Volume 2, No. 8, August 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

A NETWORK ENGINEERING SOLUTION FOR DATA SHARING ACROSS HEALTHCARE PROVIDERS AND PROTECTS PATIENTS HEALTH DATA PRIVACY USING EHR SYSTEM

Syed Mohsin Saif*[1], Sani Asnain Wani[2], Shabir Ahmad Khan[3], Anitha S Pillai[4], M Maheswran [5]
[1,2,3,4] Department Of Computer Science, Hindustan College Of Arts And Science,Padur, Chennai,Tamil Nadu, India.
[1]Syed.hcas@gmail.com

Abstract: Whenever we talk about networking, Security is the major discipline to be considered emphatically because most of the threats which we come across mediate through various network topologies .Cross-Domain cooperation takes place from time to time in Electric Health Record(EHR) System for necessary and high quality patient treatment and patient record maintenance .To maintain security , integrity ,availability and confidentiality of EHR while sharing the patient data across various clients proper accessibility , right to modify, right to maintain the data and other delegation rights should be assigned properly to the specific person of interest. In this paper we tried to design secured Electric Health Record (EHR) system which will meet or fulfill all above mentioned parameters of delegation and revocation of access rights.

***Keywords*: C**ross Domain, Electronic Health Record, fine gained access, Cryptography**.**

INTRODUCTION

Since the computer or digital media has widen its boundary and over shadowed almost every aspect of life directly or indirectly. In earlier days of Data Management, traditional databases were maintained by pen on paper, huge collection of files with so many data redundancy were the sole way to keep the data repository for future retrieval , to prepare spreadsheets and other design and analysis reports to meet the future challenges of market or corporate establishments. Similarly Hospital databases were maintained and stored on papers with number of overheads like maintainability, sharing, security, integrity, accessibility, modifiability, retrieval etc.

Computerized database management systems have opened up an entire new way of accessing data for both experienced and novice computer users .[1] Data stored in files as a result of traditional data management can be accessed via a traditional ways of data management which is quite time consuming and also takes huge Human resource overheads. The term "database management system" (DBMS) refers to a systemic approach to organizing and managing a large collection of information in a large computer system. [2] The data is structured so as to provide a foundation for future applications development. According to Date, there are many advantages in utilizing traditional databases: i) the amount of redundancy in the stored data can be reduced; ii) problems of inconsistency in the stored data can be avoided (to a certain extent); iii) standards can be enforced; iv) security restrictions can be applied; v) data integrity can be maintained; vi) conflicting requirements can be balanced; and vii) data independence is provided. [3]

The state of the art is that databases for different purposes are not only copies and/or aggregations and/or excerpts of each other, but they also require different kinds of data models. This does not only result in a waste of financial resources, computing equipment and staff needed for their creation and maintenance, but also in time-lags concerning the availability of information needed for decision-making. Moreover, the danger of semantic discrepancies in the data is always immanent. [4] Semantic errors are difficult to detect, and the reasons of errors in reports resulting from such discrepancies are almost impossible to track and to correct, in particular since large amounts of data are usually involved. [4]

The entity-relationship model is the most practicable meta-model suitable for a flexible description of objects and their relationships as occurring in the real world, also being open to future extensions. It does not depend on the structure of particular data aggregation schemes like star schemas which only know hierarchical relationships between entities; it rather enables the user to describe all kinds of attributes and relationships between all types of object and event classes and is thus suitable for a corporate database.[5] The Electronic Health Record (EHR) is the keystone of a medical information system. Acting as an electronic version of paper medical record or chart, the EHR has been touted for years [6] as an essential part of the multifaceted face of medicine in the information system era. This was reflected in a nationwide survey conducted in February 2005 by Harris Interactive of Rochester, N.Y. that found that 70 percent of people were somewhat or very concerned that personal medical information would be leaked because of weak data security. [7]

The HIPAA specifically indicates that patients' privacy should be emphasized, and this belief can be totally applied to the whole health industry throughout the world. [8][9] Among all the barriers to the implementation of EHR systems, privacy and security concerns on patients' medical records are arguably most dominating. Records stored in a central server of a healthcare provider and exchanged over the Internet for cross-organizational sharing are subject to theft [10] and security breaches. A central issue around the sharing of sensitive patient data is the delegation, verification, and revocation of permissions and access rights with respect to an outside healthcare provider. In its original form, delegation of rights is used to appoint a proxy signer who signs on behalf of the delegator in case he or she is absent. In EHR systems, delegation of rights can be used to allow the delegatee's access to shared patient data. More

challenging still, it should also restrict such access to only the portion(s) of data intended for sharing, since illegal disclosure of highly confidential data. In this paper we propose a secure system which meats almost all the above mentioned parameters based on Cryptographic constructions to enable secure patient data flow across the healthcare establishments.

SCOPE OF PROJECT

We propose some new operations for the data security which is the encryption and decryption (cryptographic constructions) technique while sharing the data between the clinics or hospitals and furthermore we do the delegation mechanism in the distributed clients to avoid the abuse of patient data. The delegation mechanism will be applied when the absenteeism of the authenticated person in the authorized clinics or hospitals. And also the fine grained accessibility is adopted so as to ensure the scope of credibility and privacy of patient data.

REVIEW OF LITERATURE

Cross Domain:

A web-specific term that refers to a situation where content comes from different web servers, or where content from one server interacts invisibly with another server that belongs to someone else.

Delegation:

Delegation (or deputation) is the assignment of authority and responsibility to another person (normally from a manager to a subordinate) to carry out specific activities.

Privacy:

Privacy (from Latin *privatus* 'separated from the rest, deprived of something, esp. office, participation in the government', from *privo* 'to deprive') is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively

Fine Grained access control:

It is the restriction of the delegate to the portions of the data. [11]

Electronic Health Record:

An electronic health record (EHR) (also electronic patient record (EPR) or computerized patient record) is an evolving concept defined as a systematic collection of electronic health information about individual patients or populations. It is a record in digital format that is capable of being shared across different health care settings, by being embedded in network-connected enterprise-wide information systems.

NEED OF THE SYSTEM

In Electronic Health Record (EHR), records stored in a central server of a healthcare provider and exchanged over the Internet for cross-organizational Sharing are subjected to theft and other security breaches. The majority of works on EHR systems relevant to handling private patient data still concentrate on the framework design or solution proposals without technical realization. The present system issues many drawbacks which should be removed from the system to make it more secure and reliable with following key features.

We design an EHR system that enables data sharing across collaborating healthcare providers and simultaneously protects patients' health data privacy.

Our delegation procedure is both role-based and proxy signature-based, with the former yielding dynamics in the face of delegatees' status/ availability changes, and the latter providing a secure avenue for basic delegation and revocation

While the basic delegation and revocation should be sufficient for common cases, we design additional mechanisms to satisfy more delicate and stringent control requirements tailored for the EHR system of interest. Specifically, in addition to the basic access control achieved by delegation, fine-grained access control based on searchable public key encryption (PEKS) technique guarantees minimum necessary data access and distributed data storage. On demand revocation based on dynamic accumulators gives rise to revoking any delegatee at any time, with minimal update and maintenance costs incurred at the delegator.

SYSTEM REQUIREMENTS

Hardware Requirements:

PROCESSOR	:	PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
RAM	:	512 MB DD RAM
MONITOR	:	15" COLOR
HARD DISK	:	40 GB
CDDRIVE	:	LG 52X

Software Requirements:

Front End	:	JAVA (SWINGS)
Back End	:	MS SQL 2000/05
Operating System	:	Windows XP/07
IDE	:	Net Beans, Eclipse

EXISTING SYSTEM

Electronic Health Record (EHR) systems are used in place of paper systems to increase physician efficiency, reduce costs (e.g., storage) and medical errors, improve data availability and sharing etc. Records stored in a central server of a healthcare provider and exchanged over the Internet for cross-organizational Sharing are subject to theft and security breaches. The majority of works on EHR systems relevant to handling private patient data still concentrate on the framework design or solution proposals without technical realization

DRAWBACK IN EXISTING SYSTEM

A central issue around the sharing of sensitive patient data is the

A. Delegation of work .
B. Verification of the patient data.
C. Revocation of permissions and

D. Access rights with respect to an outside healthcare provider

PROPOSED SYSTEM

a. We design an EHR system that enables data sharing across collaborating healthcare providers and simultaneously protects patients' health data privacy.
b. Our delegation procedure is both role-based and proxy signature-based, with the former yielding dynamics in the face of delegatees' status/availability changes, and the latter providing a secure avenue for basic delegation and revocation
c. While the basic delegation and revocation should be sufficient for common cases, we design additional mechanisms to satisfy more delicate and stringent control requirements tailored for the EHR system of interest. Specifically, in addition to the basic access control achieved by delegation, fine-grained access control based on searchable public key encryption (PEKS) technique guarantees minimum necessary data access and distributed data storage. On demand revocation based on dynamic accumulators gives rise to revoking any delegatee at any time, with minimal update and maintenance costs incurred at the delegator.

ADVANTAGES IN PROPOSED SYSTEM

The proposed EHR system satisfies the security objectives:
A. Minimum privilege delegation of work.
B. Adaptability with any database.
C. Access control using delegation mechanism.
D. On-demand revocation.

FEASIBILITY STUDY

What is a feasibility study?

The purpose of a feasibility study is to objectively and rationally uncover the strengths and weaknesses of the existing system and proposed venture, opportunities and threats as presented by the environment, the resources required to carry through, and ultimately the prospects for success. With the help of this feasibility we can select best among the proposed alternatives to have the candidate system to meet all the requisite perspectives of future with minimal consumption of cost and time parameters. Moreover to this we can also find out the best possible way to implement the candidate system so as their will be less humiliation to existing human resource from this newly designed system whether the implementation of the newly system .Once the feasibility study is over, on the bases of the said report the final commitment to start the pragmatic implementation of the system commences. The overall feasibity study coves different aspects of feasiblites to calculate the overall feasibility report. Mainly these feasibilities are considered [12];

Technical Feasibility:

The proposed system is developed by using the most popular and secure programming language of present times, the Java .As java is interpreted language can run on any platform. Whether windows 2000 environment windows NT. The hardware and software requirements of the proposed system are readily available for use. Hence is technically feasible.

Operational Feasibility:

The implementation of the proposed system is very easy. The system ensures security be encrypting the data and can be decrypted only by means of public searchable key. All the ongoing processes in the proposed will be warmly anticipated by all sects of human resource with small duration training about the new parameters without any humiliation or hesitation. The introduction of proxy sign-in has tremendously enhanced the operational perspectives of the system.

Financial Feasibility:

As the hardware and software required to meat the objective of the system are readily available in the market at affordable cost. We Well all the previous resources will also be add-on to upgrade the system. The system doesn't require any additional manpower. Hence the system is financially feasible and the Economic Feasibility will be achieved automatically.

SYSTEM DESCRIPTION

Modules:

A. User Interface Design
B. Client 1
C. Encryption of health data
D. Login
E. Public Storage Server
F. Client 2
G. Cross domain delegation
H. Decryption of health data

MODULES DESCRIPTION

User Interface Design:

The User Interface design is done in this module. We use the Swing package available in Java to design the User Interface. Swing is a widget toolkit for Java. It is part of Sun Microsystems' Java Foundation Classes (JFC) — an API for providing a graphical user interface (GUI) for Java programs. [13]

Client 1:

This is hospital A which has two logins one for first doctor and for next doctor , The first doctor (delegator) can access(send and receive) the whole EHR of a patient and he might provide the access responsibilities to the next doctor(delegatee) in case of his absent .the next doctor can access the EHR with on demand revocation this is called Roll based delegation, and this Client1 stores the EHR after the updating of EHR and after finishing treatment and it sends the updated EHR to server in encrypted format.

Encryption of Health Data:

The sender client encrypts the health data with the searchable public key of the receiver client and sends it to the public storage server for storage

Login:

The login module gives the authentication for accessing the public storage server resources with the knowledge of the

Public Storage server and it contains the username, password attributes for checking the authentication of the clients and it checks with the database.

Public Server:

The public server is the authenticator to authenticate the clients (clinics or hospitals) and it is the central storage for patient health record data. it receives the encrypted EHR from the clients and it sends the encrypted data to the client which needs the EHR .

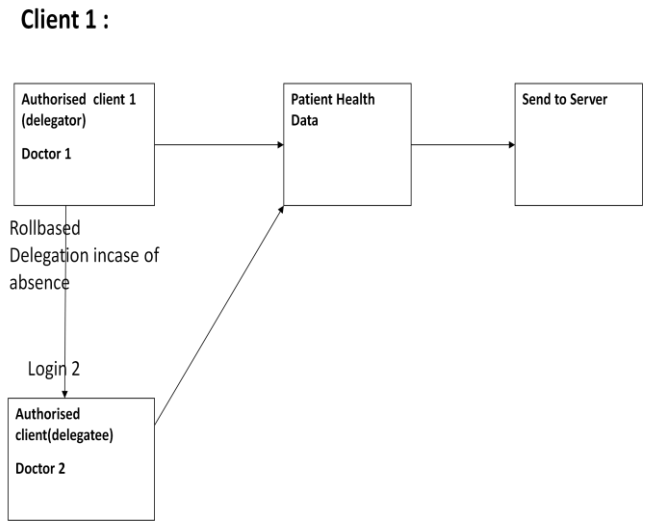


Figure 1.Module Diagram

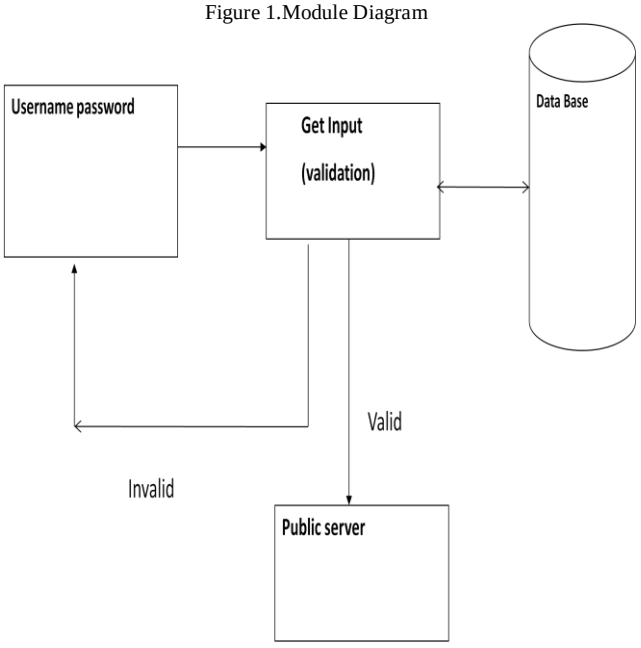


Figure 2.Login

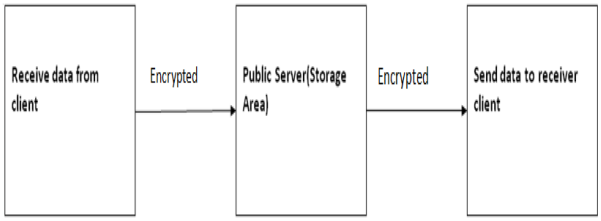


Figure 3.Public Server

Figure 4.Cross Domain Delegation

Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key, and private-key. [14]The cryptographic construction (Encryption and Decryption) technique is used while transferring the data from sender to receiver as searchable public key encryption using keyword search. Delegation mechanism is used for cross domain authentication.

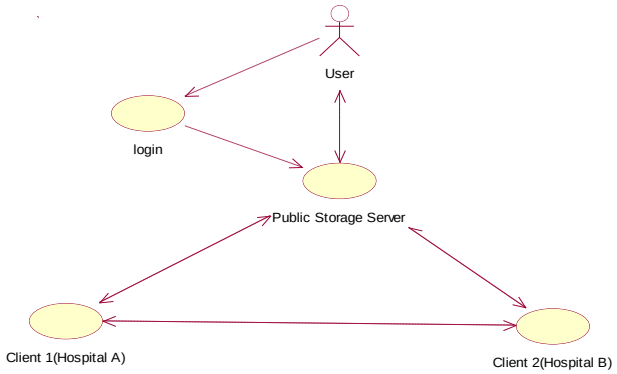


Figure 5.Use case Diagram

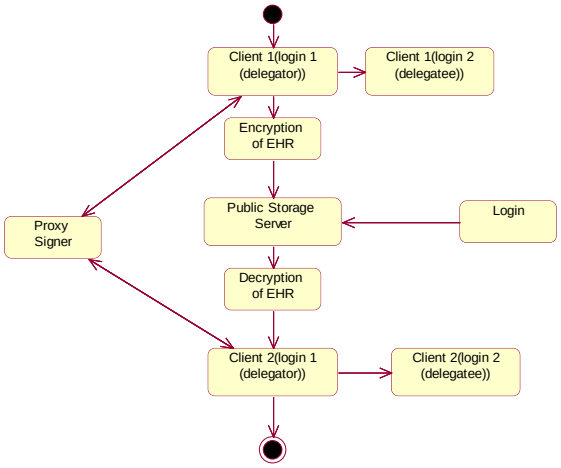


Figure 6. State Diagram

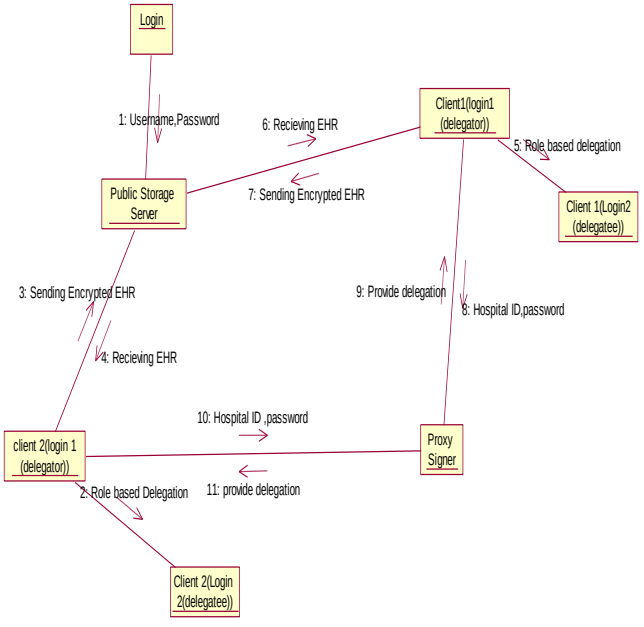


Figure 7. Collaboration Diagram

DATA FLOW DIAGRAM

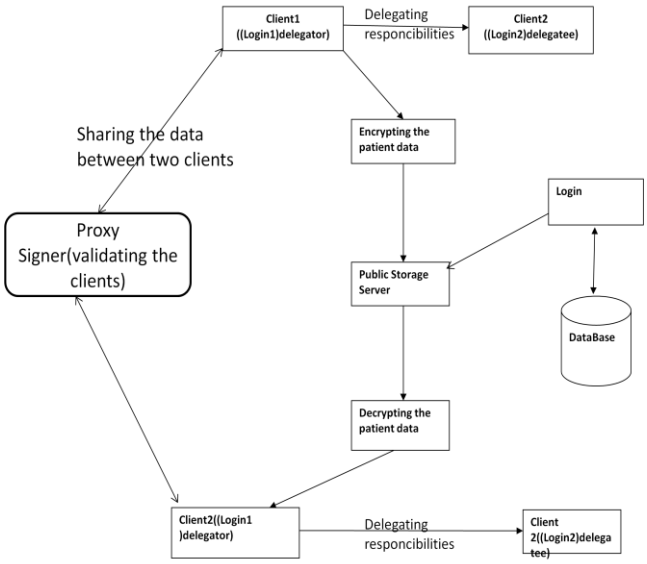


Figure 8. Data Flow Diagram of EHR

SYSTEM DESIGN

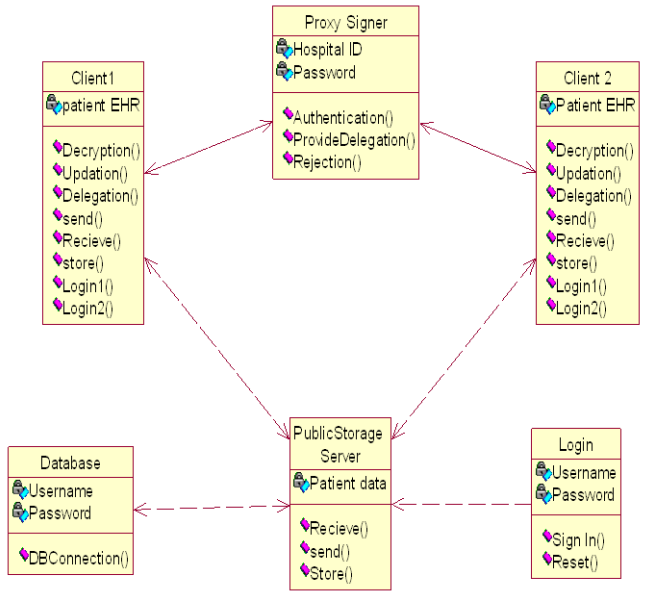


Figure 9.Class Diagram

SYSTEM IMPLEMENTATION

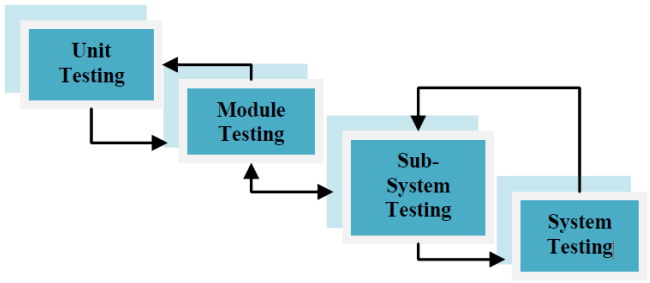
It is the process of construction of the new system and delivery of that into production i.e. day-to-day operation. Implementation is nothing but coding, testing and installing a developed software package on the client end. Implementation consists of three primary activities of training, conversation and post implementation review .Training involves system operators and users who will use the new system either by providing data, retrieving information or actually operating the equipment. Implementation is concerned with the physical creation of the candidate system. User priorities changes in the organizational requirement or environmental factors also call for system enhancement an elaborate test data is prepared and system is tested by using that test data. While testing, errors are noted and corrections are made.

SOFTWARE MAINTENANCE

Maintenance is the modification of a software product after delivery to correct faults, improve performance, or other product attributes, or to adapt the product to a new or changing environment. This topic area provides resources relevant to all aspects of software maintenance.

TESTING PROCESS

It is the process used to help to identify the correctness, completeness, security, and quality of developed computer software. Testing is a process of technical investigation, performed on behalf of stakeholders, that is intended to reveal quality-related information about the product with respect to the context in which it is intended to operate. This includes, but is not limited to, the process of executing a program or application with the intent of finding errors. Quality is not an absolute; it is value to some person. With that in mind, testing can never completely establish the correctness of arbitrary computer software; testing furnishes a criticism or comparison that compares the state and behavior of the product against a specification. An important point is that software testing should be distinguished from the separate discipline of Software Quality Assurance (SQA), which encompasses all business process areas, not just testing.



CONCLUSION

In this project, we designed a secure and functional EHR system to support patient data sharing across cooperative organizations, and at the same time, preserve patient data privacy. The system is demonstrated to satisfy the security and functional objectives characterized by our distributed EHR system featuring cross-domain delegation for sensitive data sharing. Considering the future enhancement for ensuring tightened security we can introduce biometrics as the specific tool to validate and verify the particular user to access the system. [16]

REFERENCE

[1]. Yvonne Marie Abdoo, Ph.D.Converting from Traditional File Structures to Database Managemen Systems: A Powerful Tool for Nursing Management, R.N.Wayne State University College of Nursing,5557 Cass Ave.Detroit, Ml 48202

[2]. Chou, G.T. (1985). dBASE III Handbook. Indianapolis, IN: Que Corporation, p. 2.

[3]. Date, C.J. (1977). An introduction to database systems. Reading, MA: Addison-Wesley, p. 4.

[4]. Von Wolfgang Zinke ,25 January 2011, http://www.b-eye-network.in/articles/ Why is Traditional Database Management Not Optimal for Data Warehouses.

[5]. Bill Inmon: A Tale Of Two Architectures. 2010, Http://Www.Inmoncif.Com/Products/A Tale Of Two Architectures.Pdf

[6]. Institute of Medicine. The computer-based electronic medical record: An essential technology for healthcare. NAP, Washington, DC, 1991(revised 1997).

[7]. Rash, M.C. Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area (Apr. 4, 2005).

[8]. "Health Insurance Portability and Accountability Act of 1996," 104th Congress, Public Law 104–191, 1996.

[9]. "Health Insurance Portability Accountability Act of 1996 (HIPAA)," Centers for Medicare and Medicaid Services (1996) [Online]. Available:http://www.cms.hhs.gov/ hipaageninfo. (retrieved: 05/15/2006).

[10]. Jinyuan sun,et al ,Cross-Domain Data Sharing in Distributed health System, IEEE Transaction on parallel and distributed system,21(10):3;2010

[11]. Jinyuan sun,Yuguang Fang,Cross-Domain Data Sharing in Distributed health system,IEEE Transaction on parallel and distributed system,21(10):1-11;2010.

[12]. Naseeb Singh Gill, Software Engineering.. Khanna Book Publishing Co. (P) Ltd

[13]. Java 2: The Complete Reference ,by Patrick Naughton and herbert Schildt,McGraw-Hill International Edition

[14]. www.barcodesinc.com/articles/cryptograpgy.

[15]. Razeef Mohd et al ,A Web-Engineering Solution To Academic Management System Of An Educational Institute,Journal of global research in Computer Science, 2 (1), January 2011, 20-26.

[16]. Syed. Mohsin Saif et al, Automatic Personal Identification and Verification Using Fingerprints Associated with Multimode Biometrics Approach. International Journal of Advanced Research in Computer Science, 2 (1), Jan-Feb, 2011, 127-133

ABBREVIATION

AHIPAA: THE Health Insurance Portability and Accountability Act.
EHR: Electronic Health Record

