Abstract

Objectives: This paper emphasizes on the security and privacy of the healthcare data with the help of encryption techniques and to control congestion in the data and study of various techniques which are helpful for maintenance and safety of the data. Methods/Statistical Analysis: There are various kinds of methods adapted by researchers for improving congestion mechanism and the security of healthcare information. Every method varies on the basis of the different parameters and their requirements. Methods are enhanced by using different encryption techniques and by developing secure key exchange data system in which data is transferred from patient to doctor through keys. Findings: This research manuscript shows the secure healthcare system is required to be developed or maintained. As healthcare has important role in day to day life particularly just in case of adulthood those that suffers from diseases like mental issues, vital sign, diabetes, heart issues, etc. For developing secure system secure key exchange between information is required developing keys that exchange information between consumer and the server could do this. These keys can take information from server and send it to a consumer by secure path using cryptography techniques so cannot be browse by an unauthorized user and what is more, these healthcare systems are planned for the case so immediate treatment is given to a patient when required. This paper provides the method to record health information of patients by the Health Record Management System (HRMS). Application/Improvements: To work in such cases, there is a need to develop a system which improves QOS (quality of service), efficiency, throughput, end to end time delay, etc.

Keywords: Electronic Healthcare, Healthcare Information System, Information Security, Privacy, Research Literature

1. Introduction

Typically, the wireless sensor network contains hundreds or thousands or more than that of wireless sensor nodes, in which all nodes are attached to one or more sensors. The sensor nodes commute with everyone using radio signals. The wireless sensor area has a number of detection stations called sensor motes, each of which is small, portable and lightweight. Every sensor node consists of a microcomputer or microcontroller, transceiver, transducer and the power source. Based on physical sensed effects and facts the transducers produce electrical signals. Microcontroller processes and stores the sensor output. The commands from a central computer are received by the transceiver and then transceiver transmits data to that computer. And the battery derives power for sensors.

1.1 Wireless Sensors

Wireless sensor nodes use sensors to capture data from the environment. The wireless sensors are the hardware devices that offer a computable comeback to a transform in the physical environment conditions like pressure, temperature, etc. Sensors calculate physical data of the device to be observed and have specific features such as sensitivity, accuracy etc. We may also define sensor as an object whose purpose is to detect processes or changes in its surroundings and then give a corresponding output. The sensor is a sort of transducer; that offers a variety of output, but usually uses electrical and optical signals.
These are implemented on a daily basis life in substances like the touch-handly elevator fixtures (tactile sensors) and the lamps which brighten or diffuse by tendering the base in addition, immeasurable applications of which most people are not aware.

1.2 Communication in Sensor Networks

The recent progress of MEMS (Micro Electro Mechanical Systems) skill, the sensor communication and the digitalelectronics has made promising the progress of low power, low cost, multiple practical nodes that are miniature in extent and commune untethered in a little distance. The miniature motes that have a communicating mechanism, processing of data, and sensing used the thought of sensor network implemented on mutual exertion of a great number of nodes. New wireless sensor networks correspond to a momentous enhancement over established sensors that are then used in the given following ways:

- In the approach, where huge sensors that make use of some composite mechanisms to differentiate the intention from environmental noise are needed in this the sensors can be situated far from the main features, i.e., something acknowledged by sense acuity.
- Many sensors which execute simply sensing can be used (as per Table 1). Moreover, the situation of the topology and sensors of communications is watchfully maintained. And they pass on time successions of the sensed event to the main vital nodes in which the computations are executed also the information is merged.

Table 1. WSN Security threats and possible solutions

<table>
<thead>
<tr>
<th>Security Threats</th>
<th>Security needs</th>
<th>Solutions for threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthenticated access</td>
<td>Key establishment and trust set up</td>
<td>Random key distribution</td>
</tr>
<tr>
<td>Message disclosure</td>
<td>Confidentiality and privacy</td>
<td>Access Control</td>
</tr>
<tr>
<td>Message modification</td>
<td>Integrity</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Denial of service attack (DOS)</td>
<td>Accessibility</td>
<td>Interruption detection</td>
</tr>
<tr>
<td>Routing attacks</td>
<td>Safe routing</td>
<td>Safe routing protocols</td>
</tr>
<tr>
<td>High level security attacks</td>
<td>Intrusion detection</td>
<td>Secure group communication</td>
</tr>
</tbody>
</table>

1.3 Wireless Sensor Network Security Threats and Solutions for Those Threats

1.4 Healthcare Monitoring

The medicinal uses are of two types: Implanted and Wearable. The wearable applications are employed on the body of an individual or at the closeness of the client. And the Implantable tools are those which are introduced within individual body. Several other applications are also there e.g. location of the person and body position measurement, generally examining of people who are not well in hospitals and at their residence. Wireless body area networks can collect data about an individual’s energy expenditure, health and wellness. In this work (as per Table 2) the main focus is on healthcare applications and ECG of patients is monitored.

1.5 Advantages of Wireless Sensor Networks in Healthcare

The applications of healthcare networks are explained:

- **Portability and Unobtrusiveness**
  Small devices gather data and commune in the network wirelessly, and run with minimal patients’ input. All these can be conceded on the human body and are severely embedded in the surroundings.

Table 2. The design considerations of healthcare network

<table>
<thead>
<tr>
<th>Sub-system</th>
<th>Design considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human body area network (HBAN) sub-system</td>
<td>Energy utilization Broadcast power Portability Real time system (RTS) Reliable communications Security</td>
</tr>
<tr>
<td>Individual area network sub-system</td>
<td>Energy effectiveness Scalability Self-organisation In between the nodes</td>
</tr>
<tr>
<td>Wide area network (WAN)</td>
<td>Data rate Reliable comunicación protocol Secure data transmission Coverage</td>
</tr>
<tr>
<td>End-user health-care examining application</td>
<td>Security Scalability Interoperability</td>
</tr>
</tbody>
</table>
• **Ease of Operation and Scalability**

Sensors are used in potentially in huge number with severely less complication and overhead in comparison to wired networks. Active structures, mostly decaying ones, will be simply better through a WSN while wired installations would be pricey and impossible.

• **Real Time or Always On**

Physiological and ecological facts can be examined constantly, permitting real time answer by emergency members. The information taken for a health precious and for covering in gaps in the conventional patient’s history

In recent years, the research of developing healthcare has attracted the people a lot. In this system we will develop the secure system for health data that has privacy of data by using the mechanism of secure key exchange mechanism. The following written papers helped a lot to understand and implement the algorithm used in healthcare systems and that will be used in my project. It is the first step that encourages a lot to move forward with the objective of our own development.

In 1proposed that in WSNs, congestion takes place because of the given features: Packet Collision (PC), Mote buffer overflow, broadcast rate, many-to-one data transmission scheme, channels broadcast contention and Dynamic time variation transmission channel. Certainly, congestion has a major effect on Quality of Services factors like Packet Delivery Ratio (PDR), end-to-end impediment and power utilization in wireless motes. In this author presented an inclusive study of main congestion control schemes employed in WSNs and shows the accessible methods into 4 categories i.e. queue assisted protocols, resource control protocols, priority aware and traffic control protocols.

In 2examined congestion control techniques in Wireless Sensor Networks. He compared and reviewed the existing few number of research studies on congestion control in WSNs without any classifications. Also, here viewed different performance metrics used for measuring congestion in WSNs. Nevertheless, he failed to include the impacts and findings of the conducted studies and did not discuss the theoretical and practical implications of the available studies.

In 3put forward a Key management algorithm that is Key It Simple and Secure (KISS). His paper showed new key management architecture, known as KISS, to facilitate trustworthy, client-verifiable, comprehensive, and cost-efficient key management. The algorithm key it simple and secure protects and secures the whole process circle of cryptographic keys. In scrupulous, KISS permits only the certified submissions and/or clients to utilize the keys. By employing simple devices, the administrators can distantly give validated commands to KISS and gives system output. This algorithm influences readily available product hardware and trusted computing primitives to design system bootstrap protocols and management mechanisms that will protect the system from malware attacks and insider attacks.

In 4 described Smart Vest, a wearable physiological examining structure that comprises of a vest that employs a number of sensors fixed on the fabric material to concurrently gather several medical signals in a noninvasive and unremarkable manner. Features calculated are ECG, Photo Plethysmo Grapy (PPG), heart rate, Body Temperature (BT), Blood Pressure (BP), and Galvanic Skin Response (GSR). Also, it is declared that the ECG can be taken without any exploitation of gel and that its recording is free of baseline noise and action artefacts because of h/w execute high pass, low pass, and notch filters. Besides this BP is measured non-invasively with PPT, where the executed detection algorithm is individually adjusted based on the individual ECG. Some pro and cons are defined as per Table 3.

2. **Problem Formulation**

- The patients are informed with the help of medical database centers about their health on regular basis i.e. daily, weekly or monthly basis by sending reports to their home or on their emails.
- In healthcare monitoring data is amassed on the servers and a variety of algorithms are used for the analysis of data of health.
- Main issue in these healthcare-monitoring systems is privacy of data.
- In healthcare data privacy algorithms based on authentication scheme are in the base paper that has been proposed.
- Existing authentication scheme is based on secure key exchange. In the subsisting system, these have not focused upon bandwidth allocation and Quality of Service (QoS).
- In this research, scope is attempting to solve the troubles of data integrity and confidentiality by adding together various algorithms and security protocols with the active authentication based on healthcare monitoring systems.
Table 3. Related work of researchers in this area

<table>
<thead>
<tr>
<th>Year of Publication</th>
<th>Techniques</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>K_{tss}, “K_{it}; S_{mpl} and S_{cr}“ Corporate K_{M_{g}}</td>
<td>This Show new K_{M_{g}} A_{sc}, known as K_{tss}, to F_{tss}, T_{g}, client-verifiable, C_{cr} and cost-effective K_{M_{g}}. The algorithm k_{it} S_{mpl} and S_{cr}. The whole life cycle of c_{r}, c_{sc}. In future more s_{w}, n_{p} can be made by putting control over s_{mp}, threat by t_{smg}, data t_{hr}, s_{cr} k_{ex}.</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>C_{g}, c_{mp} m_{exm} in WSNs</td>
<td>It compares the impact t_{dn} with each other in terms of c_{g}, d_{au}, c_{mp}, n_{in} and c_{mp}, m_{gn} as well as d_{mp} for future researchers and work.</td>
<td>It show that in future c_{g} can be controlled by t_{mg}, less amount of d_{au} and c_{mp}, t_{in} can also be used for the p_{rsc} of d_{au}.</td>
</tr>
<tr>
<td>2008</td>
<td>S_{mp}, V_{p}; W_{mp} m_{exm} p_{rsc} remote p_{mp} monitoring system</td>
<td>This describes S_{mp}, V_{p} a w_{p}, d_{au}, P_{mp}, examining s_{mp}, that compares of a v_{p}, which c_{mp}, n_{mp}, s_{mp}, i_{mp}, on the garment material to c_{nty}, g_{mp}, s_{mp}, t_{mp}, a non i_{mp} and u_{mp}, m_{mp}.</td>
<td>In future s_{mp} function like c_{mp}, d_{au}, p_{rsc}, can be m_{rsc} by k_{ex} exchange methods.</td>
</tr>
<tr>
<td>2011</td>
<td>A ; s_{rsc} on c_{mp} control t_{dn} in WSN</td>
<td>It examined c_{mp}, control t_{dn} in WSN. He compared and t_{rd} the e_{rsc}, few n_{rsc}, of r_{rsc}, s_{rsc}, on c_{mp}, c_{rsc} in W_{mp} without any c_{mp}, A_{sc}, here v_{rd}, d_{au}cimiento m_{gn} for m_{mp}, g_{mp} in W_{mp}</td>
<td>This s_{rsc} failed to include the impact and f_{rd}, of the c_{mp}, s_{rsc}, and did not describes the t_{rsc} and p_{rsc}, of the available s_{rsc}.</td>
</tr>
</tbody>
</table>

KISS_ Key it simple and secure, Key_ky, Management_Mgt, Showed_Shw, Architecture_Arch, Known_K, Facilitate_Fct, Trustworthy_T, Comprehensive_C, Cost_C, Efficient_e, Algorithm_a, Simple_S, Secure_S, Protects_P, Cryptographic_C, more_m, wireless_w, network_n, putting, p control_c control, over_o, security, s, threats th, transmitting t smg, data d au, mechanism m, sensor s, compares c, important i, techniques t, detection d, notification n, mitigation m, directions d, transferring t, encryption e, privacy p, smart s, vest_v, wearable_w, multi m, parameters p, physiological p, structure s, compromise c, employs e, number_n, confidentiality c, maintained m, integrated i, garment g, material m, concurrently c, invasive t, unrewarded u, wearable w, network n, reviewed r, existing c, studies s, without w, classifications c, viewed v, different d, performance p, metrics m, findings f, conducted c, theoretical t, practical p, implications i, mplexes m, available a.

Table 3. (a) Total transmission time analysis on 2G network, (b) Total transmission time analysis on wifi network, (c) Aggregation efficiency on 2G network, (d) Aggregation efficiency on WIFI network, (e) End to End delay analysis on 2G network, (f)End to End delay analysis on WiFi network

<table>
<thead>
<tr>
<th>No. Of nodes</th>
<th>Total Transmission time</th>
<th>Avg. Transmission time</th>
<th>Median Transmission time</th>
<th>Min. Transmission time</th>
<th>Max. Transmission time</th>
<th>End to End delay</th>
<th>Aggregation time</th>
<th>Aggregation efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>21.5498</td>
<td>0.476</td>
<td>0.507</td>
<td>0.467</td>
<td>1.23</td>
<td>0.1</td>
<td>0.011</td>
<td>0.001</td>
</tr>
<tr>
<td>25</td>
<td>23.0691</td>
<td>0.592</td>
<td>0.517</td>
<td>0.483</td>
<td>1.87</td>
<td>0.181</td>
<td>0.021</td>
<td>0.002</td>
</tr>
<tr>
<td>50</td>
<td>30.6414</td>
<td>0.691</td>
<td>0.524</td>
<td>0.487</td>
<td>1.881</td>
<td>0.11</td>
<td>0.093</td>
<td>0.003</td>
</tr>
</tbody>
</table>

(a)

<table>
<thead>
<tr>
<th>No. Of nodes</th>
<th>Total Transmission time</th>
<th>Avg. Transmission time</th>
<th>Median Transmission time</th>
<th>Min. Transmission time</th>
<th>Max. Transmission time</th>
<th>End to End delay</th>
<th>Aggregation time</th>
<th>Aggregation efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>12.313</td>
<td>0.308</td>
<td>0.274</td>
<td>0.26</td>
<td>0.82</td>
<td>0.048</td>
<td>0.015</td>
<td>0.002</td>
</tr>
<tr>
<td>25</td>
<td>16.5422</td>
<td>0.414</td>
<td>0.279</td>
<td>0.261</td>
<td>2.117</td>
<td>0.153</td>
<td>0.029</td>
<td>0.002</td>
</tr>
<tr>
<td>50</td>
<td>24.0082</td>
<td>0.632</td>
<td>0.288</td>
<td>0.265</td>
<td>3.814</td>
<td>0.367</td>
<td>0.046</td>
<td>0.002</td>
</tr>
</tbody>
</table>

(b)
3. Proposed System and System Design

In order to be unique or universal system, the secure healthcare system is needed to be developed or maintained. As healthcare has vital role in day to day life especially in case of old age people who suffer from diseases like mental problems, blood pressure, diabetes, heart problems, etc. For developing secure system secure key exchange between data is needed this can be done by developing keys that exchange data between client and server. These keys will take data from server and send it to client by secure path using encryption techniques so that cannot be read by unauthorized user and moreover, and this healthcare system is proposed for the case so that immediate treatment can be given to patient when needed. The keys in this system take data from (as from Figure 1) patient and send it to doctor or monitor (as per Figure 2) and then immediately treatment for that patient gets started. Our system send data as normal, critical and super critical when condition is normal then keys get combined and data of patients is send in a combined packet but in case data is critical or super critical then immediate information is given to doctor for the treatment.

3.1 Objectives of the HRMS Model

- To aggregate the normal data before offloading it to the cloud.
- To classify the data received by the BTS using three extra bits into three classes.

<table>
<thead>
<tr>
<th>No. Of nodes</th>
<th>Total Transmission time</th>
<th>Avg. Transmission time</th>
<th>Median Transmission time</th>
<th>Min. Transmission time</th>
<th>Max. Transmission time</th>
<th>End to End delay</th>
<th>Aggregation time</th>
<th>Aggregation efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>14.504</td>
<td>0.363</td>
<td>0.276</td>
<td>0.256</td>
<td>1.726</td>
<td>0.104</td>
<td>0.085</td>
<td>0.009</td>
</tr>
<tr>
<td>25</td>
<td>15.3238</td>
<td>0.383</td>
<td>0.286</td>
<td>0.263</td>
<td>1.811</td>
<td>0.12</td>
<td>0.025</td>
<td>0.002</td>
</tr>
<tr>
<td>50</td>
<td>17.755</td>
<td>0.444</td>
<td>0.285</td>
<td>0.263</td>
<td>2.552</td>
<td>0.18</td>
<td>0.018</td>
<td>0.002</td>
</tr>
</tbody>
</table>

3.1.1 Data Flow Diagram of ECG Monitoring

![Figure 1. Data flow diagram of ECG monitoring.](image)

3.1.2 Process of monitoring of patients

![Figure 2. Process of monitoring of patients.](image)
An Intelligent System to Improve Quality of Service in Healthcare Monitoring Over WSN

There are many smart health applications\textsuperscript{11} that are useful in calculating the various biological parameters. For this experiment, we are choosing ECG as the physiological parameter\textsuperscript{12}. The data on the smart mobile device is processed using the QRS Detect Algorithm; used for ECG calculations; and it is converted into the digital signal. The digital signal\textsuperscript{14} from the smart mobile device is thus transmitted onto the network in the communication channel. The following algorithm explains the working of the sensor nodes.

Algorithm: Computation of ECG by the QRS detect algorithm and the transmission of the signal on the network.

1. The sensor nodes sense the ECG signal from the human body.
2. The sensor nodes collect the information on the sampling rates of 256 or 512 bytes per second.
3. It rearranges and transmits the ECG signal to the smart phone device.
4. The smart phone loads the ECG signal.
5. The pre-embedded QRS detection algorithm in the smart-phones finds the QRS-peaks in the ECG signal.
6. The smart phone computes the heartbeat rate by calculating the number of QRS-peaks detected earlier.
7. The smart phone device then broadcasts the signal to the cloud healthcare network.

The processed data thus reaches the BTS in case of a cellular network\textsuperscript{14} and AP in case of a Wi-Fi network. The Base Transceiver Stations (BTS) or AP that acts as the aggregator node (as per Figure 4) receives the data. The major HRMS operation of aggregating data is performed by BTS. BTS of the network is chosen as the aggregator because it is highly secured point in the network and cannot be hacked. BTS performs two functionalities mainly i.e. Data Classification and Data Aggregation. Upon receiving the data; firstly, BTS classifies the data into three classes\textsuperscript{13} namely normal, critical and super critical. Data classification (as per Figure 5) is based on bits. Three extra bits are appended with the data bits to classify the data. Data classification\textsuperscript{16,17} is based on the nature of the data and the value of the physiological parameter being calculated.

Algorithm: To aggregate is an algorithm that explains the working of BTS while dealing with the data classification and performing aggregation. It classifies the data as super critical, critical and normal data. Aggregation is performed on the normal data and the super-critical and critical data are propagated with minimum delay.

1. The base transceiver station (BTS) receives the ECG signal from the smart phone\textsuperscript{18}.
2. The BTS evaluates the criticality level of the patients heartbeat by applying the following rule:

Figure 3. context level diagram of process.

Figure 4. Level 1 data flow diagram of ECG monitoring.

Figure 5. Level 1 data flow diagram of ECG monitoring.
Amit Verma, Madhu and Er. Amandeep Kaur

in terms of the communicational network i.e. cellular or Wi-Fi both at moderate and peak hour Figure 6 (a) represents the total transmission time analysis of the HRMS model on a 2G Network at moderate hours. The x-axis in the graph plots the dynamically changing patient data on the network. With the increasing number of sensor nodes, the patient data changes as ‘na’ where ‘n’ denotes the number of patients and ‘α’ may have character values as n, c, and s where n, c, and s denotes normal, critical and super-critical patients respectively. The y-axis plots time in seconds. It is quite clear form the graph that data the proposed HRMS model offloads the patient data in minimum transmission time while performing on 2G networks at moderate hours and the above graph (b) represents the aggregation efficiency of the HRMS model on a Wi-Fi Network at moderate hours. The normal data on the network is aggregated to improve the efficiency of the already existing health monitoring systems and to reduce network congestion. The x-axis in the graph plots the dynamically changing patient data on the network (Table 3 and Figure 7). With the increasing number of sensor nodes the patient data changes as ‘na’ where ‘n’ denotes nk.

a. Classified as Super critical, if beatRate > 150 or beatRate < 50.
b. Classified as critical, if (beatRate > 120 and beatRate <=150) or (beatRate >= 50 and beatRate < 65)
c. And Normal otherwise.

3. The super critical and critical patient information is marked as the important using the three-bit pattern, whereas the normal heart beat rate data is classified as normal:
a. [1 1 1] for super critical
b. [0 1 1] for critical
c. [0 0 0] for normal

4. All records classified as the super critical and critical patient information are propagated to the server individually with higher priority for delivery.

5. All normal records are aggregated together and propagated from the BTS to cloud based healthcare network in the aggregated form.
a. The patient information is counted for the normal patients.
b. The normal patient data is aggregated using the patient id and heartbeat information.

6. The aggregated data is forwarded to the cloud based healthcare record management service.

4. Experimental Results and Discussion

This chapter discusses the results generated by the HRMS model based on the algorithms for data generation, data classification, data aggregation and data offloading to cloud explained in the methodology of the HRMS model. The procedure explained in the methodology is used to produce the output from the proposed HRMS model. This experiment is dynamic and network dependent. This experiment is performed with 12, 25 and 50 sensor nodes in a WBAN and the data is offloaded to the cloud for a total of 40 offloading iterations on a cellular and having the network bandwidth of 1Mbps in WiFi network, in which the upload data channel is available at 1/8 Mbps at moderate hours.

During the peak hours, the bandwidth availability may vary due to the traffic coming from the higher density of the users. The number of normal, critical and super-critical patients in the network changes with each offloading iteration. The results are compared in terms of three parameters aggregation efficiency, total transmission time and end-to-end delay. The results are also compared in terms of the communicational network i.e. cellular or Wi-Fi both at moderate and peak hour Figure 6 (a) represents the total transmission time analysis of the HRMS model on a 2G Network at moderate hours, (b) Aggregation Efficiency of HRMS model on Wi-Fi Network at moderate hours.

![Figure 6](image-url)

Figure 6. (a) Total Transmission Time Analysis on 2G Network at moderate hours, (b) Aggregation Efficiency of HRMS model on Wi-Fi Network at moderate hours.
5. Conclusion

The wireless healthcare systems are becoming more and more important useful in day to day life and so, for this reason, there is a need to develop the secure system for patients and doctors which has privacy of data. In this, we have discussed and implemented secure healthcare system in which encryption based schemes are used for the privacy of data by which readable data becomes unreadable for unauthorized users. It also improves the factors like QOS, bandwidth, efficient, etc. this system uses the secure key exchange system for data privacy of healthcare systems. This developed system will help both patients and doctors to treat the disease as soon as possible as in this health report of patients goes to doctors with the help of the wireless sensor. These are wearable body sensors, which are wearied by patients, and these sensors send reports to doctors. This system develops secure healthcare system for data privacy of users.

6. References