ISSN:2320-0790

An International Journal of Advanced Computer Technology

Securing PHR in Cloud Computing by Using ABE Technique

S. Thivyananth[1]M. Saikumar[2]A. R. Arunachalam[3]
[1,2]UG Student, Department of CSE, Bharath University, Chennai
[3]Asst.Professor, Department of CSE, Bharath University, Chennai

Abstract: Personal Health Records (PHRs) is based on cloud virtual machine in web oriented application in which the lifelong health data of patients are stored. In this paper, we present PHR Machines, a cloud-based PHR system taking a radically new architectural solution to health record portability. In PHR Machines, health-related data and the application software to view and analyze it are separately deployed in the PHR system. After uploading their medical data to PHRMachines, patients will be able to access them again from remote virtual machines that contain the right software to visualize and analyze them without any need for conversion. Patients will be able to share their remote virtual machine session with selected caregivers. The person will need only a Web browser to access the pre-loaded fragments of their lifelong PHR.

Keywords: Cloud computing, electronic health record, personal health record, personalized medicine, radiology

I. Introduction

In a recent review paper, Kaelberet al. define a Personal Health Record (PHR) as —a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it‖. PHRs should be able to be accessed everywhere, that is, it should be kept with the patient and contain lifelong information about the patient. PHRs should not be restricted by file formats or other local issues . In other words, PHRs are electronic health records (EHRs) that are owned by patients. Unlike the hospitals‘Electronic

Medical Records (EMRs), which only contain medical data generated within one specific hospital, PHRs can be accessed by many hospitals. between the EHR and the EHR system. The PHRMachines architecture clearly separates PHR data from the software to work with these data. This paper shows how this creates novel opportunities for the market of PHR software services without compromising patient privacy.

In existing system the EMR Electronic medical record is derived by a process of identification for

II. Design and Implementation Of PHR Machines

A. System architecture

In this paper, we present PHR Machines, a novel PHR system. Leveraging virtualization techniques, PHR Machines allows patients to build lifelong patient health record which is maintained by a caregiver. It allows for an entire patient history to be viewed without a self secure in PHR record. The EMR has no security measures and can be easily viewed by a third party. The EMRs are created and maintained only by a specific hospital and it is not portable. So the EMRs will be valid only within that institution and the patient cannot use the anywhere else.

The project is to make the Personal health record to be maintained by following a process thus the electronic health record maintenance is taken place by various progresses in cloud computing. New techniques are used to secure the medical records in the cloud. Attribute based encryption scheme and its different variations are chosen as the main encryption primitive for the personal health records which makes storage, retrieval and sharing of the medical information more secure and efficient. But in attribute based encryption, the on demand user revocation is a challenging problem. So the cipher text policy –attribute based encryption and key-policy based attribute based encryption are also applied for the security of the personal health record.

PHRs. The records can be shared by the patient with any stakeholder interested in those. PHR Machines allows also the controlled sharing of application software that is required to view and/or analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. Moreover, as technology evolves, patients will always be able to use original software to view and analyze data, even when that software becomes obsolete and possibly no longer supported by the stakeholder that produced the data.

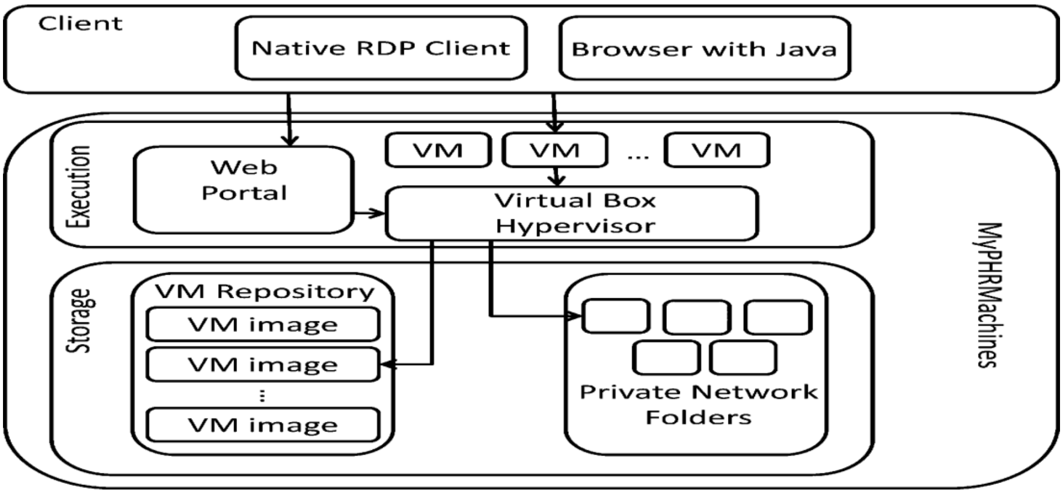


Fig 1.Technical architecture of PHR Machines

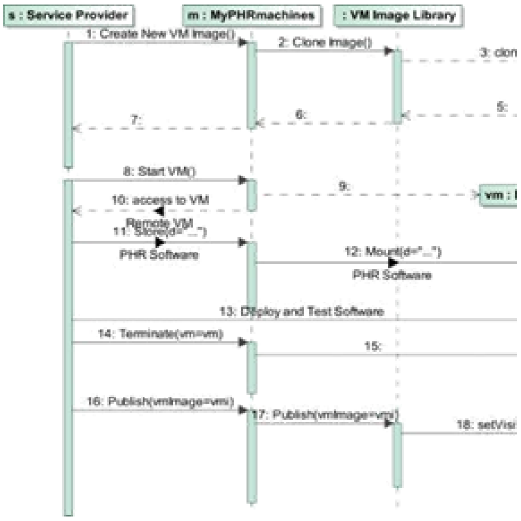


Fig 2. Adding a new software service to PHR machine

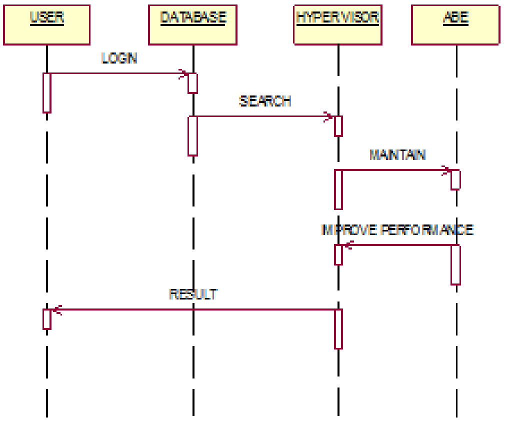


Fig. 3. Sharing a VM session in PHR Machines

The diagram shows the technical architecture of PHR Machines, identifying, besides the components constituting PHR Machines, also the components of the front-end *Client*. The prototype reuses parts of, a mature system for making computational research results more accessible and reproducible. The key technological components have, therefore, undergone various development cycles, which adds to the robustness of PHR Machines technical architecture.

Hyper visor is very important for maintain the cloud database. And also maintain the user request and response. Suppose the user give one request mean hyper visor find out what type of request is that and transfer into correct course. And then transfer the response to the client or user. This all works are maintained by the hyper visor.

A web server is the combination of computer and the program installed on it. Web server interacts with the client through a web browser. It delivers the web pages to the client and to an application by using the web browser and HTTP protocols respectively.

Then define the web server as the package of large number of programs installed on a computer connected to Internet or intranet for downloading the requested files using File Transfer Protocol, serving e-mail and building and publishing web pages. A web server works on a client server model.

Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. Moreover, as technology evolves, patients will always be able to use original software to view and analyze data, even when that software becomes obsolete and possibly no longer supported by the stakeholder that produced the data.

B. Module Description

- User interface

EXISTING SYSTEM	PROPOSED SYSTEM
EXISTING CONCEPT • In existing system we can define the EMR Electronic medical record by deriving a process of identification for patient health record is maintained by caregiver • It allows for an entire patient history to be viewed without a self secure in PHR record.	**PROPOSED CONCEPT:-** • In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. • We leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file..
EXISTING TECHNIQUE Electronic Medical Record (EMR)	**PROPOSED TECHNIQUE** Attribute Based Encryption (ABE)
TECHNIQUEDEFINITION • EMR system has a wide variety of Virtual machines for straightforward extension and derived directly from care givers. • The technical implementation of standpoint, this extension does not represent a substantial obstacle	**TECHNIQUE DEFINITION** • To improve the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. • There has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).

- PHR(Personal Health Record)
- Hyper Visor
- ABE(Attribute Based Encryption)
- Improve the server performance

C. Algorithm Used

Attribute based Encryption

It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of an unique cipher text. A critical security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

InitFirst fix y1 . . . yk, {tk,i} i=1...n,k=1...K ←Zq.
Let y0 = PK

k=1 yk.

System Public Key Y0 = e(g, g)y0 .
Attribute Authority k

Authority Secret Key The SW secret key: yk, tk,1. . . tk,n.

Authority Public Key Tk,ifrom the SW public key:
Tk,1 . . . Tk,nwhere

Tk,i= gtk,i.

Secret Key for User u from authority k Choose random d −1 degree

polynomialp with p(0) = yk. Secret Key: {Dk,i= gp(i)/tk,i} i∈Au.

Encryption for attribute set AC Choose random s ←Zq.
Encryption: E =

Y s

0 m, {Ek,i= T s
k,i} i∈Ak C, ∀k.

Decryption: For each authority k, for dattributes i ∈Ak C ∩ Au, compute

e(Ek,i, Dk,i) = e(g, g)p(i)s. Interpolate to find Y s
k = e(g, g)p(0)s = e(g, g)yks. Combine
these values to obtain QK k=1 Y s
k = Y s0 . Then m = E/Y s0 .

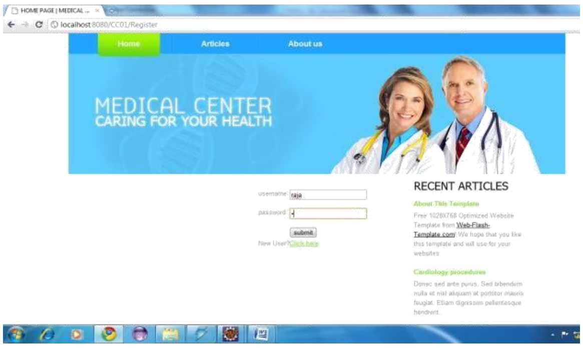
D. Implementation

In ABE access, policies are expressed based on sets of attributes of user inputs, rather than on the unique identity of users. This allows patients to selectively share their PHR data in a secure way to a set of users without the need to know their complete identity and characterization of ABE encryption in the context of PHRs. We consider as for ABE encryption a solution that should complement the current implementation of PHR Machines. In this paper, in fact, we brief about such generic security techniques to enable a deeper discussion of the unique privacy protection mechanisms that are offered by PHR Machines.

Results

Screenshots

Login Page



username: raja

password:

New User?Click here

RECENT ARTICLES

About This Template

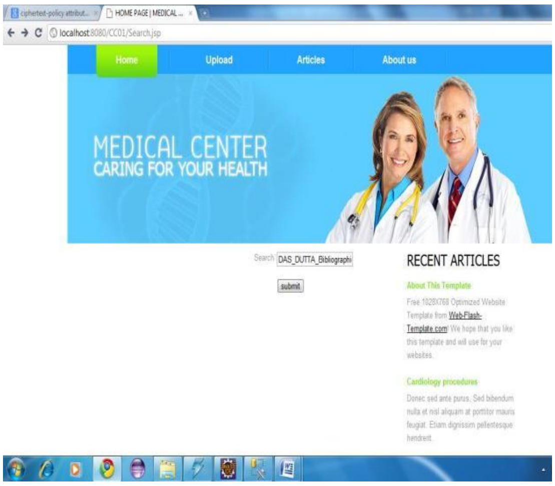
Free 1028X768 Optimized Website Template from Web-Flash-Template.com! We hope that you like this template and will use for your websites

Cardiology procedures

Donec sed ante purus. Sed bibendum nulla et nisl aliquam at porttitor mauris feugiat. Etiam dignissim pellentesque hendrerit..

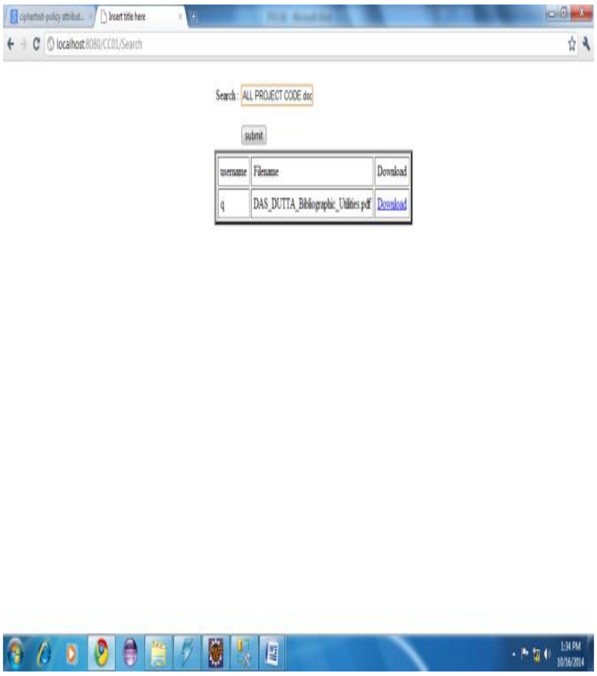
To connect with server user must give their username and password then only they can connect to the server.

Search page



Search: DAS_DUTTA_Bibliographi

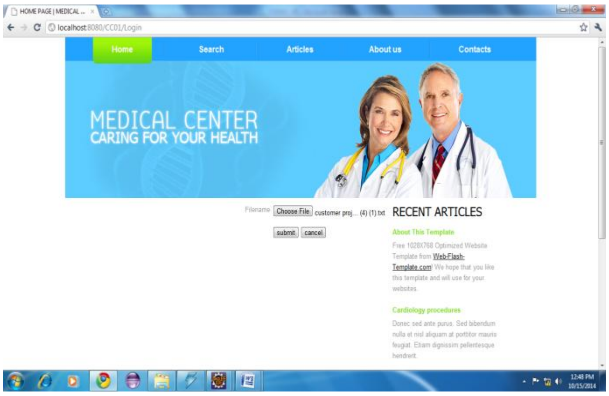
Search result



Search : ALL PROJECT CODE.doc

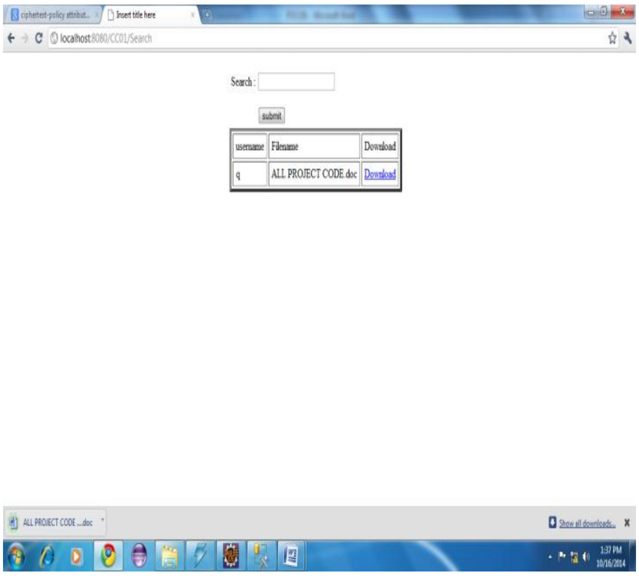
username	Filename	Download
q	DAS_DUTTA_Bibliographic_Utilities.pdf	Download

Upload page



Filename: customer proj... (4) (1).txt

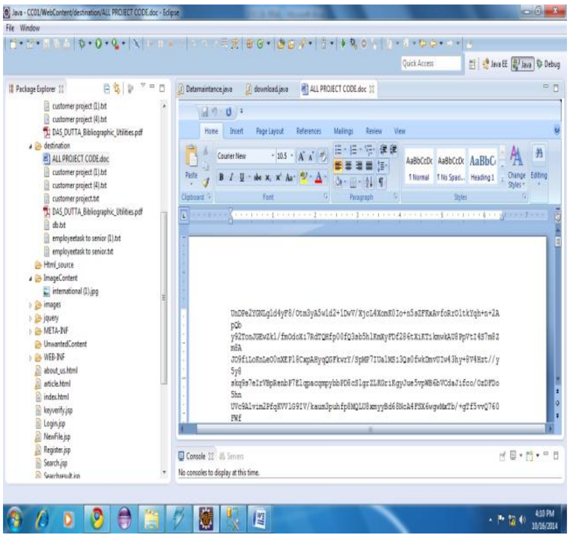
Download page



Search :

username	Filename	Download
q	ALL PROJECT CODE.doc	Download

Encrypted Data



```
UnDPe2YGNLg1d4yF8/Otm3yA5w1d2+1DwV/XjcL4XcmK0Io+n5sZFKxAvfoRrO1tkYqh+n+2A
pQb
y92TonJGEwZk1/fmOdoXi7RdTQHfp00fQ3sb5h1KmKyFDf286tXiKTikmwkAU8PpVtI457m8Z
m8A
JO9fiLoRnLeO0nXEP18CxpAHyqQGFkwrY/SpMP7IUalMSi3Qs0fwkDmvUIw43hy+8V4Hzt//y
5y8
skq9s7eIrVBpRenbP7ElqpacqmpybbPD8cSlgrZLKGriKgyJue5vpWB6bVCdaJifco/OzDFDo
5hn
UVc9Alvim2PfqKVV1G9IV/kaum3puhfp8MQLU8xmyyBd68NcA4FSX6wgwMxTb/+gTf5vvQ760
PWf
```

No consoles to display at this time.

III. Future Enhancement

Future enhancement of lifelong PHRs. The records can be shared by the patient with any stakeholder interested in those. My PHR Machines allows the controlled sharing of application software that is required to view and/or analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. Moreover, as technology evolves, patients will always be able to use original software to view and analyze data. Here the patient data is shared securely in cloud using ABE technique. Using this technique one private key is generated for each user. Depends upon the security key it will retrieve the uploaded data. Suppose a user has uploaded many data using a key he/she can retrieve the same data using the same authorized key. This key is only shared to that particular user via e-mail.

IV. Related Work

[6]Reliability at massive scale is one of the biggest challenges at Amazon.com, one of the largest e-commerce operations in the world; even the slightest outage has significant financial consequences and impacts on the trust of the customers. The Amazon.com platform, which provides services for many websites worldwide, is implemented on top of an infrastructure of tens of thousands of servers and network components located in many data centres around the world. At this scale, many components fail continuously and the way persistent state is managed in the face ofthese failures drives the reliability and scalability of the software systems. This paper shows the design and implementation a highly available key-value storage system, the Dynamo, that some of Amazon‘s core services use to provide an ―always-on‖ experience. To achieve this level of availability, Dynamo sacrifices consistency under certain scenarios which are failures. It makes extensive use of object versioning and application-assisted conflict resolution in a manner that provides a novel interface for developers to use.

[7]A new class of data storage systems, called NoSQL(Not Only SQL), have emerged to complement the traditional database systems, with elimination of general ACID transactions as a common feature. Different platforms and different primitives within one NoSQLplatform, can offer various consistency properties, from Eventual Consistency to single-entity ACID. For the platform providers, weaker consistency will allow better availabilities, lower latencies, and other benefits. This paper investigates what the consumers observe of the consistencies and performance properties of various offerings. We find that many platforms s in practice offers more consistencies than they promise; we also investigate cases where the platform offers consumers a choice between stronger and weaker consistencies, but there is no observed benefits from accepting weaker consistency properties.

[8]Cloud computing has recently emerged as a key technology to provide individuals and companies with access to remote computing and storage infrastructures. To achievehighly-available and high-performing services, cloud data stores depends upon data replication. But, providing replication brings with it the issue of consistency. Given that the data will be replicated in multiple geographically distributed data centres, and to meet the increasing needs of distributed applications, many cloud data stores accept eventual consistency and therefore it will allow running data intensive operations under low latency. This comes at the cost of data staleness. In this paper, we arrange data replication based on a set of flexible data semantics that can suit all types of Big Data applications, and avoid overloading of both network and systems during large periods of disconnection or partitions in the network. Therefore we integrated these data semantics into the core architecture of a well-known NoSQL data store (e.g., HBase), which leverages a three-dimensional vector-field model (i.e., regarding timeliness, number of pending updates and divergence bounds) to provision data selectively in an on-demand fashion to applications. This improves the former consistency model by providing a number of required levels of consistency to different applications ,such as, social networks or ecommerce sites, where the preference of updates also differ. In addition, our implementation of the model into HBase will also allow updates to be tagged and grouped atomically in logical batches, akin to transactions, ensure atomic changes and precission of updates as they are propagated.

[9]Since 1984, the Condor project has enabled ordinary users to do amazing computing. Today, the project continues to analyze the social and technical problems of co-operative computing on scales ranging from the desktop to the world-wide computational grid. In this paper, we provide the history and philosophy of the Condor project and illustrate how it has collaborated with other projects and evolved along with distributed computing. We describe the core components of the Condor system and also describe how the technology of computing must correspond to social structures. Throughout, we react on the lessons of experience and chart of

the course travelled by research ideas as they evolve into production systems.

[10]Eventually-consistent key-value storage systems sacrifice the ACID semantics of conventional databases to achieve superior latency and availability. Yet, this means the end-users, can be exposed to stale data. The amount of staleness observed depends on various tuning knobs set by application developers (customers of key-value stores) and system administrators (providers of key-value stores). Both parties must be observant of how these tuning knobs affect the consistency observed by client applications in the concern of both giving the best end-user experience and increasing revenues for storage providers. Quantifying consistency in a useful way is a critical step toward both knowing what clients actually look at, and supporting consistency-aware service level agreements (SLAs) in next generation storage systems. This paper proposes a novel consistency metric called (Gamma) that occupies client-observed consistency. This metric provides significant answers to questions regarding consistency anomalies, such as how often they occur and how bad they are when they do occur. We argue that it is more useful and accurate than current metrics.

V. Conclusion

In this paper, we presented MyPHRMachines, a novel PHR system. Leveraging virtualization techniques, MyPHRMachines allows patients to build lifelong PHRs. The records can be shared by the patient with any stakeholder interested in those. MyPHRMachines allows also the controlled sharing of application software that is required to view and/or analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. Moreover, as technology evolves, patientswill always be able to use original software to view and analyze data, even when that software becomes obsolete and possibly no longer supported by the stakeholder that produced the data.

VI. References

[1] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, ―Viewpoint paper:Aresearch agenda for personal health records (PHRs),‖ J. Amer. Med. Inform. Assoc., vol. 15, no. 6, pp. 729–736, 2008.

[2] AHIMA e-HIM Personal Health Record Work Group, ―Defining the personal health record,‖ J. AHIMA, vol. 76, no. 6, pp. 24–25, Jun. 2005.

[3] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, ―White paper: Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption,‖ J. Amer.Med. Inform. Assoc., vol. 13, no. 2, pp. 121–126, 2006.

[4] Health Informatics—Electronic Health Record—Definition, Scope and Context, International Standards Organization, ISO/TR 20514:2005, Jan. 2005.

[5] Giuseppe DeCandia, DenizHastorun, MadanJampani "Dynamo: Amazon‘s Highly Available Key-value Store"

[6]Hiroshi Wada, Alan Fekete, Liang Zhao "Data Consistency Properties and the Trade offs in Commercial Cloud Storages:the Consumers‘ Perspective"

[7]Álvaro García-Recuero, SérgioEsteves, Luís Veiga."Quality-of-Data for Consistency Levels in Geo-replicated Cloud Data Stores"

[8]Douglas Thain, Todd Tannenbaum, and MironLivny"Distributed Computing in Practice The Condor Experience"

[9]WojciechGolab, MuntasirRaihanRahman, Alvin AuYoung "Client-centric Benchmarking of Eventual Consistency for Cloud StorageSystems"

[10] A. Rosenthal, P. Mork, J. Li, M.H. and Stanford, D. Koester, and P. Reynolds, ―Cloud computing: A new business paradigm for biomedical information sharing,‖ J. Biomed. Inf., vol. 43, pp. 342–353, 2010.

[11] Accelarad. (2012, Jul.).Seemyradiology – medical image sharing. [Online]. Available: http://www.seemyradiology.com.

[12] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, ―Cloud computing—The business perspective,‖ Decis. Supp. Syst., vol. 51,pp. 176–189, 2011.

[13] M. Beyer, K. A. Kuhn, C. Meiler, S. Jablonski, and R. Lenz, ―Towards a flexible, process-oriented IT architecture for an integrated healthcare network,‖ in Proc. ACM Symp. Appl. Comput., 2004, pp. 264–271.

[14] T. J. Bittman, G. J. Weiss, M. A. Margevicius, and P. Dawson, ―Magic quadrant for x86 server virtualization infrastructure,‖ Gartner Inc.,Stamford, CT, USA, RAS Core Research Note G00205369, Jun. 2011.

[15] D. T. Mon, J. Ritter, C. Spears, and P. Van Dyke, ―PHR system functional model,‖ HL7 PHR Standard, May 2008.