INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.ljariit.com

Optimized Healthcare Data Management and Critical Handling Using Smart Data Categorization Method

Divisha Poonia
ECE Department, CEC Landran
Mohali

Satvir Bajwa
ECE Department, CEC Landran
Mohali

ABSTRACT—the cloud based healthcare models are coming to the emergence very quickly and growing their roots across the globe for the empowering of the active healthcare services. The wearable body sensors are utilized to track the health of the patient when they are out of the healthcare premises. Also the telemedicine and remote healthcare monitoring applications has empowered the healthcare systems to grow their roots into the remote areas of the countries, where it becomes the very tough task to provide the healthcare services or setup the hospitals, dispensaries, etc. The telemedicine practices empower the doctors to remotely monitor the health of the patients and prescribe the best medicines or the precautionary practices. But such healthcare applications suffers from the many performance based issues such as critical data handling, slow data delivery, etc. The healthcare specific network data classification and flow prioritization methods can be utilized to mitigate the healthcare network problems by decongesting the healthcare networks from the heavy loads by smartly optimizing the data outcome on the dominating controller nodes to optimize the healthcare data inflow volumes. The proposed model is expected to solve the problems associated with the existing systems designed for healthcare data management.

Keywords— Data management, Data categorization, Quality of Service, Healthcare monitoring.

I. INTRODUCTION

The proposed model is Cloud based Healthcare Models (CHM) model that can efficiently offload the ECG data of the patient to the cloud. It is the outcome of distant health monitoring with the usage of WBANs and cloud computing. eHealthCare is provided by CHM model that is composed of a single WBAN with many sensor nodes. Each sensor node is attached to a single patient. It monitors the patient and collects the ECG data. The data is processed by the smart health applications on the smart mobile devices of the patients. The processed data is transmitted on the network. The BTS receives the data and performs the data classification and the aggregation of the patient data. The data is thus offloaded to the cloud. The data on the cloud is easily accessible by the medical fraternity thus providing real-time feedback from the doctor.CHM model consists of four basic modules namely *Sensor Nodes, Aggregator Node, Real-Time Cloud and the end user i.e. Medical fraternity*. Fig.4. explains the basic modules of CHM model. Sensor nodes collect the data from the patient and communicate it to the smart mobile device of the patient where the data is processed by the smart health application. The mobile device transmits the data onto the network and the data reaches the aggregator node (BTS). It performs the aggregation of the patient data and offloads the data to the cloud.

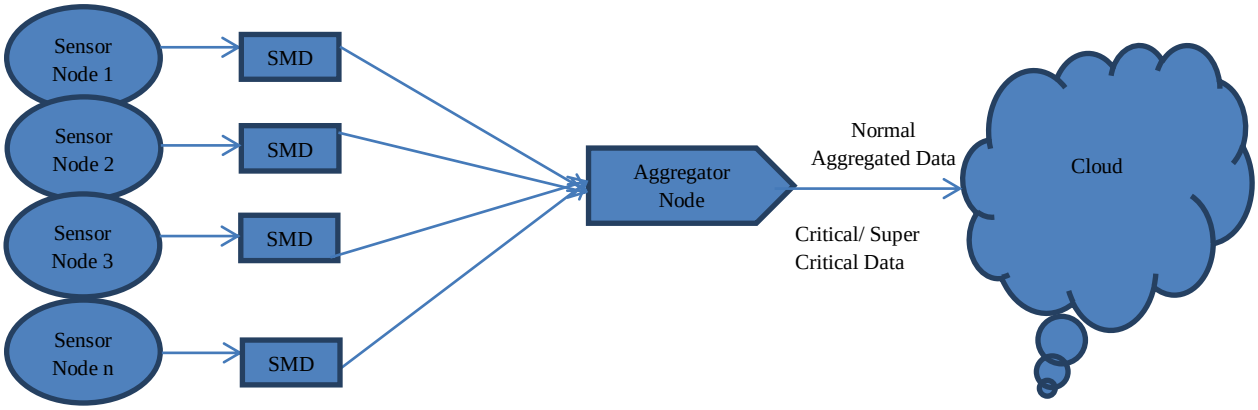

Fig.1 depicts the cloud based healthcare model

Sensor nodes are the building blocks of a WBAN that are miniature nodes either implanted on the patient body or are wearable. Sensor nodes are low power nodes that collectively form a WBAN and are used to collect information from the patient's body. They are wearable on shirt, wrist watches or belts of the patients. They collect the various physiological parameters of the patients such as ECG rate, Body Temperature, Blood Pressure etc. Sensor nodes are either connected to the communication network directly or are connected to the smart mobile device of the patient. CHM model connects the sensor nodes to the smart mobile device via communication technology such as Bluetooth or Wi-Fi. The smart mobile device processes the collected data from the patient body with the help of a smart mobile application that calculates the desired physiological parameters. Many smart mobile devices such as Samsung Galaxy Series, Nokia Lumia Series, Apple iOS Series, Blackberry Phones, etc. support such healthcare applications. There are many smart health applications that are useful in calculating the various biological parameters. For this experiment, we are choosing ECG as the physiological parameter. 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 from the smart mobile device is thus transmitted onto the network in the communication channel.

CHM model uses real-time cloud for data storage and processing of the patient data. The cloud having better resources such as storage, memory and processing power; is used for storing and accessing information. The data from the BTS is offloaded to the cloud and the healthcare database is maintained on the cloud. It records the patient data, physiological parameters to be measured, patient profile and patient history. Cloud provides efficient data accessing and processing. The patient data is also secured on the cloud. Real-time cloud is used for offloading the patient data from the BTS to the cloud. It enhances the proposed model as it provides distributed, reliable and flexible access to the data. Real-time cloud also provides real-time health services management system.

The fourth component of the CHM model is the end user of the data on the cloud. The end user is the medical staff of a hospital that has access to the cloud and can process the patient data. The medical fraternity can access the patient data, profile and history from the cloud and can provide the desired alarms or notifications to the patient. This provides real-time feedback from the doctor. The medical fraternity can raise alarms for the patients or inform the family in case of emergency to avoid any serious consequences. The data stored on the cloud can also be used for future references.

II. LITERATURE REVIEW

Xiang, Chaocan et. al. [1] has worked on the QoS-based service selection with lightweight description for large-scale service-oriented IoTs. The authors have addressed these challenges with the following three basic ideas. Firstly, the authors have presented the lightweight description method to describe the QoS, dramatically decreasing the time complexity of service selection. Moreover, based on this QoS description, they have decomposed the complex problem of QoS-based service selection into a simple and basic sub-problem. Finally, based on this problem decomposition, they have also presented the QoS-based service matching algorithm, which greatly improves selection accuracy by considering the whole meaning of the predicates. Kumar, Adarsh ET. al. [8] has worked upon simulation and analysis of authentication protocols for mobile Internet of Things (MIoT). This work proposes a single bar circular topology based authentication protocol for MIoT. This protocol helps in authenticating the mobile devices for constructing secure network. The proposed protocol is modeled using Alloy model. Delay analysis shows that construction of secure network is possible with maximum delay of 0.91 msec. Node can enter or leave the network with minimum of 0.13

and maximum of 0.20 msec. Further, Zone Routing Protocol (ZRP) is considered to be the best protocol for constructing a secure network. Lee, Jun-Ya et. al. [2] has proposed a lightweight authentication protocol for internet of things. In this paper, the authors have proposed an encryption method based on XOR manipulation, instead of complex encryption such as using the hash function, for anti-counterfeiting and privacy protection. The enhancement of the security is described and hardware design methodology is also demonstrated. Abomhara, Mohamed et. al. [3] has given the study on security and privacy in the Internet of Things: Current status and open issues. As IoT systems will be ubiquitous and pervasive, a number of security and privacy issues will arise. Credible, economical, efficient and effective security and privacy for IoT are required to ensure exact and accurate confidentiality, integrity, authentication, and access control, among others. In this paper, the IoT vision, existing security threats, and open challenges in the domain of IoT are discussed. The current state of research on IoT security requirements is discussed and future research directions with respect to IoT security and privacy are presented. Ali, Syed Taha et. al. [4] has worked on the authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. In this paper, the authors have proposed a lightweight robust authentication scheme. They have analyzed and validate a practical approach for their research to develop the authentication scheme. The authors have aimed their research for healthcare monitoring systems. The proposed scheme has been lower on cost and loss-resilient. The new scheme has been proved to effective on almost 99% of data and it has added as low as 5% overhead. Khan, Farrukh Aslam et. al. [5] has proposed a cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. The authors have presented a secure cloud-based mobile healthcare framework using WBANs. The authors have developed a multi-biometric based key generation scheme for WBANs. They have also worked upon electronic medical records (EMRs) and secured them using the authentication scheme based on the key sharing process. The evaluation and analysis shows that the proposed multi-biometric based mechanism provides significant security measures due to its highly efficient key generation mechanism. Xiangdong Peng et. al. [6] has proposed an ECG compressed sensing method of low power body area network. Aimed at low power problem in body area network, an ECG compressed sensing method of low power body area network based on the compressed sensing theory was proposed. Random binary matrices were used as the sensing matrix to measure ECG signals on the sensor nodes. After measured value is transmitted to remote monitoring center, ECG signal sparse representation under the discrete cosine transform and block sparse Bayesian learning reconstruction algorithm is used to reconstruct the ECG signals. The simulation results show that the 30% of overall signal can get reconstruction signal which's SNR is more than 60dB, each numbers in each rank of sensing matrix can be controlled below 5, which reduces the power of sensor node sampling, calculation and transmission. The method has the advantages of low power, high accuracy of signal reconstruction and easy to hardware implementation.

III. FINDINGS OF THE LITEARTURE REVIEW

The literature survey in the previous chapter infers that the recent research in the field of ubiquitous mobile healthcare delivers health monitoring systems monitoring many vital biological parameters such as blood pressure, body temperature, pulse rate, heartbeat, ECG, EEG, respiration rate etc. These systems integrate technologies such as WBANs, CC, MCC and Data Offloading. In the present scenario, health monitoring systems consist of WBANs that are efficient in terms of patient data collection performed by the sensor nodes. The data collected is thus transmitted onto the communicational network consisting of routers and gateways. As there exists many WBANs, enough data is generated which must be managed to fully utilize the resources of the network. This is done by offloading the patient data to the cloud where the data is saved for easy accessing and retrieval. But for every patient; data is offloaded to the cloud thus increasing the number of packets on the network and overhead of acknowledgements and header. Data aggregation is performed to control the network congestion and the aggregated data is thus offloaded to the cloud. The following sections give details of the research gaps in the present scenario and the proposed algorithm.

IV. METHODOLOGY

Aggregation decision made by the BTS depends upon the data classification. Normal data also referred to as non-urgent data is aggregated as it does not require quick response from the doctor so it can be offloaded with a minimum delay. Normal data is aggregated before offloading the data to the cloud. HRMS model allows the BTS to club the normal data into a single packet. Whereas critical or super critical data, also referred to as urgent data requires quick attention of the medical staff to avoid any dire consequences. So the urgent data must be offloaded as soon as it is received without a minimum queuing delay. The proposed HRMS model presents two scenarios for offloading patient data to the cloud. Two scenarios depend upon the critical nature of the patient data. Scenario 1 represents the normal data which do not require urgent attention of the doctor. Data of various normal patients from the BTS is aggregated into a single packet. This single packet is then offloaded to

the cloud thus decreasing the network traffic by reducing number of packets on the communication links and overhead of packet headers and acknowledgements. Fig3 illustrates scenario 1 of normal data which is aggregated and then offloaded to the cloud via BTS. The data received from the three sensor nodes is aggregated by the BTS and then sent to the cloud in a single packet.

V. CONCLUSION

The proposed model has been designed by aiming at the decongestion of the network resources usability under the healthcare applications. The smart healthcare data management applications are specifically designed for the purpose of active data classification and optimization to avoid the congestion over the networks. The healthcare applications survive major failures sometimes and left with the minimized service levels, which must be mastered for the delivery of the critical data towards the centralized healthcare data storage services in order to value the human life under risk. In this paper, the healthcare applications are being optimized and specialized for the handling of the critical situations. The proposed model has been equipped with the data inflow optimization and gradation over the flow controller nodes which can categorize the data into the primary categories of the normal data and healthcare data, where the healthcare data undergoes the further classification, which includes the critical or normal graded data. The normal and critical data is handled individually and the critical is prioritized higher than the normal data. Also the specific channel mechanism can be incorporated for the delivery of the critical healthcare data.

REFERENCES

[1] Xiang, Chaocan, Panlong Yang, Xuangou Wu, Hong He, and Shucheng Xiao. "QoS-based service selection with lightweight description for large-scale service-oriented internet of things." *Tsinghua Science and Technology* 20, no. 4 (2015): 336-347.

[2] Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang. "A lightweight authentication protocol for internet of things." In *Next-Generation Electronics (ISNE), 2014 International Symposium on*, pp. 1-2. IEEE, 2014.

[3] Abomhara, Mohamed, and Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues." In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, pp. 1-8. IEEE, 2014.

[4] Ali, S. T., Sivaraman, V., & Ostry, D. (2014). Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. Future Generation Computer Systems, 35, 80-90.

[5] Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks. Procedia Computer Science, 34, 511-517

[6] Peng, X., Zhang, H., & Liu, J. (2014). An ECG Compressed Sensing Method of Low Power Body Area Network. TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(1), 292-303.

[7] Hernandez-Ramos, Jose L., Marcin Piotr Pawlowski, Antonio J. Jara, Antonio F. Skarmeta, and Latif Ladid. "Toward a Lightweight Authentication and Authorization Framework for Smart Objects." *Selected Areas in Communications, IEEE Journal on* 33, no. 4 (2015): 690-702.

[8] Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal. "Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT)." In *Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on*, pp. 423-428. IEEE, 2014.

