is better as compared to on demand messages and normal messages. The throughput of the network initially higher and when the traffic intensity increase, the throughput value decreases for all the three messages. As the emergency packets delivery rate per unit time is higher than the on-demand packets and normal packets then the throughput of emergency packets is better as compared to other two packets in higher traffic intensity also.

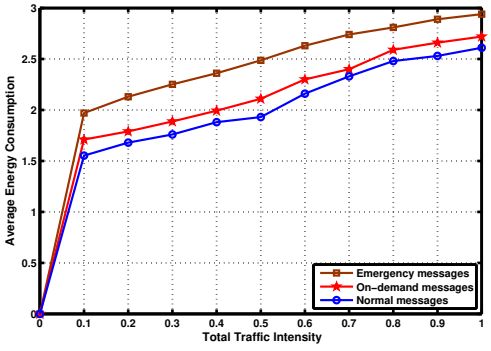

Fig. 6: Traffic intensity vs energy consumption

Figure 6 depicts the average energy consumption for three types of messages vs network traffic intensity. The average energy consumption increases when traffic intensity increases for all the three types of messages. As the emergency packet message loss rate is less and the waiting time is less, the energy consumption per node becomes also less, compared to other two messages. The normal messages are the less priority message which throughput is less than other messages, so the energy consumption for normal message is less than on demand and emergency message.

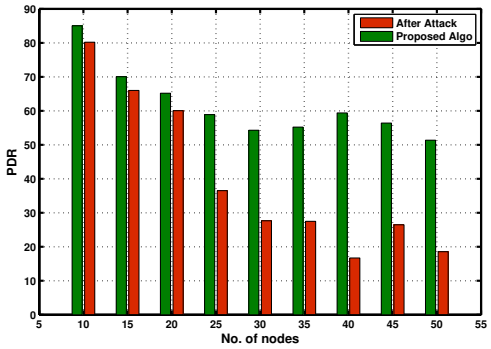

Fig. 7: Number of nodes Vs PDR

In above graph 7 due to black hole attack in smart sensors, the PDR is decreasing with the increase of number of smart sensor nodes in the micro-controller, But after modification by the proposed algorithm, the packet delivery ratio gives better result.

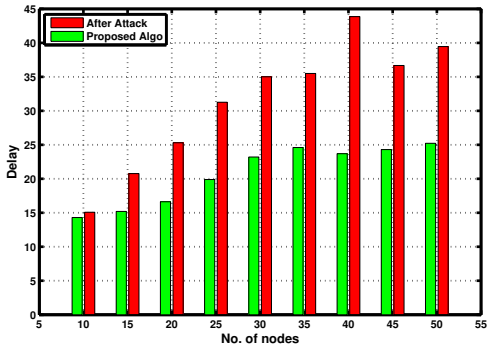

Fig. 8: Number of nodes Vs Delay

Figure 8 depicts the increasing delay with increase in number of sensor nodes. After the detection of all the malicious nodes present inside micro-controller the communication starts with the server (destination). By using the proposed algorithm, the result will be better compared to previous one.

Figure 9 due to black hole attack in smart sensors, valid packets are dropped by malicious nodes which creates delay. But after modification in algorithm, malicious nodes can be detected and replaced with proficient sensors. Hence throughput increases in the network.

We have gone through two proposed algorithms i.e. the Patient's servicing system algorithm and the Black-hole prevention algorithm. The Patient's servicing system algorithm

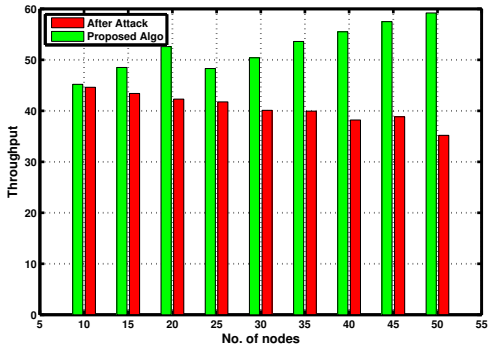

Fig. 9: Number of nodes Vs Throughput

takes $\mathcal{O}(N \log N)$ time and the Black hole Prevention algorithm takes $\mathcal{O}(N)$ time.Therefore the overall time complexity becomes $\mathcal{O}(N \log N)$.

VI. Conclusions

The implementation has various practical advantages. Such as it collects always real-time data, it overcomes from manual note making so that no typing error could occur and, it makes easier the installation process. WSN meant no need of cabling or any physical setup. Re-usability can be seen. This work contributes to the field of science and society. As expert medical staffs are not available all the time, only a single authorized doctor is taken into consideration. This proposed model is very much helpful in saving the time, for many doctors and also helps in reducing workloads of support staffs in medical environment. The traffic intensity decreased in our model, after all the patients were prioritized. Previously no security models were added in any of the telemedicine research papers so far. But in our model, a black hole prevention model is added to our Patience Servicing System Model. The implementation results were satisfying and the time complexity achieved is $\mathcal{O}(N \log N)$.

Due to its pragmatic approach the model can be said as a cost-effective solution which satisfies the modernization telemedicine concept in developing countries. The quality of medical assistance is improved by using our model. As a future work, we will propose a real world setup and the automation process will be implemented over cloud.

References

[1] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in *eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10. Second International Conference on*, pp. 95–99, IEEE, 2010.

[2] J. W. Ng, B. P. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G.-Z. Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (ubimon)," in *International Conference on Ubiquitous Computing (Ubicomp)*, Citeseer, 2004.

[3] "The world bank rural population data." http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS. Accessed: 2017-04-02.

[4] K. Singh and K. Singh, "Biotelemetry: could technological developments assist healthcare in rural india," *Rural Remote Health*, vol. 5, no. 2, p. 24, 2005.

[5] M. Burrow, M. Sinclair, and T. Gadacz, "A telemedicine testbed for developing and evaluating telerobotic tools for rural health care," *Medicine Meets Virtual Reality. San Diego, CA*, 1994.

[6] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities," in *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*, pp. 5–13, Ieee, 2008.

[7] A. Mahapatro and P. M. Khilar, "Fault diagnosis in wireless sensor networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2000–2026, 2013.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[9] M. Aakay, I. Marsic, A. Medl, and G. Bu, "A system for medical consultation and education using multimodal human/machine communication," *IEEE Transactions on information technology in Biomedicine*, vol. 2, no. 4, pp. 282–291, 1998.

[10] H. H. Asada, P. Shaltis, A. Reisner, S. Rhee, and R. C. Hutchinson, "Mobile monitoring with wearable photoplethysmographic biosensors," *IEEE engineering in medicine and biology magazine*, vol. 22, no. 3, pp. 28–40, 2003.

[11] T. R. Sheltami, A. S. Mahmoud, and M. H. Abu-Amara, "An ad hoc wireless sensor network for telemedicine applications," *Arabian Journal for Science and Engineering*, vol. 32, no. 1, pp. 131–146, 2007.

[12] R. R. Swain and P. M. Khilar, "Composite fault diagnosis in wireless sensor networks using neural networks," *Wireless Personal Communications*, vol. 95, no. 3, pp. 2507–2548, 2017.

[13] R. R. Swain and P. M. Khilar, "Soft fault diagnosis in wireless sensor networks using pso based classification," in *2017 IEEE Region 10 Conference (TENCON)*, pp. 2456–2461, Nov 2017.

[14] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 2, pp. 4–18, 2005.

[15] K. Madhusudhananagakumar and G. Aghila, "A survey on black hole attacks on aodv protocol in manet," *International Journal of Computer Applications (0975–8887) Volume*, pp. 23–30, 2011.

[16] R. R. Swain, P. M. Khilar, and S. K. Bhoi, "Heterogeneous fault diagnosis for wireless sensor networks," *Ad Hoc Networks*, vol. 69, pp. 15–37, 2018.