SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 185–189

ISSN No: 2454-9614

Using Medical Big-Data Platforms to Creating Stochastic Preference for Adaptive Crowd sourcing

L. Poornima Devi, N. Sathyabalaji*

[a] *Department Of Computer Science and Engineering, J. K .K. Munirajah College of Technology, T.N.Palayam, Erode, Tamilnadu, India.*

*Corresponding Author: Poornima Devi. L

E-mail: poorni12june93@gmail.com

Received: 19/11/2015, Revised: 17/12/2015 and Accepted: 12/03/2016

Abstract

This project proposes to store a massive value of data in medical platform. In this medical storage system uses 60GHz wireless technologies for in hospital wireless network access. Crowd sourcing used for big data platforms, in which data are gathered by user participation. The data's stored on a centralized server via access point. The technology, which are used to process the data parallel on different CPU node. These technologies provide storage for billions and trillions of unstructured data. While sending input data to centralized server via wireless medium, the power allocation method make decision to allow the data to server and perform schedule operation when data's from multiple CPU node. In this project it store vast amount of unstructured data which are stored on centralized server and the stored data be accessed secure with high availability.

Keywords: 60GHz, crowd sourcing, centralized server.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

In recent years, the volume of medical data generated by large hospitals is becoming increasingly large due to technological advancements in medical devices, including high-resolution magnetic resonance imaging (MRI), motion MRI, ultrasound, and digital microscopy **[1].** Furthermore, centralized storage of medical records is a common practice for sharing medical data among medical practitioners, as illustrated in Fig. 1. Oftentimes, medical records are collected and uploaded to the centralized medical record using modern mobile equipments, such as smart phones, and via wireless access points (APs). Because of the sensitive nature of medical data, data aggregation, as shown in Fig. 1, needs to be privacy preserving. Therefore, interconnecting medical storage platforms with external networks (such as the Internet) is not recommended. Medical data in the proposed medical storage platform is often gathered and organized by fixed users—e.g., purposed medical tablets, smartphones, computed tomography scanners, etc.—with the principle of crowdsourcing. In this proposed medical storage system, we consider using 60-

GHz wireless technologies for in-hospital wireless network access. The choice of wireless technologies has been widely advocated and accepted in the literature because of high data rates achieved by ultra wide bandwidth. One of the many interesting design problems that need to be addressed to construct the centralized privacy preserving data storage system shown in Fig.1.

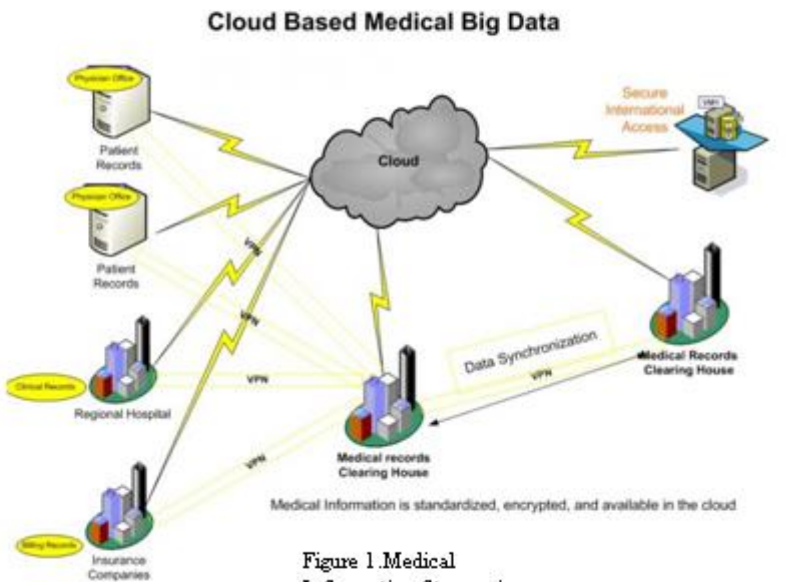

Figure 1.Medical Information Storage in Centralized server

2. Defining Big Data.

Big data typically refers to the following types of data:

1. Traditional enterprise data – includes customer information from CRM systems, transactional ERP data, web store transactions, and general ledger data.
2. Machine-generated /sensor data – includes Call Detail Records ("CDR"), weblogs, smart meters, manufacturing sensors, equipment logs (often referred to as digital exhaust), and trading systems data.
3. Social data – includes customer feedback streams, micro-blogging sites like Twitter, social media platforms like Facebook .
4. In fact, there are three key characteristics that define big data:
5. Volume is the amount of data generated by organizations or individuals. Enterprises in all industries are looking for ways to handle the ever increasing data volume that's being created every day.
6. Velocity is the frequency and speed at which data is generated, captured and shared. Consumers as well as businesses now generate more data and in much shorter cycles, from hours, minutes, seconds down to milliseconds.

7. Variety is the proliferation of new data types including those from social, machine and mobile sources. New types include content, location or geo-spatial, hardware data points, log data, machine data, metrics, mobile, physical data points, process, radio frequency identification (RFID), search, sentiment, streaming data, social, text and web. Also, variety includes traditional unstructured clinical data (i.e., free text).

3. Big Data in Health Care

The types of data anticipated to be of use in BDA include:

1. Clinical data – up to 80 per cent of health data is unstructured as documents, images, clinical or prescribed notes;
2. Publications – clinical research and medical reference material;
3. Clinical references – text-based practice guidelines and health product (e.g., drug information) data;
4. Genomic data – represents significant amounts of new gene sequencing data;
5. Streamed data – home monitoring, tele health, Hand held and sensor-based wireless or smart devices are new data sources and types;
6. Web and social networking data – consumer use of Internet – data from search engines and social networking sites; and
7. Business, organizational and external data – administrative data such as billing and scheduling and other non-health data.

BDA can mine volumes of medical literature and other unstructured data and integrate these results with the increasing volumes of discrete data captured in EHRs, EMRs and PHRs. BDA can combine content analysis, evidence-based data and through natural language processing technology can understand, learn and then

Predict future events. These analytics are then fed back to clinicians as considerations in their decision making. Patients or consumers also use BDA to get answers for their own conditions. Data could be presented back in a meaningful way and encourage patient participation in their health care plans and potentially reduce re-admissions or adverse outcomes.

4. Big Data Challenges in Health Care

1. Leveraging the patient/data correlations in longitudinal records.
2. Understanding unstructured clinical notes in the right context.
3. Efficiently handling large volumes of medical imaging data and extracting potentially useful information and biomarkers.
4. Analyzing genomic data is a computationally intensive task and combining with standard clinical data adds additional layers of complexity.
5. Capturing the patient's behavioral data through several sensors; their various social interactions and

communications.

5. Security Issues

In cloud-based HIS, security should be the top priority from day one. Patients' data should be protected with comprehensive physical security, data encryption, user authentication, and application security as well as the latest standard-setting security practices and certifications, and secure point-to-point data replication for data backup. These security issues have been extensively investigated for cloud computing in general. A major challenge to healthcare cloud is the security threats including tampering or leakage of sensitive patient's data on the cloud, loss of privacy of patient's information, and the unauthorized use of this information.Hence, a number of security requirements should be satisfied by healthcare cloud computing systems. The main security and privacy requirements for healthcare clouds are discussed below[3,4]:

1. Authentication: in a healthcare cloud, both healthcare information offered by CSPs and identities of users (HPs, practitioners, and patients) should be verified at the entry of every access using user names and passwords assigned to users by CSPs.
2. Authorization: is an essential security requirement that is used to control access priorities, permissions and resource ownerships of the users on the cloud. Each cloud user is granted privileges based on his account. Patient can allow or deny sharing their information with other healthcare practitioners or CDOs. To implement patient consent in a healthcare system, patient may grant rights to users on the basis of a role or attributes held by the respective user.
3. Non-repudiation: implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. In a healthcare system,technologies such as digital signatures, timestamps, confirmation receipt, and encryption can be used to establish authenticity and non-repudiation for patients, CDOs, and practitioners.
4. Integrity and Confidentiality: integrity means preserving the accuracy and consistency of data. In the healthcare system, it refers to the fact that EHRs have not been tampered by unauthorized use. Confidentiality is defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access". Confidentiality and integrity can be achieved by access control and encryption techniques in EHR systems.
5. Availability: For any EHR system to serve its purpose, the information must be available when it is needed. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) attacks.

6. Example of Healthcare's Transition to Big Data

In conclusion, here is a brief example of how the transition from relational databases to big data is happening in the real world. We, at Health Catalyst, are working with one of our large health system clients and Microsoft to create a massively parallel data warehouse in a Microsoft APS Appliance that also includes a Horton works Hadoop Cluster. This means we can run a traditional relational database and a big data cluster in parallel. We can query both data stores simultaneously, which significantly improves our data processing power. Together, we are beginning to experiment with big data in important ways, such as performing natural language processing (NLP) with physician notes, predictive analytics, and other use cases.The progression from today's symmetric multiprocessing (SMP) relational databases to massively parallel processing (MPP) databases to big data in healthcare is underway.

7. Conclusions and Future-work

This paper proposes a framework for secure Health Information Systems (HISs) based on big data analytics in mobile cloud computing environment. The framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients and practitioners. The cloud permits a fast Internet access, sharing, and provision of EHRs by authenticated users. Big data analytics helps analyze patient data to provide right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. The ultimate goal of the proposed framework is to introduce a new generation of HISs that are able to provide healthcare services of high quality and low cost to the patients using this combination of big data analytics, cloud computing and mobile computing technologies. In the future we plan to design and implement HIS based on the proposed framework.

Reference

[1] Rasid Z[Cited Mar 17, 2014]. Available from: http://www.asigra.com/blog/bigdata-infographic-what-big-data.
[2] Dembosky A: "Data Prescription for Better Healthcare." Financial Times, December 12, 2012.
[3] R. Zhang L. Liu, "Security Model &Requirements for Healthcare Application Clouds", IEEE 3rd International Conf on Cloud Compt, 2010.
[4] A. Youssef and M. Alageel, "Security Issues in Cloud Computing", the GSTF International Journal on Computing , Vol.1 No. 3, 2011.
[5] Ahmed E. Youssef and Manal Alageel, "A Framework for Secure Cloud Computing", International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 4, No 3, pp. 478-500, July 2012.
[6] J. Kim, Y. Tian, S. Mangold, and A. F. Molisch, "Joint scalable coding and routing for 60 GHz real-time live HD video streaming applications," IEEE Trans. Broadcast., vol. 59, no. 3, pp. 500–512, Sep. 2013.
[7] G. Chatzimilioudis, A. Konstantinidis, C. Laoudias, and D. Zeinalipour-Yazti, "Crowd sourcing with smart phones," IEEE Internet Comput., vol. 16, no. 5, pp. 36–44, Sep./Oct. 2012.
[8] J. Kim, Y. Tian, S. Mangold, and A. F. Molisch, "Quality-aware coding and relaying for 60 GHz real-time wireless video broadcasting," in Proc. IEEE Int. Conf. Commun. (ICC), Budapest, Hungary, 2013, pp. 5148–5152.
[9] M. Allahbakhsh et al., "Quality control in crowdsourcing systems:," IEEE Internet Comput., vol. 17, no. 2, pp. 76–81,Mar./Apr. 2013.
[10] A. Youssef and M. Alageel, "Security Issues in Cloud Computing", the GSTF International Journal on Computing , Vol.1 No. 3, 2011.
[11] R. Buyya, J. Broberg, and A. Goscinski, "Cloud Computing Principles and Paradigms", John Wiley & Sons, 2011.
[12] Feldman B, Martin EM, Skotnes T:"Big Data in Healthcare Hype and Hope." October 2012. Dr. Bonnie.
[13] P. Smulders, "Exploiting the 60 GHz band for local wireless multimedia access: Prospects and future directions," IEEE Commun. Mag., vol. 40,no. 1, pp. 140–147, Jan. 2002.
[14] J. Sun and C. K. Reddy, "Big Data Analytics for Healthcare" Tutorial presentation at the SIAM International Conference on Data Mining, Austin, TX, 2013.