Tackling Cloud Security Issues and Forensics Model

Shaftab Ahmed
Department of Computer Science and Engineering
Bahria University, Islamabad, Pakistan
Shaftab_2010@yahoo.com,

and

M. Yasin Akhtar Raja
Physics and Optical Science,
Center for Optoelectronics & Optical Communications
UNC Charlotte, NC 28223-0001
raja@uncc.edu; http://maxwell.uncc.edu/raja

Abstract

Cloud computing is getting increased attention of the information and communication technologies (ICT) industry recently. The cloud service providers foresee it as a source of promising financial gains, the clients find it a convenient solution where the enterprises may get started on their computing activities without investing on the in-house facilities of hardware and software. They can outsource the computing and archiving activities to the cloud service providers (CSP) though Internet. There are many dimensions of these activities and the researchers are trying to find acceptable solutions for the industry. In this paper, we have focused on the information security issues when migrating to a cloud environment. The confidence of end user can be won partially by the guarantees of service provider and use of cryptographic techniques. It is important that the Intrusion Detection Systems (IDS) should be included in the models which support forensic study whenever required. It is equally important to address the issue of anti-forensic methods that the service providers may use to hide their malicious activities. Therefore the clients would like to have a better, in-depth knowledge of information management at service providers' end. For this purpose tools to probe into the cloud services are required. To elaborate on this issue we have chosen the data archiving and storage model used for medical service providers and hospitals. It is a classic test-case where Patients' history has to be maintained under the guidelines of HIPPA. The Amazon security model has been reviewed for this purpose both for archiving and disaster recovery. An acceptable security model over the cloud architecture is also proposed.

Keywords: CSP, HIPPA, IDS,TPA,CFT

I. INTRODUCTION

The cloud is a virtual computing environment which provides applications, platforms and software support as services. The applications are extended over the Internet domain to the Cloud Service Provider (CSP) which maintains computer systems in clusters; they usually have large storage capacity over Storage Area Networks (SAN) called Data Centers (DC). The CSPs support fault tolerant systems meeting the user requirements of hardware, software and platform in scalable, elastic service architecture through a contract. The enterprise using a datacenter support, out sources its computation load on a "pay as you go" basis [1]. Hence beginning an application in a smaller scope, then extending it with proven viability is a great advantage of this new paradigm in ICT. The CSP takes care of all the day to day maintenance of systems and software usage i.e. logging and accounting procedures. The clients do not maintain computing facilities instead they have access to the Data center over the Internet connectivity on anywhere anytime basis. Cloud computing architecture, opportunities and concerns are reviewed in this section. The software and services offered by leading software developers are used as reference [2].

The enterprises like data banks, medical facilities and hospitals, scientific, industrial and research organizations usually need large storage facilities to maintain archives which run into peta -bytes in size. It is therefore feasible to outsource this activity to a Data Center. In many cases a hierarchical ordering based on usage coupled with intelligent search utilities with caching support improve data availability. In cloud environment a developer leases data center facilities saving time for research and innovative development rather than handling routine jobs.

Ian Foster [3] defined cloud as, "A computing paradigm which is a pool of abstracted, virtualized, dynamically scalable, managed, computing, power storage platforms and services for on demand delivery over the Internet". The clouds can be implemented at Private, Enterprise and External levels. The clouds may also be federated into virtual private clouds [4]. The community clouds may also be formed by joining trustful domains of similar activities together to share computing and data storage resources.

The hypervisor technologies are used to compose virtual machines on demand; they are dynamically managed and provisioned over the web services resource framework [5]. The cloud service provider supports distributed identity and trust management, persistence and parallelism of data. The clients are charged for virtual machines leased, computing time and network bandwidth.

978-1-4244-9924-3/10/$26.00 ©2010 IEEE

Cloud computing is expected to be another success surge in ICT which will change the industry significantly. The leading service providers at present include Amazon Compute Cloud EC2 and the Data Cloud S3, Google AppEngine, Microsoft Azure, Ubuntu Enterprise Cloud and Aneka of Manjrasoft and others [5-9]. They offer computation and data storage services at very low upfront costs easily scalable to match the user requirements.

Amazon Elastic Computing Cloud (EC2) [5] offers a library of available Amazon Machine Images (AMI). The users may configure an AMI of their choice as well and exercise control over software starting from Kernel upwards. The Simple Storage Service (S3) of Amazon is used to upload the selected or composed AMIs before execution. Amazon charges the user by instance / hour for each machine instance and data storage in GB-month basis. Data transfer is charged in tera bytes. Application engine for Web Services (AWS) offers a number of higher level managed services for use in conjunction with EC2.

Google Application Engine offers web application services through web based Admission Console (AC) to manage and run web applications. It supports an API for data storage, email services etc. The AppEngine has impressive automatic scaling and high availability features [6]. The Mega store based on Bigtable data storage is available to the AppEngine applications. However AppEngine is not suitable for general purpose computing

Microsoft Azure [7] applications are developed using .NET libraries and compiled using Common Language Routine (CLR). The Azure is intermediate between compute application framework of AppEngine and the hardware virtual machine of EC2. The system supports general purpose computing. The libraries provide a degree of automatic network configuration and failover / scalability.

Ubuntu Enterprise Cloud Architecture [8] offers Linux distribution for cloud services. The claimed mission of Ubuntu is to select best components from open source, refine and provide them to users. Its strategy includes multi vendor support and procedures to avoid “data lock in” to counter the fear that monopolies in cloud industry might emerge. The three components developed are as under:

Aneka [9] is a .NET based service oriented platform for grid/cloud applications. It is built on a de-centralized architecture consisting of executers accessible over the Internet through a configurable container.

Cloud computing is being projected as the fastest growing technology with the inclusion of heavy weights ready to field data centers providing solutions to customers in almost all fields. However a lot of road blocks have yet to be cleared. A de facto standard for application development and deployment over the cloud is required to avoid monopolization of services. Interoperability and portability between clouds has to be ensured by international acceptable practices to build confidence of the end users and entrepreneurs to feed their applications without any hesitation. The application developer should be allowed to flexibly migrate to desired cloud service provider without compromising security and functionality of their intellectual assets [10].

Cloud Computing has a wide range of applications ranging from social networking, web hosting, data archiving presentation and high performance computing. The composition of services for a cloud computing application is a challenging task involving configuration and deployment over the virtual environment offered by a service provider. Hence cloud simulation can play an important role in the design phase by conceiving and operating computer architecture and applications on a simulator. The Cloudsim [11] is a simulator which supports a virtualization engine and services model to field an application. It provides an opportunity to test an application in a repeatable and controllable environment to tune for performance, speed, availability and other measuring parameters before setting up an application on a real Cloud computing environment.

The rest of the paper is organized such that in section 2 we elaborate the cloud security issues and related work, in section 3 we discuss the issues regarding medical data management of a hospital over cloud, we discuss forensic and anti forensic techniques usable over the cloud, section 4 a model data management system is proposed for a medical facilities and hospitals using cloud services.

II. Cloud Security issues and Related Work

Security of data in conventional systems is handled by authentication, Access Control and Authorization principles. The ICT experienced serious security problems in data communication for distributed computing, data sharing applications in client server or P2P arrangements. The security problems were further aggravated with increasing use of Internet. In the past two decades high speed communication and Internet has led to innovative developments in distributed information storage management. The grid developers have successfully demonstrated the viability of virtual super computing architectures. The digital libraries and decision support tools are now available. To address the fundamental issue of trust management the cloud architecture is designed to outsource computing activities to a Cloud Service Provider, who may undertake to provide assurance of secure data handling [12]. The data security issues are still the main concern but cloud computing architecture helps to reduce the complexity.

The data communication is vulnerable to the hacker attacks of various natures. In the past two decades researchers have produced a number of methods for secure communication which are not easy to break. The ecommerce has flourished in trustful domains and use of ATM for banking transactions is very common. But the fundamental issue which hampers wide acceptability of Grid or cloud is the vulnerability in non-trustful domains of users and service providers [13] [14].

The last few years have given a new buzz word to the industry, “Cloud Computing”. It has shifted the responsibility of data management and security to the service provider. Hence good data communication connectivity and a trustful CSP provide a fool proof arrangement. But in this process a client loses control over the hardware and data further down the line [15]. The requirement of trust is higher and the loss of control over the virtual environment has given rise to a number of additional problems, being addressed by the developers. To elaborate on security issues, the requirement of greater client monitoring and control over the Cloud Service Provider activities we have chosen ICT services for data archiving, storage systems in a medical hospital.

The e-healthcare is an important component in medical systems for medical treatment and patient monitoring. On line patient history log is often available at all times and anywhere allowing patient and doctor’s mobility [16]. Intelligent agents can be embedded in such systems to analyze patient’s record in the background to raise alerts or messages to the doctor. The telemedical diagnosis and treatment is extremely important in disaster, war and emergency conditions when the physical infrastructure may not be available [17].

The e-healthcare informatics is handled in mainly three tiers i.e. organizational, operational and technological realms. Cloud computing provides workflow management and dynamic integration of medical communities. High performance virtual machines available in the cloud can be acquired to provide analysis at high speed [18]. It may provide an excellent decision support system for medical image interpretation diagnosis and second opinion scenarios often required by the experts in medical science for complex cases [19]. Collaboration in medical community through mutually agreed security standards for Digital Rights Management (DRM) is extremely important because the medical data is a personal property with a high-level of sensitivity. The data management for a hospital cannot be satisfactory by contractual obligations committed by a trustful service provider unless it is augmented by provenance methods. Medical data security is a serious issue which needs to be critically discussed and suitable forensic methods have to be enabled along with verifiability of the data assets. The Third Party Auditor (TPA) may be required to certify the Cloud service provider’s activities [20]. A mutual agreement and the deep accessibility in the system are therefore required. The researchers and developers are actively trying to find acceptable solutions [21].

III. TELEMEDICINE OPPORTUINITIES AND SECURITY ISSUES IN CLOUD INFRASTRUCTURE

A. *Medical diagnosis and requirements of storage*

The data libraries of medical images and transcripts are scattered over heterogeneous systems at geographically diverse locations requiring flexible system of storage, retrieval and persistence management over the services architecture. The cloud service requirements for image reconstruction, rendering and diagnosis require high performance machines due to large volume of data generated per day by diagnostic scanning and medical imaging like CT (Computed Tomography), MRI (Magnetic Resonance Imaging), and PET (Positron Emission Tomography etc [22].

The fault tolerance and data availability at all times with the rapidly growing needs in hospitals usually require professional ICT staff besides the capital commitment for computers, peripherals and large data archives. These archives are very large containing medical histories of patients spanned over a number of years. Some of these are current but others must be retrievable on short notice to handle emergency conditions. The hospitals have an opportunity to out source the data archiving, searching activities and all time availability etc to the cloud service provider. The hospitals have to pay services cost only, the rest is done by the service provider.

B. *Forensics and anti-Forensics Techniques*

Forensics deal with detection, preservation, acquisition and provenance methods used as digital evidence to establish cyber crime in court of law [23]. Computer Forensic Tools (CFT) have been developed to recover deleted files, collect evidence of intruder activities and to preserve the evidence in a non refutable manner. The CFTs are mainly of two types i.e. persistent data tools and volatile data tools. The persistent data tools analyze the data available in log files etc which can be traced even after the system is shutdown. The volatile data tools deal with the data generated during the system running various applications generating forensically important information which might be lost when the system is turned off. The forensic experts install sniffers and data loggers on the threatened machine to capture volatile information. The nonvolatile information has to be protected through authentication, authorization and access control procedures suitably augmented by signatures.

The cloud computing will earn the confidence of business and financial institutions by using strong forensic methods to ensure privacy, confidentiality and tracking of the activities at the service provider end. The healthcare information management is sensitive where the personal privacy has to suitably protected, hence the cloud computing models have to ensure that the owner’s control is not compromised while handing over the data to cloud service provider. The provenance procedures [24] maintain a log of data access and management activities like, who created, modified or copied the data objects; the forensic tools extract evidence from this data. It is important that the client of a CSP is convinced that the data forensics have provenance data managed in a secure manner. If this data is compromised then the whole model may collapse. Hence the concept of unforgeability and conditional privacy preservation are considered to be fundamental to win the confidence of client communities for cloud computing. [25]

Anti-forensic techniques are used for destroying evidence [26]. On one hand it is used by the hacker or maligned user to hide their activities and on the other hand the sensitive secret organizations would like to leave no traceable information. In the case of cloud service provider the anti-forensic activities have to be watched, reported and suitable action should be taken so that the users' confidence in the services is not compromised [27].

C. Requiremnts of HIPPA

The Hospital Information Systems (HIS) are used for handling a large number of patients and variety of activities like consultation, medical prescription, diagnostic tests etc. The Patient History Information (PHI) has to be maintained through mechanisms to ensure security and privacy supported by well documented, auditable log of activities. Transparency is required for regulatory reasons and to address the issues of potential data breaches. The regulations for medical data management have been laid out in the HIPAA's Privacy Rule. [28] [29]

HIPAA security safeguards require in-depth auditing capabilities for data management, back-up procedures and disaster recovery mechanisms. In designing a HIPAA-compliant system [29], the service providers are bound to provide on-line probing features which may be invoked without prior notice. The architecture should allow security analysts to drill down into detailed activity logs or reports to see who had access to data, the IP address used etc. This data should be tracked, logged, and stored in a central location for extended periods of time for audit. For example, Amazon has provided web services which can be used to create HIPPA compliant medical data management and applications [29].

D. Data Managemnt and Security Services Support Offered by Amazon[29]

In this section we review the service requirements of an enterprise like a medical facility or a hospital, and the mechanisms offered by Amazon to address the security and confidentiality issues through client verifiable procedures for data management at the service provider end.

Data management in a cloud originates from the client side that has outsourced the storage to a CSP. The remotely maintained hardware at the service provider end is logically available to the client like the AMI (Amazon Machine Instance), the client may like to go beyond the service agreement for secure management of data by verifiable data access and manipulation activities. For example a client would like to exercise direct control over the hardware and system software through access to the socket layer in the communication protocol stack for verification of various activities. He/she may like the service provider to maintain a log structured information for direct review by the client. Hence a concept of verifiable security of data management activities over the cloud architecture is the core activity to win the confidence of ICT players [26].

Classical data encryption mechanisms can be used for data communication between the client and cloud host. Additional requirements have to be provided for example the Amazon EC2 provides full root access and administrative control over virtual servers. Amazon S3 can be accessed via Secure Socket Layer (SSL)-encrypted endpoints over the Internet. The encryption methods used by the cloud service providers are similar to the conventional encryption and security procedures e.g. 256 bit AES algorithms. The authentication may be token or key-based to access virtual servers. Amazon EC2 creates a 2048 bit RSA key pair, with private and public keys and a unique identifier for each key pair to help facilitate secure access.

i. **Data security for client server access**

AWS security uses policies and processes regarding authentication, access and audit controls to ensure restricted access to a system which may be constantly monitored by the client. AWS follows the concept of least privilege for grant of access and control of data. For example, AWS employees cannot look at customer data, or have access to customer EC2 instances. In rare circumstances the service provider may be explicitly authorized access by the client through an elaborate arrangement

ii. Access Control Processes

The client system administrator is responsible to setup user controls to restrict data access and ensure security. Using Amazon EC2, SSH network protocols can be used to authenticate remote users or computers through public-key cryptography. The administrator may use group or individual level control to allow or block access at account or instance level.

Using Amazon S3, access can be easily controlled down to the object level through associated Access Control List (ACL) detailing the activities authorized. The system administrator maintains full control over who has access to the data at all times and the default settings only permit authenticated access to the owner or creator of the object. For both Amazon S3 and EC2, each account has a secret key that is crucial for maintaining security of customer accounts. Secure HTTP (HTTPS) connections for web applications running in the cloud ensure that any information presented in the interface is protected as it travels from AWS to the clients. With all these features offered by AWS the HIPPA compliance certification will be required based on real-time testing of data services along with provenance tests conducted periodically.

IV. Acceptable Medical Security Model over the Cloud

The medical diagnostic procedures evolved in the past two decades generate digital data which requires imaging techniques and decision support tools to view the anatomical cross-sections of bones and other organs of human body. They are used to assess the damage caused by a disease or progress in recovery; the clinical measurements and assessments are used by the doctors for medical therapy, drug administration or surgical procedure planning. Hence the Picture Archiving and Communication Systems (PAC) have become essential in medical treatment and biomedical research [31].

The in house facilities of a typical hospital are shown in figure 1, which cater for image acquisition, storage and retrieval. The Network Access and Storage (NAS) or Storage Area Network (SAN) are usually setup in data services architecture. The viewing and reporting stations are used by the doctors for online data and accessibility to the data archives.

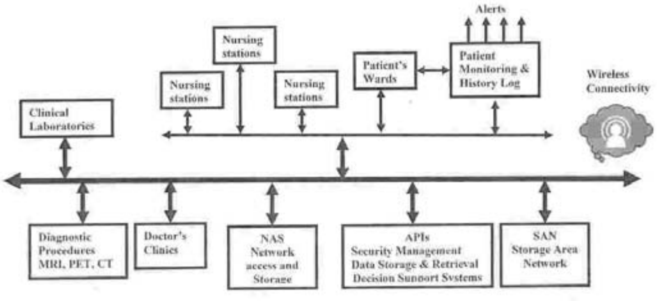
Alerts
Nursing stations
Nursing stations
Nursing stations
Patient's Wards
Patient Monitoring & History Log
Wireless Connectivity
Clinical Laboratories
Diagnostic Procedures MRI, PET, CT
Doctor's Clinics
NAS Network access and Storage
APIs Security Management Data Storage & Retrieval Decision Support Systems
SAN Storage Area Network

Figure 1 Clinical data management in a typical hospital

The data availability over the web allows easy access to the patients, doctors and medical staff on anywhere anytime basis. So the data services are extended from the hospital or enterprise level to the web using Application Service Provider (ASP). A typical data access and management system will include Internet server or gateway at the hospital end connected to ASP as shown in figure 2. This model is then extended to support data sharing and accessibility of other medical facilities and hospitals, research institutes and medical data repositories.

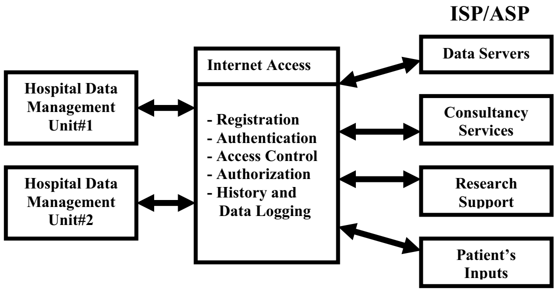

Figure 2 Hospital Information System extended over the web through an ASP

The cloud based services replace the Internet domain ISP/ASP with the Cloud Service Provider as shown in figure3. The services architecture is extended and the responsibilities regarding data integrity, accessibility and management is outsourced to service provider having professional experts in computer software and hardware who can be bound through legal mechanisms and periodic certification by a Third Party Audit (TPA). This is in contrast to the free for all vulnerable Internet access through a website. The forensic and anti-forensic studies are performed by TPA to check the CSP activities dynamically. Mutual agreement and the provenance methods as discussed before will help in making the model acceptable for sensitive data storage and sharing.

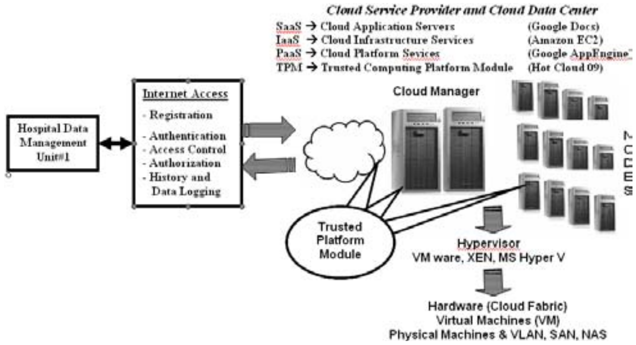
Cloud Service Provider and Cloud Data Center
SaaS → Cloud Application Servers (Google Docs)
IaaS → Cloud Infrastructure Services (Amazon EC2)
PaaS → Cloud Platform Sevices (Google AppEngine
TPM → Trusted Computing Platform Module (Hot Cloud 09)
Hospital Data Management Unit#1
Internet Access
- Registration
- Authentication
- Access Control
- Authorization
- History and Data Logging
Cloud Manager
NODES
Trusted Platform Module
Hypervisor
VM ware, XEN, MS Hyper V
Hardware (Cloud Fabric)
Virtual Machines (VM)
Physical Machines & VLAN, SAN, NAS

Figure 3 Cloud based services offered by a CSP in a next generation Hospital Information System

It is desirable that the software designs should include cloud services for in house data management as well extendable over the Internet through the CSP. This will make the enterprise data model easily adaptable to wider range of applications in the long run.

The architecture design of a cloud based medical information system should include secure data interchange, access to decision support tools for clinical data repositories. These repositories could be at local, regional or global levels. Microsoft cloud services and characteristics of CSP e.g. Windows Azure services [30] can be adapted in enterprise data centre through:

- Standardized virtualized hardware model
- Virtualized and abstracted application model
- Service centered operational model

V. Conclusion

The cloud computing is a new platform which is a potent solution for a number of applications in ICT industry. Some of these areas include large data archives, ultra /super computer speeds of computing engine configurable on demand with pay as you go feature. The business enterprise structures are going to experience a significant new dimension where the physical office environments and in house IT infrastructure will not necessarily be required. The software developers and IT managers should include cloud computing architectures and technologies in their system development strategy to take advantage of growing new enterprise solutions. In such solutions the data within the enterprise is maintained in the local or enterprise cloud which is extended to the cloud domain hosted by a service provider.

The cloud computing models have to win the trust of clients through acceptable security procedures. The client may choose for levels of security with a corresponding service cost strucutre. The security control measures offered by the CSPs at present are not sufficient to address the concerns of business and research communities. The trusted cloud service provider is the central point of security in such solutions. The giants in the IT industry like Amazon, Google and IBM foresee a large billion dollar market if they can address the security concerns to win the user confidence and evolve data hosting environments enjoying the trust like, banking system of modern society for monetary purposes. The cloud computing platforms are evolving and are expected to become a part of our society soon. Verifiable data management activities and audit reports acceptable to the end users along with low level accessibility will help in this regard.

The self describing software development may be considered for creating virtual secure computing environments in the cloud. The data may be encrypted and packaged with a usage policy mutually agreed between client and CSP which is extended to built-in security policy has to validate the data access by a user. This may be used to create virtual environments in a glass box where the actual data is extracted. Later this temporary setup is destroyed and properly verified.

VI. References

[1] Gerald Briscoe, Alexandros Marinos, “Digital Ecosystems in Clouds: Towards Community Cloud Computing”, Department of Media and Communications London School of Economics and Political Sciene.

[2] Shaftab, Azween, “Telemedicine in a cloud – A Review” Department of Computer Science and Engineering, Bahria University, Islamabad, Pakistan, Department of Computer and Information Sciences,, Universiti Teknologi Petronas, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia

[3] Ian Foster, Yong Zhao, Ioan Raicu, Shyong Lu, “Cloud Computing and Grid Computing 360-Degree Compared”, Department of Computer Science University of Chicago

[4] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, “Market-Oriented Clou Computing: Vision, Hype and Reality for Delivering IT services as Computing Utilities” Manjrasoft Pvt Ltd, Melbourne, Australia

[5] Amazon Elastic Compute Cloud (EC2), http://www.amazon.com/ec2

[6] Google App Engine, http://appengine.google.com

[7] Windows Azure Platform http://windowsazure.com

[8] Simon Wardley, Etiene Goyer, Nick Barcet, “Ubuntu Enterprize Cloud Architecture” Technical white paper August 2009

[9] Aneka: Enabling .NET-based Enterprise Grid and Cloud Computing manjrasoft.com/products.html

[10] Michael Armburst, Armando Fox and group, “Above the Clouds: Berkely View of Cloud Computing”, UC Berkeley, adaptive Distributed Systems Laboratory, February 10, 2009

[11] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, “Modeling and Simulation of Scalable Cloud Computing environments and the CloudSim Toolkit: Challenges and Opportunities”, 2009

[12] Carl Almond, “Practical guide to Cloud Computing security” Accenture and Microsoft

[13] “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1”, prepared by Cloud Security Alliance, December 2009

[14] “Cloud Computing, risks and recommendations for information security”, enisa – European Network and Information Security Agency report -2009

[15] Chow, Golle, Jakobsson, Masuoka, Molina, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”, *CCSW’09*, November 13, 2009, Chicago, Illinois, USA.

[16] Shaftab, “Grid Services Architecture for Archiving and Presentation of Medical Images”Department of Computer Science and Engg. Bahria University, Islamabad, Pakistan HONET 2007

[17] Kevin D. Bowers, Ari Juels, Alina Oprea, “HAIL: A High-Availability and Integrity Layer for Cloud Storage” RSA Laboratories, Cambridge, MA, USA

[18] Apu Kapadia, Steven Myers, XiaoFeng Wang, and Geoffrey Fox, “Secure Cloud Computing with Brokered Trusted Sensor Networks” School of Informatics and Computing Indiana University, Bloomington

[19] *Raza Hashim, PhD; Thomas L. Lewis, MD;Stephen J. Rosenfeld, MD, “*Managing Clinical Research Information: A Case Study in Information Access, Presentation, and Analysis” Journal of Healthcare Information Management®, vol. 14, no. 3, Fall 2000

[20] Cong, Qian, Kui, Lou,” Ensuring Data Storage Security in Cloud Computing”, Department of ECE Illinois Institute of Technology and Worcester Polytechnic Institute

[21] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”, Illinois Institute of Technology, Chicago IL 60616, USA,

[22] Habib Zaidi, “Medical Imaging: Current status and future perspectives” Division of Nuclear Medicine, Geneva University Hospital, CH-1211 Geneva. Switzerland

[23] Gary C. Kessler, “Anti-Forensics and the Digital Investigator” Champlain College Burlington, VT, USA Edith Cowan University, Mount Lawley, WA, Australia

[24] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing” Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada

[25] Ragib Hasan, Radu Sion, Marianne Winslett, “Introducing Secure Provenance: Problems and Challenges” Dept. of Computer Science University of Illinois at Urbana-Champaign

[26] Ari Juels and Burton S. Kaliski Jr, “PORs: Proofs of Retrievability for Large Files”, RSA Laboratories Bedford, MA, USA, EMC Corporation Hopkinton, MA, USA

[27] Rayan Harris, ”Arriving at an antiforensic concensus. Examining how to define and control control the anti-forensics problem” Purdue University, USA

[28] “Protecting Personal Health Information in Research: Understanding the HIPPA Privacy Rule”, Department of Health and Human Services, USA,NIH Publication Number 03-5388 http://www.hhs.gov/ocr/hippa

[29] “Creating HIPPA-Compliant Medical Data Applications with Amazon Web Services”, April 2009

[30] Website_MMS_2010_Whitepaper, “Microsoft’s cloud computing infrastructure vision & approach”