Plugging the Health Needs of Users by Creating an E-Hospital Environment.

Aleena Wahid\textsuperscript{1}, Anice John\textsuperscript{2}, Athira S\textsuperscript{3}, Prabha M R\textsuperscript{4}, Sivendu B S\textsuperscript{5}, Jooby E\textsuperscript{6} & Deepa K Daniel\textsuperscript{7}.
\textsuperscript{1,2,3,4,5}UG Scholar, College of engineering Perumon, Kerala, India. 
\textsuperscript{6}Assistant Professor in CS, College of engineering Perumon, Kerala, India. 
\textsuperscript{7}Assistant Professor in IT, College of engineering Perumon, Kerala, India.

Abstract: Information technology transforms the ways of healthcare services by converting the olden method of consulting a doctor to patients seeking online health information. Many healthcare services has been brought into action. These include Heath Tap, HaoDF, WebMD etc. They provide faster and trusted answers for the questions asked by the patients. This paper consists of two components: mining and learning. A personal health record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast to the more widely used electronic medical record, which is operated by institutions (such as hospitals) and contains data entered by clinicians or billing data to support insurance claims. The intention of a PHR is to provide a complete and accurate summary of an individual’s medical history which is accessible online.

1. Introduction

PHR is a tool that can be used to collect, track and share past and current information about a person’s health. Sometimes this information can save money and inconvenience of repeating routine medical tests. Even when routine procedures do need to be repeated, a PHR can give medical care providers more insight into personal health story. PHR has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centres, many PHR services are outsourced to or provided by third-party service providers. The term “personal health record” is not new. The earliest mention of the term was in an article indexed by Pub Med dated June 1978. However, most scientific articles written about PHRs have been published since 2000. It is important to note that PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR.

This paper consists of five different levels of users—Search users, Patients, Doctors, Hospital and Agents representing a particular hospital. Search users can search for their queries in their own narrative language for which the medical experts provide answers. The creation of Personal Health Record of a person is done by a registered hospital. For access security a username and password is given to the patient (PHR owner). The details in PHR are entered by the doctor whom the patient consults. These details include allergies and adverse drug reactions, chronic diseases, illnesses and hospitalizations, prescription record, surgeries and other procedures, vaccinations etc. Doctors are the core part that provides expert advice and clarifies the doubts of patients as well as search users. Doctors can access a patient’s PHR
with their permission and thus securing their system. Agents help in handling the emergency situation. They can search for the details of any registered patients for the corresponding hospital. These details are protected from any kind of attack by providing security with the help of hardware tokens. The health seekers can create their PHRs by the registration process available in the corresponding hospital. These details can be made available to the doctors for further consultations.

The patients and search users ask their queries in their own narrative language. Sometimes the answers provided by the specialists may contain medical terms which might be unknown to the users. This may create confusions and incomplete clarification of doubts. In order to bridge this vocabulary gap we use the following two techniques - local mining and global learning. Mining aims to locally code the medical records by extracting the medical concepts from individual record and then mapping them to terminologies based on the external authenticated vocabularies. Global learning collaboratively learns missing key concepts and propagates precise terminologies among underlying connected records over a large collection.

2. Related Works

SAPPHIRE (Semantic and Probabilistic Heuristic Information Retrieval Environment) was introduced by Hersh and David in 1995 which used simple lexical approach which automatically assigned UMLS terminologies to medical documents [9]. This was used as an optimal approach to overcome problems of indexing, retrieval, and evaluation of IR resources in the biomedical domain. SAPPHIRE too provided solutions to many problems but it has unrevealed many new facts. The disadvantages of system are less benefits of concept mapping, Substitution of synonyms. Later in 2007 K. Crammer, M. Dredze, S. Carroll, K. Ganchev, P. Talukdar brought a new technique of coding large amount of health records which should be maintained in modern hospitals [11]. This method has proved to be helpful in data mining, information extraction, relation extraction etc. This approach was performed by initially explaining the task and difficulties finally evaluate the system based on human performance and the best score is preferred. One of the systems is ICD-9-CM (International classification of Diseases, Ninth Revision, Clinical Modification) and is used for classification of a symptom, disease, procedure, injury or information from the health records. The codes are organized hierarchically where the top level represents general information such as respiratory diseases and bottom level represents specific information such as brain tumour. In the rule-based system uses a short description of ICD-9-CM codes and their types. Each description is considered as a group of words. If all the words in a code description is found in a sentence, a flag is set corresponding to that code. If the code is a disease consider it as a negation and the flag is removed. As a whole this system reduced the costs, work of coders and even standardized the hospital data collection but it left behind many shortcomings since it cannot be tested when there are limited number of codes and the hierarchy is removed. Also the number of codes in each document has wider range varying between 1 and 15 codes. In the same year 2007, Dozier, R. Kondadadi, K. Al-Kofahi, M. Chaudhary, and X. The main aim was to provide a Question-Answer scheme to meet the objective of the users [7]. It uses NLP (Natural Language Processing) to process the questions posed by the users and thereby the proper meaning can be revealed. Medical terms are collected and grouped so that checking with the synonyms of keywords could result in normalization. The retrieval of medical records using a query is challenging but using medical search for relevant documents are very specific which may sometime leads to granularity mismatch [4]. To overcome this, a symbolic reasoning called subsumption (or ‘is-a’) relationship between parent and child is used to tackle granularity mismatch [12]. Here parent-child relationship is defined as one concept is a subset of other concept’ so it is important to add subsumed concepts in the retrieval function. Simply, free-text documents to concepts defined in medical terminologies (SNOMED CT) ontology has taken place.

In 2011, G. Leroy and H. Chen brought a new tool named Medical Concept Mapper which enabled people to search their personal queries by providing
appropriate medical terms [3]. This system helped the common people who had inadequate medical knowledge and also the medical experts to acknowledge outside their expertise field. The construction of this system is challenging. Instead of converting the corpus data to terminology, users are provided with medical terminology for their queries.

Personal health record (PHR) is an emerging patient-centric model of health information exchange. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In this paper, a novel patient-centric framework and a suite of mechanisms is proposed for data access control to PHRs stored in semi trusted servers [13]. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users [14]. The main aim of this research work is to propose a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access [15].

4. Security

4.1 RSA Algorithm

RSA algorithm is used for securing password and patient's details (contents in PHR). RSA is a public key encryption algorithm. RSA involves a public key and a private key.

1. Choose two distinct prime numbers p and q.
   For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2. Compute \( n = pq \).
   \( n \) is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute \( \phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1) \), where \( \phi \) is Euler's totient function.

4. Choose an integer \( e \) such that \( 1 < e < \phi(n) \) and \( \gcd(e, \phi(n)) = 1 \); i.e., \( e \) and \( \phi(n) \) are co-prime.
   \( e \) is released as the public key exponent and having a short bit-length and small Hamming weight results in more efficient encryption – most commonly \( 2^{16} + 1 = \)
65,537. However, much smaller values of $e$ (such as 3) have been shown to be less secure in some settings.

5. Determine $d$ as $d^{-1} \equiv e \pmod{\phi(n)}$, i.e., $d$ is the multiplicative inverse of $e$ (modulo $\phi(n)$). This is more clearly stated as solve for $d$ given $d \cdot e \equiv 1 \pmod{\phi(n)}$. This is often computed using the extended Euclidean algorithm. $d$ is kept as the private key exponent.

Encryption
Alice transmits her public key $(n, e)$ to Bob and keeps the private key secret. Bob then wishes to send message $M$ to Alice. He first turns $M$ into an integer $m$, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext $c$ corresponding to $c \equiv m^e \pmod{n}$. This can be done quickly using the method of exponentiation by squaring. Bob then transmits $c$ to Alice.

Decryption
Alice can recover $m$ from $c$ by using her private key exponent $d$ via computing $m \equiv c^d \pmod{n}$. Given $m$, she can recover the original message $M$ by reversing the padding scheme.

5. Conclusion
This paper provides an efficient way to store and retrieve Personal Health Record. It also helps to handle emergency situation smoothly. Here an agent is introduced who can view and download the PHR if the patient is unable to reveal his/her details to the corresponding hospital. The PHR details are kept secure using security algorithm.

In future the health seekers can have a video chat with the health experts. This work can be introduced to the villages by storing their details and to solve their health problems.

References


