ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

SCHOOL OF INFORMATION SCIENCE

HEALTH INFORMATICS PROGRAM

FRAMEWORK TO ADOPT CLOUD COMPUTING FOR MEDICAL IMAGE ARCHIVING AND SHARING

BY:-

BIZUAYEHU GETNET DEMSASH

NOVEMBER, 2012

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

SCHOOL OF INFORMATION SCIENCE

HEALTH INFORMATICS PROGRAM

FRAMEWORK TO ADOPT CLOUD COMPUTING FOR MEDICAL IMAGE ARCHIVING AND SHARING

A Thesis Submitted in Partial Fulfillment of the
Requirement for the Degree of
Master of Science in Health Informatics

BY:-

BIZUAYEHU GETNET DEMSASH

NOVEMBER, 2012

ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES
SCHOOL OF INFORMATION SCIENCE
HEALTH INFORMATICS PROGRAM

FRAMEWORK TO ADOPT CLOUD COMPUTING FOR MEDICAL IMAGE ARCHIVING AND SHARING

BY:-

BIZUAYEHU GETNET DEMSASH

Name and signature of members of the examining board,

Name	Title	Signature	Date
1. Ayele Belachew	(Advisor)	_____	November 02,2012
2. Workshet Lamenew	(Advisor)	_____	November 02,2012
3. Solomon Tefera (PhD)	(Examiner)	_____	November 02,2012
4. Getnet Mitikie (PhD)	(Examiner)	_____	November 02,2012

Dedicated To:
Abinew Ejigu

Acknowledgement

Writing an acknowledgement is not an easy task. This is because there are so many people who have helped along the way. The authors' greatest fear is forgetting someone, so I start off by saying thank you to all. If your name is not mentioned, please forgive me!

Thanks go to Dr. Ayele Belachew of the school of public health, at Addis Ababa University, who served as my advisor supervisor during the course of writing this dissertation. Thanks to Workshet Limenew of the school of Information Science, at Addis Ababa University, who is also my advisor during this thesis writting. Workshet helped me greatly by providing critical directions whenever needed.

Special thanks to my friends Hiwot Araya, Haben Solomon, for their help all the way in this thesis writing. I would be negligent if I did not mention my family, my parents Getnet and Atalie; and especially my sister Almaz, who have supported me through the thick and thin of this MSc studies.

Last but not least, all Health Informatics department members, lecturers and students for the different discussions, challenges and experiences shared during the this MSc. Course.

Table of Contents

Acknowledgment……..……..I
List of Figures……...VI
List of Acronyms and Abbreviations ……VII
Abstract……..VIII
CHAPTER ONE ..... ……1
1. Introduction .... ….. ..1
1.1 Background ..... ……1
1.2. Statement of the Problem ..... ……4
1.3. Objective of the Study ..... ……7
1.3.1. General objective 7
1.4. Methodology of the Study ..... …….7
1.4.1. Literature review 8
1.4.2. Expert Interview 8
1.4.3. Expert Survey 8
1.5. Significance of the Study 8
1.6. Scope of the Study.....9
1.7. Organization of the Thesis 9
C**HAPTER TWO** 11
2. Conceptual Discussion and Literature Review ..... ……...11
2.1. Cloud Computing ..... ……11
2.1.1 Definitions 12
2.2. Cloud Computing Characteristics 13
2.2.1. Abstraction of Infrastructure 13
2.2.2. Resource Democratization 13
2.2.3. Services Oriented Architecture 14
2.2.4. Elasticity/Dynamism 14
2.2.5. Utility Model of Consumption & Allocation 14
2.3. Cloud Computing Service Models 14
2.3.1. Software as a Service 14
2.3.2. Platform as a Service 15
2.3.3. INFRASTRUCTURE AS A SERVICE (IaaS) 15

2.4. Cloud Computing Deployment Models 16
2.4.1. Public Cloud 16
2.4.2. Private cloud 17
2.4.3. Hybrid Cloud 18
2.4.4. Community Cloud 19
2.5. Related Technologies 19
2.5.2. Computer Clusters 20
2.5.3. Virtualization 20
2.5.4. Service Oriented Architecture 20
2.6. Cloud Computing and Healthcare 20
2.6.1. Health care IT 21
2.6.2. The current role of technology in healthcare 21
2.6.3. Challenges in the Present healthcare 22
2.6.4. Cloud computing in the health sector 24
2.6.5. Benefits of Health Care Service in the Cloud 25
2.6.6. Risks of health care services in the cloud 27
2.7. Cloud Computing for Medical Image Sharing 29
2.7.1. Medical Imaging 29
2.7.2. Data and Workflow sharing 30
2.7.3. Benefits of Image Sharing 33
2.7.4. Prerequisites for data sharing and shared workflow 35
2.7.5. Recent Technologies to Support Medical Image Sharing 43
2.7.6. Barriers for data sharing and shared workflow 48
2.7.7. Emerging Technology for Medical Image Sharing 51
2.8. Related Works 56
CHAPTER THREE 58
3. Security, Legal and Compliance Issues in Cloud Computing 58
3.1. Security..... 58
3.1.1. Security challenges in cloud computing 60
3.1.2. Security Vulnerabilities of Cloud Computing 64
3.1.3 Security and cloud computing (Standards and Best Practices) 65
3.2. Legal Issues 70
3.2.1 The Legal framework 70

3.2.2. Legal regulations relevant to eHealth 71
3.2.3 Legal challenges 73
3.3. Compliance issues 74
C**HAPTER FOUR** 76
4. Cloud Service and Provider Selection 76
4.1. Cloud Services Selection 76
4.1.1. Software as a Service (SaaS) 77
4.1.2. Platform as a Service (PaaS) 77
4.1.3. Infrastructure as a Service (IaaS) 78
4.2. Selecting Cloud Service Providers 79
4.2.1. Amazon Web Services 79
4.2.2. Google AppEngine 81
4.2.3. Microsoft Azure 82
4.3. Pilot Proposed Services of the Cloud 87
4.3.1. Database Development Service 87
4.3.2. Operating Systems Service 88
4.3.4. Information Management Systems 88
4.4. Toolkits/Frameworks For Simulate Cloud Computing 88
4.4.1. CloudSim 88
4.4.2. GreenCloud 88
4.4.3. OpenNebula 89
4.4.4. Aneka 89
C**HAPTER FIVE** 90
5. Cloud Based Services for Medical Image Archiving and Sharing 90
5.1. Building the Framework 90
5.1.1. User Interface Layer 91
5.1.2. Clinical Application Tier: (SaaS) Layer 92
5 5.1.3. Platform as a Service (PaaS) Layer 98
5.1.4. Infrastructure as a Service (IaaS) Layer 98
5.2. Proposal for Implementation Medical Image Archive and Sharing on a Hybrid Cloud…99
5.2.1 Building Private Cloud 99

CHAPTER SIX 98

6. MIAS Design Framework Evaluation 98
CHAPTER SEVEN 113
7. Conclusions and Future Work 113
REFERENCES 116

List of Figures

Figure 11: Design Science research methodology ……..7
Figure 2.1: Cloud Computing Definition ……..13
Figure 2.2: The Cloud Taxonomy ……16
Figure 2.3 Public Cloud ……..17
Figure 2.4: Private Cloud ……17
Figure 2.5: Hybrid Cloud ……18
Figure 2.6: Community Cloud ……19
Figure 2.7 Paradigm shift in healthcare cloud ecosystem ……..25
Figure 2.8 Illustrative model of the Tele-Cloud ……29
Figure 2.9.Evolution of database integrations. ……..31
Figure 2.10 Shared workflow based on XDS profile and shared databases ……...33
Figure 2.12: Decision Framework for Cloud Migration ……..53
Figure 2.13: Selecting Services for Cloud Migration ……54
Figure 3.1: Mapping Cloud model to Security and Compliance Model ……59
Figure 3.2: The four phases of ISO 27001 ……..66
Figure 3.3: Overall COBIT 4.1 Framework ……68
Figure 4.1: Windows Azure Platform Products and Components ……83
Figure 5.1: Virtual Model of Medical Ecosystem for Users on Cloud Computing ……91
Figure 5.2: Design Framework for medical image management solutions on the cloud ……...93
Figure 5.3: overview of OpenNebula ……100
Figure 5.4: Different Services of OpenNebula ……...102
Figure 5.5: Typical Aneka Cloud deployment ……104
Figure 5.6: Proposed Cloud service for Medical Image Exchange and Management. …….106

List of Acronyms and Abbreviations

A6	Automated Audit, Assertion, Assessment, and Assurance API
ACM	Automatic Capacity Management
ADT	Admission Discharge and Transfer
AMI	Amazon Machine Image
API	Application Program Interface
ATNA	Audit Node and Node Authentication
AWS	Amazon Web Services
BPPC	Basic Patient Privacy Consents
BS	British Standard
CAMM	Common Assurance Maturity Model
CCIF	Cloud Computing Interoperability Forum
CDA	Clinical Document Architecture
CDN	Content Delivery Network
CERN	European Organization for Nuclear Research
CMIAS	Cloud Based Medical Image Archiving and Sharing
COBIT	Control Framework for Information and related Technology
CP	Cloud Provider
CPU	Central Processing Unit
CR	Computed Radiography
CRM	Custormer Relation Management
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DICOM	Digital Imaging and Communication in Medicine
DMTF	Distributed Management Task Force
DSS	Data Security Standard
EC2	Elastic Compute Cloud

eHealth	Electronic Health
EMPI	Electronic Master Patient Index
EMR	Electronic Medical Record
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	Eurpean Union
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
GUI	Grafical User Interface
HER	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
HIT	Healthcare Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
HL7	Health Level 7
HMIS	Hospital Management Information System
HTTP	Hyper Text Transfer Protocol
I/O	Input/ Output
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IEC	International Electro technical Commission
IHE	Integrating the Healthcare Enterprises
IIS	Internet Information Service
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JTC1	Joint Technical Committee 1
LDAP	Lightweight Discovery Access Protocol
LOINC	Logical Observation Identifiers Names and Codes
MRI	Magnetic Resonance Imaging

NIST	National Institute of Standardization and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCCI	Open Cloud Computing Interface
OGF	Open Grid Forum
OS	Operating System
PaaS	Platform as a Service
PACS	Picture Archiving and Communication System
PCI	Payment Card Industry
PDA	Personal Digital Assistance
PDF	Portable Document File
PDQ	Patient Demographics Query
PET	Positron Emission Tomography
PHI	Protected Health Information
PHR	Personal Health Record
PIX	Patient Identifier Cross-refferencing
QoS	Quality of Service
R&D	Research and Development
RDS	Relational Database Service
RESERVOIR	Resources and Services Virtualization without Barriers
REST	REpresentational State Transfer
RIS	Radiology Information System
RLS	Resource Locator Service
RPC	Remote Procedure Call
RRS	Reduced Redundancy Storage
S3	Simple Storage Service
SaaS	Software as a Service
SDK	Software Development Kit
SimpleDB	Simple Data Base
SLA	Service Level Agremeent

SNOMED-CT	Systematized Nomenclature of Medicine – Clinical Terminology
SOA	Service Oriented Architecture
SPECT	Single Photon Emission Computed Tomography
SQL	Structured Query Language
SSL	Secure Socket Layer
SSO	Single Sign On
TLS	Transport Layer Security
UCI	Unified Cloud Interface
UK	United Kingdom
URL	Universal Resource Locator
US	United States
USA	United States of America
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNA	Vender Neutral Archive
VPN	Virtual Private Network
WPF	World Privacy Forum
XCA	Cross Community Access
XCA-I	Cross Community Access for Imaging
XCPD	Cross Community Patient Discovery
XDS	Cross Enterprise Document Sharing
XDS-I	Cross Enterprise Document Sharing fo Imaging
XDW	Cross Document Workflow
XML	Extensible Markup Language

Abstract

Today's best practices in medicine rely heavily on the use of diagnostic images and reports, throughout the hospital and in nearly every part of the healthcare enterprise. Since patients are nomadic in today's healthcare environment there is a need to distribute and retrieve images across different healthcare providers. This often requires the interaction of multiple heterogeneous platforms. Multi-site implementations therefore require advanced integration capabilities and excellent IT skills. In this context, outsourcing of computation and storage resources using cloud infrastructure has become a potential alternative. Recently there has been an increase in the number of organizations adopting and implementing Picture Archiving and Communication Systems using cloud computing model.

The research paper discusses the advantages of cloud computing for healthcare and specifically to medical imaging, the limitations of current IT utilization in healthcare organizations. It also discusses standard, legal and compliance issues for healthcare data. By doing so, this research set out to determine how a PACS can be implemented using cloud computing architectures and implementation tools, and developing a framework that helps to provide a complete and timely access to critical imaging/diagnostic information at the point of care, regardless of the source, age or location of the information in an cloud environment. In addition to the general framework to adopt cloud services, a design framework is developed in order to provide medical image archiving and sharing solution as a service.

A rigorous analysis of the latest research on Cloud Computing as an alternative to IT provision, management and security for medical image archive and sharing is done. It also took into account the best practices for Cloud Computing usage within different hospitals and imaging centers, by interviewing with selected radiologists, physicians and healthcare IT professionals.

The research finding shows that Cloud Computing is a potential alternative the framework is useful to healthcare organizations for medical image archiving and sharing. The paper finally recommends further research directions.

Key words: PACS, ICT, Cloud Computing.

Chapter One

1. Introduction

1.1 Background

Information management in hospitals, dispensaries and healthcare centers particularly in rural areas is a complex task [1]. High quality healthcare depends on extensive and carefully planned information processing. The current development of cloud computing in the healthcare context will have a big impact on the healthcare sector. It is evolving as a key computing platform for sharing resources that include infrastructures, software, applications, and business processes [1]. Virtualization is a core technology for enabling cloud resource sharing. Cloud Computing may be applied to solve problems in many domains of Information Technology like GIS (Geographical Information Systems), Scientific Research, e-Governance Systems, Healthcare Industry, Decision Support Systems, ERP, Web Application Development, Mobile Technology etc. Information Support Systems are computer based Information Systems that supports business or organizational information processing and information dissemination activities. Information Support Systems serve the management, operations, and planning levels of an organization and provide information accessibility to a wide range of users distributed over a large geographical area.

Health care organizations use variety of IT applications and infrastructures which always need to be updated as a result of the rapid growth in health care services. And the cost of IT systems in health care services is very expensive, considering that IT is not their primary activities, and many of health care organizations pass this cost to their patients. Many of these health care organizations have developed their own or purchased IT systems to support their operations. But, also many of other health care organizations are still use manual or paper-based form in their operations, especially the small-medium health care organizations, because they think that IT investment is costly. The diversification on how the health care organizations maintaining their operations, especially on maintaining patient's medical information resulted in the difficulty of accessing patient's data. Cloud computing introduces a new business model and way of delivering service and value to the medical community, as well as medical-related trading partners, business associates and customers.

There are a number of benefits—point-of-care service delivery, cost-savings, the leveraging of new applications and support for an increasingly mobile workforce—that are enabled through adoption of cloud technologies.

Information Support Systems serves as the computer technology/network support system for varied users. Information Support Systems manages and provides technical support and service for centrally administered services such as software and hardware support. Information Support Systems is responsible for the upgrade and maintenance of both hardware and software for different shades of users of an organization/enterprise. Over the past few years most of Information Support Systems are more and more dependent on high performance computing (HPC) environments such as clusters and computational grids. Most of Information Support Systems usually deal with large volume of data (structured and unstructured) that requires huge CPU power to produce results in reasonable time on which wide range of users are dependent which may be located over a large geographical area. However, configuring and maintaining a cluster or a computational grid is usually a very cumbersome activity that requires specialists to support it. In addition, the high cost to acquire this computational apparatus can be considered a serious problem to the effective use of the Information Support Systems in terms of timeliness service and availability. Furthermore with the passage of time needs have emerged for enormous infrastructure, unlimited system accessibility, cost effectiveness, increased storage, increased automation, flexibility, system mobility and shift of IT focus. Since

Cloud Computing is a fast growing trend that includes several categories of service, all offered on demand over the Internet in a pay-as-you-go model, it promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing system agility. Using a Cloud Computing strategy for Information Support Systems will help in conducting core business activities with less hassle and greater efficiency. Organizations can maximize the use of their existing hardware to plan for and serve specific peaks in usage. Thousands of virtual machines and applications can be managed more easily using a cloud-like environment. Businesses can also save on power costs as they reduce the number of servers required. And with IT staff spending less time managing and monitoring the data centre, IT teams are well placed to further streamline their operations as staff complete more work on fewer machines. Information Support Systems in

Cloud would refer to a collection of technologies that include hosted infrastructure (IaaS), like virtual servers, network equipment and disk space; hosted operating systems (PaaS), like Windows Azure and Google App Engine; and application-level services (SaaS).

In recent days, many research institutes are struggling to adapt Cloud Computing for solving problems that are continuously increasing computing and storage. There are three main factors that interests in Cloud Computing: [2] rapid decrease in hardware cost and increase in computing power and storage capacity, and the advent of multi-core architecture and modern supercomputers consisting of hundreds of thousands of cores; [3] the exponentially growing data size in scientific instrumentation/simulation and Internet publishing and archiving; and [4] the wide-spread adoption of Services Computing and Web 2.0 applications [5]. Cloud based medical image management can offer flexible solutions for hospitals and medical imaging facilities to allow clinicians to quickly access patient imaging data across multiple PACS systems at the point of care.

The benefits of using cloud technology for image archiving and sharing are numerous. The main advantages are the following:

- Cloud computing can make connectivity possible, among physicians, hospitals and imaging centers, which can reduce ordering repeat exams. This saves time, money, and limits patient radiation exposure [6].
- Cloud brings powerful IT resources to the healthcare providers: Healthcare organizations of all sizes, across all geographies, can access information technology resources that previously were out of reach. World-class applications and computing infrastructure are available to all without considerable up-front investment [6].
- Providing flexible fee structure to suit user needs: For hospitals where study volume fluctuates and capital budgets are tight, the pay-as-you-go payment structure is a good fit [7].
- Smooth transition when healthcare providers change or upgrade PACS by eliminating the need for costly data migrations [7].
- Unifies data management: It can act as the information management backbone for the entire enterprise, potentially addressing all imaging data types in a single sharing archive strategy.

However, there is an ongoing debate within healthcare as to the viability of cloud-based solutions given the need for patient privacy and sensitive personal information [8]. In considering cloud computing for health care organizations, systems must be adaptable to various departmental needs and organizational sizes. Architectures must encourage a more open sharing of information and data sources. Many HIS and clinical systems deal with processes that are mission critical, and can make the difference between life and death. Cloud computing for healthcare will need to have the highest level of availability and offer the highest level of security in order to gain acceptance in the marketplace [8]. Hence there might be a need to create a 'Healthcare-specific Cloud' that specifically addresses the security and availability requirements for healthcare.

Many regions in the US and other developed countries are establishing health information exchanges (HIEs), which are cloud-based information clearing houses where information can be more easily shared between hospitals, health systems, physicians, and clinics [8]. There are many technology vendors and service providers, who are already building cloud-based HIEs, many of which are already functioning and providing tremendous value to patients, administrative authorities, and providers. Hospitals and physicians are starting to see cloud-based medical records and medical image archiving services. The objective is to offload a burdensome task from hospital IT departments and allow them to focus on supporting other imperatives such as EMR adoption and improved clinical support systems.

Early successes of cloud-based physician collaboration solutions such as remote video conference physician visits are being trialed. Extending such offerings to a mobile environment for rural telehealth or disaster response is becoming more real with broader wireless broadband and smartphone adoption. We are convinced that traditional healthcare IT vendors will benefit from aligning and collaborating with each other, such that healthcare domain-specific clouds can be created, creating a transformational shift in the healthcare industry.

1.2. Statement of the Problem

Technology is ushering in a new world of possibilities for smarter healthcare [9]. Provider organizations have unprecedented opportunities to become increasingly patient-centered and information-driven—a combination that holds the promise of more personalized patient care than ever before—delivered in a more cost-efficient manner than previously

possible. Many healthcare providers and insurance companies today have adopted some form of electronic medical record systems, though most of them store medical records in centralized databases in the form of electronic records [10]. Typically, a patient may have many healthcare providers, including primary care physicians, specialists, therapists, and other medical practitioners. In addition, a patient may use multiple healthcare insurance companies for different types of insurances, such as medical, dental, vision, and so forth.

Imaging is routinely used for screening, surveillance, diagnosis, and as part of therapy[11]. Thus, images and associated reports are central to tracking and providing best advice to all citizens. In today's healthcare environment, a mid-sized to large hospital may conduct more than 300,000 imaging procedures per year [12]. Image data are produced and/or used by different specialties, ranging from dental x-rays, dermatology photographs, and pathology slides to computerized tomography scans for oncologists and magnetic resonance images for cardiologists [11]. Most hospitals store these images in picture archiving and communications systems (PACS), and each clinical department typically has its own unique PACS application.

Image sharing across institutions is critical to reducing unnecessary, redundant procedures as well as providing comprehensive access to data to enable good patient care [11]. Unfortunately, most PACS applications cannot share information with each other. Likewise, PACS applications may run on different hardware and operating-system platforms [12]. For these reasons, it is cumbersome and time consuming for physicians to obtain time-sensitive medical images from other departments. For example, a cardiologist who needs an image from radiology probably cannot access it directly from the cardiology department's PACS application. Instead, when doctors need to share images, they typically sign on to the other PACS application or view read-only CDs or DVDs that do not support full diagnostic manipulation and analysis [12].

Furthermore, the main task of healthcare IT organizations is to fulfill the productivity and workflow requirements of the changing healthcare workforce [13]. Today's clinicians work in a world of scarce resources, rising demand for healthcare services, and the emergence of new, patient-centered care models. Health workers are increasingly likely to be mobile, to work at multiple locations, and to face more complex demands for information access, analysis, and collaboration. They use rich graphics and video, and they need

information access at the point of care — whether that's at the bedside, in the home, or at a clinic or remote office. A high level of performance and mobility provides a basis for coordinated care delivery, and requires new levels of support and technology to enable secure, efficient, and timely access to critical healthcare information.

Cloud services (known in modern tech jargon as "the cloud") refers to a network of servers connected by the Internet or other network that enables users to combine and use computing power on an as-needed basis [14]. Each user does not have to purchase and maintain individual computing power. The cloud provides virtual centralization of applications, storage, etc. which can be accessed by any web-friendly device (computer, laptop, smart phone, tablet, etc.) virtually anywhere. Centralization gives the cloud service provider system-wide control over, for example, security and application upgrades, negating the need for installation of upgrades on individual devices. Typically customers pay for the amount of computing power they use (comparable to how we pay for electricity or other utilities). For the healthcare industry, cloud services represent an enormous opportunity. Storing, archiving, sharing and accessing images in the cloud allows the industry to manage data more efficiently and cost-effectively while overcoming many of the legal, regulatory and technical challenges that data requirements pose.

Hence the main concern of this study will be finding solutions for the above aforementioned factors so that healthcare organizations can get the advantages of cloud computing in efficient and affordable manner. Therefore, the research will intend to get answers for the following research questions.

I. Are the current technologies for medical imaging and sharing efficient?
II. What are the critical factors influencing the adoption of cloud computing in healthcare for medical image archiving and sharing?
III. Could it be possible to develop a cloud based framework that helps to adopt cloud computing successfully for medical image archiving and sharing?

1.3. Objective of the Study

1.3.1. General objective

The principal aim of this thesis is to develop a cloud based framework that helps to efficiently utilize the potential of cloud computing for the purpose of medical image archiving and sharing.

1.3.2. Specific objective

- Identifying the current technologies used in image archiving and sharing ICT service delivery strategy and efficiency.
- Examining the efficiencies of current technologies.
- Identifying factors that affect implementation of medical image archiving and sharing solution.
- Identifying services and service models appropriate in the cloud.
- Identifying tools and models appropriate for adoption
- Assessing cloud service providers by their services and pricing models
- Designing cloud computing framework that helps for successful cloud adoption in healthcare institutions.

1.4. Methodology of the Study

In order to achieve the specific and general objectives of the study and answer the research questions, the following research methods are used. Figure 1.1 shows design research methodology.

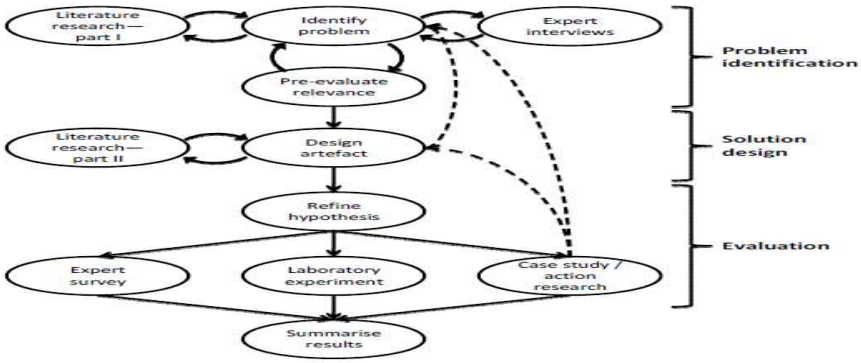

Figure 1.1 Design Science research methodology [10]

1.4.1. Literature review

Extensive review of acknowledged texts, standards documents, industry periodicals and white papers, analysts' reports and conference journals is done in order to have detail understanding on this research work. Different techniques and tools which are relevant for the current research are analyzed, modified and used from previous works.

1.4.2. Expert Interview

Different persons including physicians, radiologists, researchers, developers and healthcare IT specialists from public and private health care providers have been interviewed to understand the issue of current ICT utilization strategy, Effectiveness and efficiency of service delivery, and their recommendations for better service delivery was covered by the interview.

1.4.3. Expert Survey

The survey is done online to evaluate the design framework of medical imaging archiving and sharing solution around the world. The respondents were physicians, healthcare IT specialists and consultants. Questioner is attached at the appendix.

1.5. Significance of the Study

This research will allow healthcare providers to consider alternative ways of deploying ICT infrastructures for an efficient and effective medical image sharing. The study gives new insights to the officials and policy makers on how to invest ICT budgets in healthcare institutions especially for medical image sharing. The Proposed Hybrid cloud computing model and the presented implementation plan can be used as a baseline for the physical realization of the cloud. Additionally the study could be used as a baseline for further studies of this newly emerged ICT utilization strategy to be considered in different institutions.

1.6. Scope of the Study

The main intent of the study is to examine the current ICT service delivery strategies to support hospitals and imaging centers, to consider cloud computing in the field of medical image sharing. Finally, the researcher proposed cloud computing framework that could be used as a baseline for implementation of Cloud for image sharing.

1.7. Organization of the Thesis

The remaining chapters of this thesis are organized as follows:

Chapter 2 focuses on the literature review of the cloud computing and medical imaging. The first five sub sections are about cloud computing (definitions, characteristics, service models, delivery models, and enabling technologies) and while the rest two sub sections discuss about introducing cloud computing in healthcare in general and in medical image management in particular. Especially, on section 2.7 whole aspects of image sharing (types, benefits, prerequisites, barriers, current enabling technologies, and emerging technologies) are discussed. Furthermore, cloud adoption strategy is recommended in this chapter. This chapter ends by giving summary of all topics discussed earlier in this chapter.

Chapter 3 discusses the main issues (security, legal and compliance) in general and specific to healthcare IT systems (for both traditional and Cloud based). It provides the definition of security, challenges, vulnerabilities, requirements and best practice standard frameworks. In addition it discuss about legal issues in general and specific to healthcare systems. Furthermore compliance issues are discussed in the third sub section. The chapter ends with security recommendations and summary.

Chapter 4 On the first subsection of this chapter, a ranges of services that are provided by the Cloud providers are discussed. That means, which type of services are provisioned by which model (SaaS, PaaS, and Iaas). And how healthcare providers can utilize these services models is briefed in detail. The next subsection is about who are the service providers and what kind of platforms and pricing models are used in each CSP is discussed. World Cloud market leaders, like Amazon, Microsoft Azure and Google AppEngine are discussed and compared. Finally the chapter ends by presenting a comparative analysis of CSP.

Chapter 5 brings together all concepts discussed in the above three chapters in to a framework, which is used as a baseline for developers and organizations which decide to adopt a standard base cloud enabled medical image management solutions.

Chapter 6 presents evaluation of the framework by different experts. Here the pros and cons of the proposed framework is analyzed by the expert survey.

Chapter 7 summarizes the research, provides conclusions and discusses further areas of research.

CHAPTER TWO

2. Conceptual Discussion and Literature Review

INTRODUCTION

Technology has created a level playing field with the rise of telecommunications and the internet. This leveling has helped in creating emerging leaders like India and China who are leveraging favorable demographics with technology. Technology is often a savior during the downward economic cycles as it enables the creation of more efficient business models and ecosystems. The Cloud is one such phenomenon that has stirred up interests and investments in many parts of the world [15]. With it's new economic model, it removes the need for the organization to invest a substantial sum of money for purchase of limited IT resources that are internally managed by outsourcing to the third party service provider and pay per use. This may be especially advantageous for developing countries that do not have the technology, skilled personnel, or resources to create world-class ICT infrastructures.

While there is a strong case for the adoption of the Cloud, there are several challenges that need to be overcome [15]. The challenges that are raised are: trust, security, legal, compliance and organizational.

This chapter covers all about Cloud Computing and medical imaging. It begins by discussing the different definitions of cloud computing. The second subsection is about the related techniques to cloud computing, here relevant mutual and differentiating features are discussed. These features are the corner stone for developing cloud based systems. The characteristics of cloud computing follows next to related techniques which are basic to define common behavior and characteristics of cloud computing. The third section is about the different types of cloud computing that operate on different abstraction layers.

2.1. Cloud Computing

Over the years many organizations have invested in massive in-house computing capacities and specialized Information Technology (IT) staff around the world in order to support their primary business processes or to achieve a competitive advantage. According to [16] Porter and Millar IT create competitive advantage by giving companies new ways to outperform their rivals. Nowadays organizations are looking for IT to operate more

efficiently and help to reduce the overall costs. The concept of outsourcing has contributed to this development by transferring entire business functions to an external service provider.

A recent phenomenon in the domain of outsourcing is called Cloud Computing. “Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs” [17].

The first attempt at cloud computing were in 1999 when Marc Anderson founded the Loud Cloud Company. The company intended to be a managed service provider. It was the first company to offer services which are now called Software as a Service (SaaS) using an Infrastructure as a Service model (IaaS) [18]. The company does not exist today. In 2000 Microsoft launched web services as SaaS offering, followed in 2001 by IBM with their Autonomic Computing Manifesto [19][20] and in 2007 collaboration between IBM and Google launched research in cloud computing [21].

2.1.1 Definitions

So far, globally accepted definition of cloud computing has not been established. There are lots of definitions by academia, industry. However the definintion given by NIST is most widely used definition. In this research I used this definition. It goes like this

> *“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. This cloud model promotes availability and is composed of five essential characteristics and three service models and four deployment models”*.

This definition covers many perspectives and it is widely used around the world. The concept of this definition is represented diagramaticaly on figure 2.1. Figure 2.1. Shows *the framework of the NIST definition of Cloud Computing*

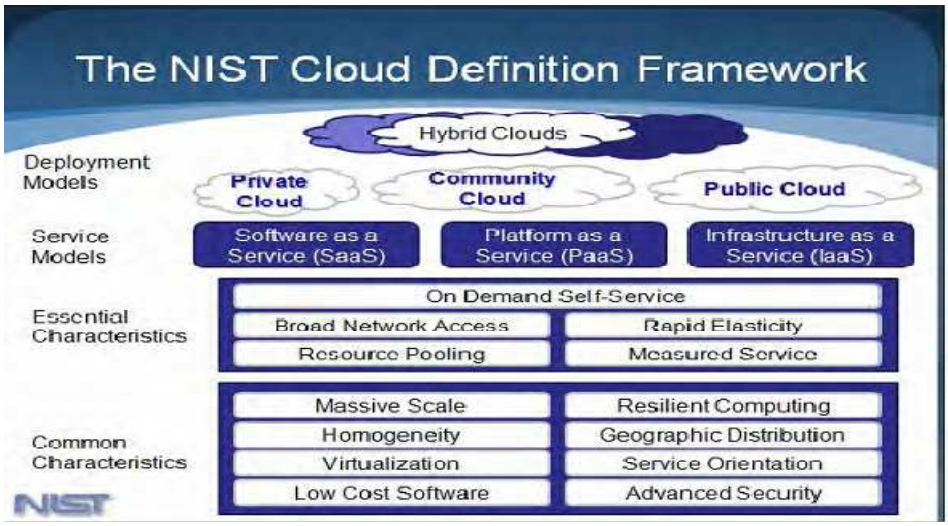

Figure 2.1: The NIST Cloud Computing Definition Framework [22]

2.2. Cloud Computing Characteristics

Cloud services are based upon five principal characteristics that demonstrate their relation to, and differences from, traditional computing approaches. Below I try to discuss each characteristic in detail.

2.2.1. Abstraction of Infrastructure

The computing, network and storage infrastructure resources are abstracted from the application and information resources as a function of service delivery. Where and by what physical resource that data is processed, transmitted and stored on becomes largely opaque from the perspective of an application or services' ability to deliver it. Infrastructure resources are generally pooled in order to deliver service regardless of the tenancy model employed – shared or dedicated. This abstraction is generally provided by means of high levels of virtualization at the chipset and operating system levels or enabled at the higher levels by heavily customized file systems, operating systems or communication protocols.

2.2.2. Resource Democratization

The abstraction of infrastructure yields the notion of resource democratization – whether infrastructure, applications, or information – and provides the capability for pooled resources to be made available and accessible to anyone or anything authorized to utilize them using standardized methods for doing so.

2.2.3. Services Oriented Architecture

As the abstraction of infrastructure from application and information yields well-defined and loosely-coupled resource democratization, the notion of utilizing these components in whole or part, alone or with integration, provides a services oriented architecture where resources may be accessed and utilized in a standard way. In this model, the focus is on the delivery of service and not the management of infrastructure.

2.2.4. Elasticity/Dynamism

The on-demand model of Cloud provisioning coupled with high levels of automation, virtualization, and ubiquitous, reliable and high-speed connectivity provides for the capability to rapidly expand or contract resource allocation to service definition and requirements using a self-service model that scales to as-needed capacity. Since resources are pooled, better utilization and service levels can be achieved.

2.2.5. Utility Model of Consumption & Allocation

The abstracted, democratized, service-oriented and elastic nature of Cloud combined with tight automation, orchestration, provisioning and self-service then allows for dynamic allocation of resources based on any number of governing input parameters. Given the visibility at an atomic level, the consumption of resources can then be used to provide an "all-you-can-eat" but "pay-by-the-bite" metered utility-cost and usage model. This facilitates greater cost efficiencies and scale as well as manageable and predictive costs.

2.3. Cloud Computing Service Models

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model," where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively — defined thus:

2.3.1. Software as a Service

In this delivery model a consumer uses the provider's application running on a cloud infrastructure as a service. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer

does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage. Examples of SaaS providers are salesforce.com, Netsuite and Oracle CRM on Demand.

2.3.2. Platform as a Service

In this delivery model the consumer is provisioned to deploy and develop his/her owned applications on the cloud infrastructure using compatible programming languages and tools supported by the cloud provider. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools (NIST Security). As in the case for Saas, the consumer does not have control of the cloud infrastructure; however he/she administers the created applications and its configuration preferences. For instance radiology department can deploy or migrate its legacy system on to the cloud provider's platform. In addition it can control the application and it's configuration preference. A few examples are Force.com, Google App Engine, Windows Azure.

2.3.3. INFRASTRUCTURE AS A SERVICE (IaaS)

In this delivery mode, the consumer has to provision two things, deploying and running applications. Which means the consumer uses the providers resources like, storage , processing, networking and other computing resources to run an arbitrary software. The deployed software can be application or operating system. As that of PaaS the consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

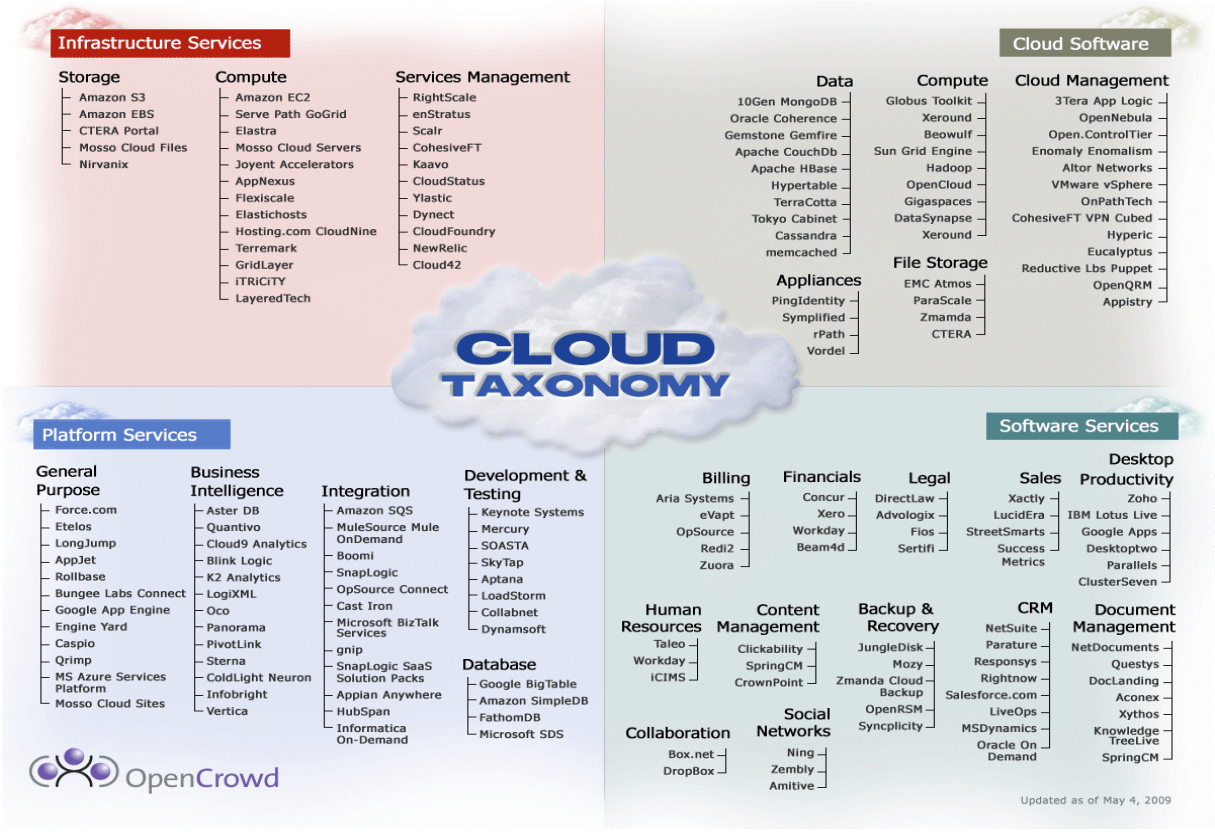

Figure 2.2 The Cloud Taxonomy (OpenCrowd, 2010)

2.4. Cloud Computing Deployment Models

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements:

2.4.1. Public Cloud

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. In this case a business, academic, or government organization, or some combination of them may be the owner of the infrastructure, as well as the one managing and operating it. In this model clients can choose security level they need, and negotiate for service levels (SLA). The first and most used type of this offering is the Amazon Web Services EC2. Figure 2.3 show the structural formation of public cloud.

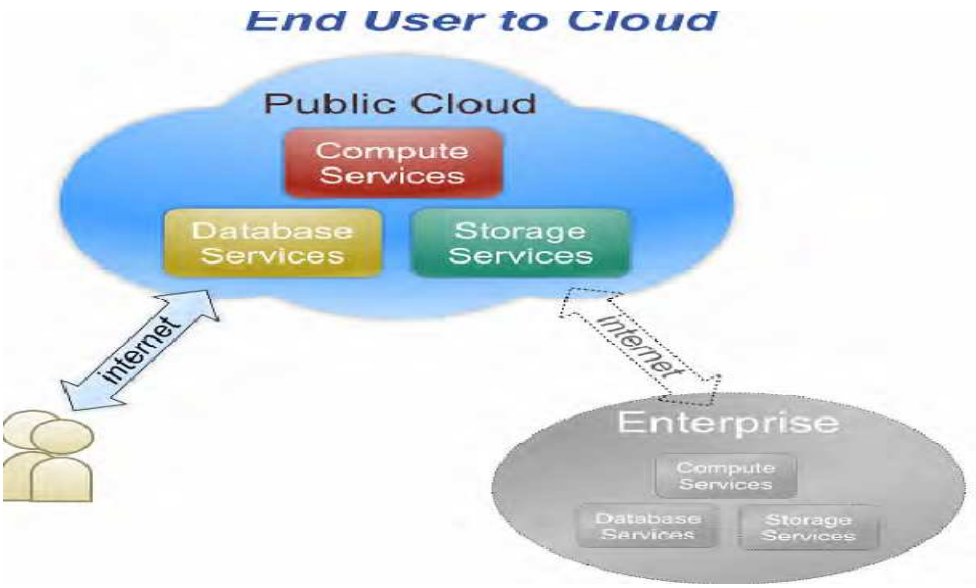

Figure 2.3 Public Cloud [30]

2.4.2. Private cloud

The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises. A private cloud gives the organization greater control over the infrastructure and computational resources than does a public cloud. Figure 2.4 shows the structural formation of private cloud.

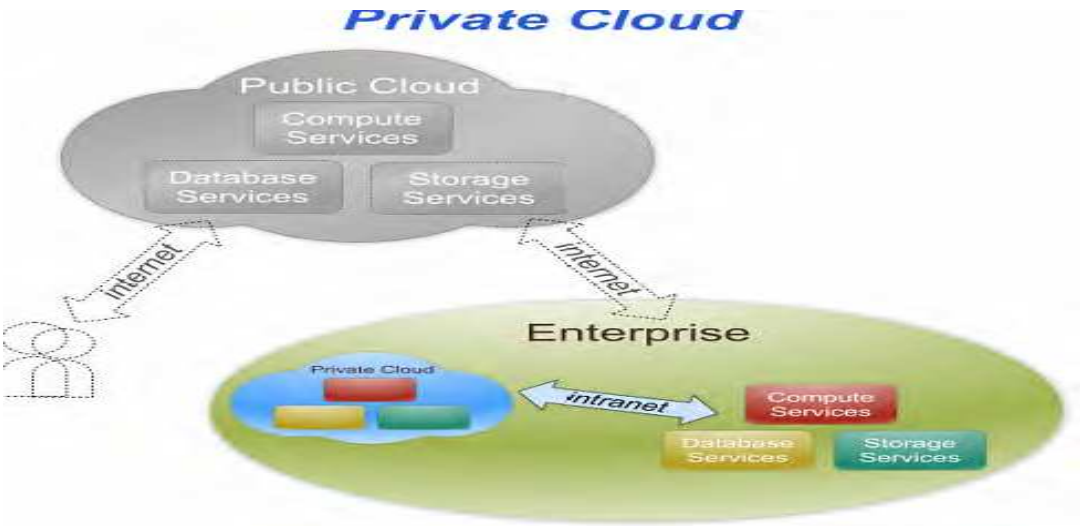

Figure 2.4: Private Cloud [30]

2.4.3. Hybrid Cloud

It is a blend of cloud-computing delivery models, most commonly a blend of a public cloud model with a private cloud model. Once an organization has made the leap in terms of leveraging a self-service interface with a service catalog, and automated service delivery behind that, adding an alternative sourcing option (an external service provider) for some services or some instances of services becomes easier. Figure 2.5 shows the structural formation of hybrid cloud

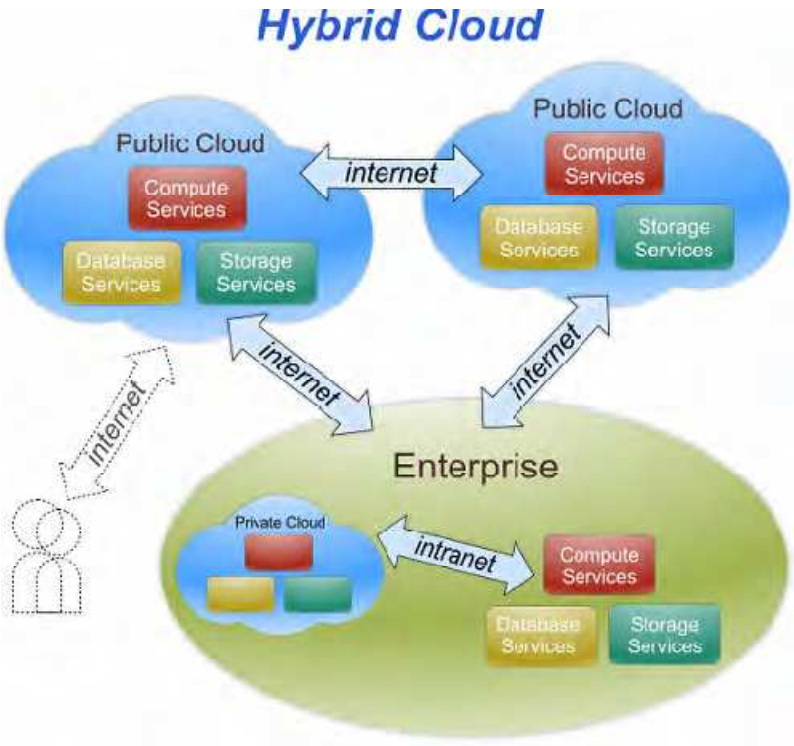

Figure 2.5: Hybrid Cloud [30]

2.4.4. Community Cloud

It is a pooled resource cloud that combines the resources of multiple community users [29]. The idea of community cloud is the similar to grid computing in resource pooling, however, they differ in management. Community cloud offers resources on demand to the users, while grid offers according to the plan. Figure 2.6 shows the structural formation of community cloud.

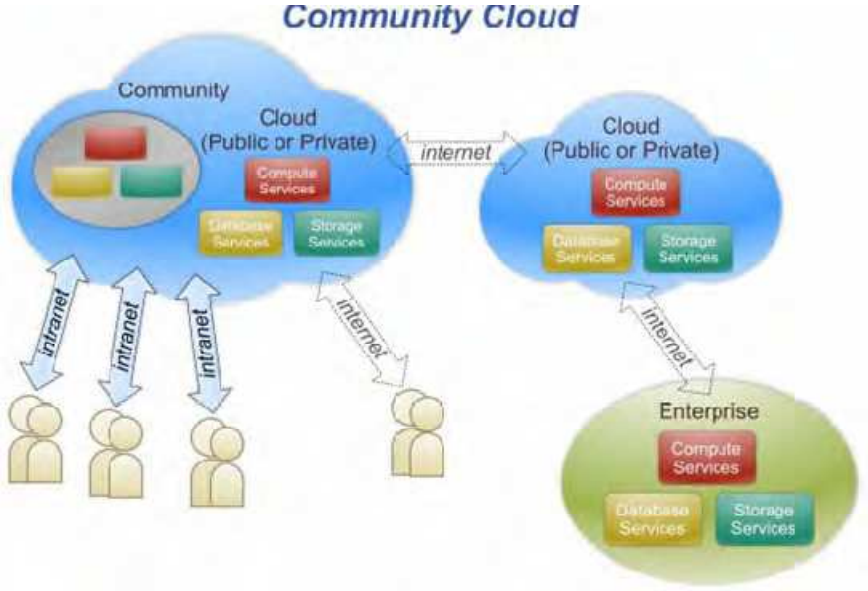

Figure 2.6: Community Cloud [30]

2.5. Related Technologies

These technologies are the key technologies underpinning the evolution and success of cloud computing. This is because these technologies paved the way for the platform from which cloud computing is launched. They provided the technology and infrastructure that cloud computing relies on. They also provided the theoretical and practical experiences which cloud computing capitalizes on for its success and adoption in business organizations. These technologies are Grid, cluster, virtualization and SOA computing, ancestor of cloud computing.

2.5.1. Grid Computing

It is a form of distributed computing that implements a *virtual supercomputer* made up of a cluster of networked or internetworked computers acting in unison to perform very

large tasks. Thus grid computing offers to cloud the capabilities for resource sharing, heterogeneity and ability to de-centralise resource control [17].

2.5.2. Computer Clusters

A cluster is a set of multiple interconnected computers. Classifying a set of computer as a cluster requires software that makes that computers work together. Couple of very reason for clustering is performance and high availability, which means a fault tolerant hard and software configuration. Performance clustering is a natural way to add performance if one node configuration is not enough. High availability configuration adds reliability by avoiding a single point failure. These configurations are also used together in an active cluster configuration.

2.5.3. Virtualization

Virtualization allows a complete separation of operating system from hardware. This is possible by allowing the host operating system, the system that runs on the hardware, to create a virtual environment that can run any machine code that the hardware supports. In cloud computing sense, this allows splitting of big multi core machines with huge amounts of memory in to smaller units in a controlled fashion. This means that a cloud computing provider can allow users to split an environment to a desired size unit. Virtualization takes care that this smaller units do not take more resources than they are supposed to. This allows for a cloud computing provider to offer a stable quality of service to the customer.

2.5.4. Service Oriented Architecture

SOA is a standard way for creating connections for enterprise systems. These systems offer their capabilities as services. So service oriented architecture and web services enables offering of cloud computing services as web services accessible via the Internet, also SOA makes it possible for cloud services to be available in multiple platforms [31].

2.6. Cloud Computing and Healthcare

A typical healthcare ecosystem consists of the providers namely doctors, physicians, specialists (those who work out of hospitals, clinics, nursing homes, etc.), payers (health insurance companies), pharmaceutical companies, imaging centers, IT solutions and services firms, and the patients [15]. In the context of technology usage or information management, the healthcare ecosystem handles a major key process, the healthcare provisioning process.

This process manages massive information loads and as such relies heavily on computing resources

2.6.1. Health care IT

IT systems for healthcare can bring lots of advantages in many ways, since this sector depends very much on information. In terms of computer usage, hospitals are even seemed to be outdone by the public administration: collection of data is mostly done on paper and is seldom fed into a computer system. The little data that does reach a computer system usually stays in isolated systems, such as a database for lab analysis values. However, especially in the healthcare domain, a closer integration of systems and a use of computer-aided data processing could be very helpful. Like almost no other domain, quality of healthcare depends on the availability of data. When a clinical decision has to be made, all the required information has to be available. [32]

Integration of Information and Communication Technology (ICT) enables faster feedback, remote monitoring and analysis and above all ensure mobility of individuals across countries. Neither these benefits come for free, nor can they be achieved without proper knowledge of the pitfalls and complexities specific to the domain of healthcare. This subsection tries to show health care challenges and available information technologies that help to address the challenges.

2.6.2. The current role of technology in healthcare

The healthcare industry has been leveraging technological innovations for decades to provide superior quality services to patients [15]. Medical technology-based devices and equipments such as Computed Tomography (CT) Scanners, Diagnostic Sonographic Scanners, Magnetic Resonance Imaging (MRI) Scanners, remote monitoring devices, health and wellness-check devices, etc. have helped in diagnosing health problems without the need for expensive and hazardous surgeries. Most countries invest significantly in medical technologies and this market is growing rapidly.

Information and Communication Technology (ICT) has performed a major role in digitizing and communicating patient information, leading to rapid patient diagnosis which further leads to faster time-to-treatment and superior overall health services [15]. Stakeholders in the healthcare industry have benefited by ICT applications in terms of efficiency and quality.

Communicating digitized patient information is typically done through a system like 'Telecare'. Volumes of patient data are transformed into information for decision-support through HIT applications and systems that are crucial for providing successful telecare services. Typically, healthcare providers make use of systems like Hospital Management Information System (HMIS), Picture Archiving and Communication Systems (PACS) , Electronic Medical / Health Records (EMR /EHR) system or Personal Healthcare Records (PHR) system to facilitate clinical workflows in order to provide telecare services.

2.6.3. Challenges in the Present healthcare

The digitization of clinical data, particularly in the form of EMR / EHR or PHR, and the automation of back office operations, will generate lots of data. As a result managing this data is not an easy task. As such, it becomes mandatory for them to put a robust network of IT systems in place [15]. Maintaining such a robust network of systems in-house increases the overall operational costs. The current ecosystem faces several challenges that demand technological advancement for sustaining itself in the future.

- **Ageing population driving the need for advanced, cost-effective technology**

  Patient care for the elderly is necessitating advanced technologies and expensive healthcare services. This is increasing patient care provisioning costs for healthcare service providers. With the generation of large amounts of health data or information, huge IT storage infrastructure and backup solutions would be required. The use of technologies such as mobile phones, PDAs, laptops, iPads, etc. to reach out to patients in remote locations may not be a cost-effective solution. The back-end technology infrastructure needed to provide such services is expensive to source and maintain

- **Inadequate government spending**

  Government spending on healthcare has been largely inadequate in developing countries. This has led to the poor development of the public healthcare infrastructure. As appropriate funding is unavailable, governments and healthcare providers need to focus on sourcing / developing and deploying cost effective solutions that include technologies that could aid in providing healthcare to the masses.

- **Shift in disease burden from acute to chronic diseases challenging the limits of the traditional IT environment**

  There is a significant shift in the disease burden from acute to chronic diseases in developing countries. According to a World Bank report, the incidence rate of cancer, diabetes, obesity and heart disease in developing countries are nearing those of developed nations, and these chronic 13 diseases would be the leading cause of death in developing countries by 2015 . With the spread of the disease burden globally, there is expected to be an increasing need of resources, both hum an and material, to address this need. This is likely to further add to the additional information management infrastructure requirement that can raise healthcare provisioning costs. Deploying advanced technology efficiently and cost effectively would be essential to address the growing demand for healthcare facilities in the remotest of areas. Innovation in the technology deployment is critical to meet this demand.

- **Workforce shortages and migration of skilled labor affecting specialist availability**

  Healthcare providers in developing countries are also struggling to maintain a well-trained and committed workforce. There is a huge mismatch in terms of the disease burden and resources required to handle them in these countries. Moreover, lower salaries, lack of better career prospects for healthcare professionals in developing countries is driving brain drain and creating a demand-supply gap. As this gap widens, accessing superior medical expertise would become expensive, further increasing healthcare costs.

- **Changing regulatory framework forcing digitization of health records to handle information efficiently**

  At the core of Healthcare Information Technology (HIT) applications is the management of patient records. Digitization of these or converting them to Electronic Health Records (EHRs) offers several important benefits to all stakeholders. Realizing the potential of cost containment by deploying EHRs, several countries have slowly started implementing HIT policies, making EHRs mandatory.

  Among the various geographies, Europe currently is a leader in health IT and EHR adoption followed by Asia-Pacific and the Americas. Countries like Australia,

Canada, Denmark, the UK, New Zealand, the Netherlands and more recently the US have implemented EHRs, where the governments have mandated its adoption. In Canada there is a public-private partnership in the implementation of HIT and EHRs.

Though the startup costs are high, EHRs can provide long-term solutions in delivering cost-efficient healthcare services for developed nations. In developing countries like India, there is no particular law or regulation mandating adoption of EHRs and the healthcare industry is unorganized to a large extent with minimum collaboration. In such cases, large-scale adoption of HIT and EHRs may not be a feasible option. Rather, they could first focus on localized usage of EHRs within their own network of hospitals and try improving other areas such as procurement, supply chain management and resource management.

2.6.4. Cloud computing in the health sector

The healthcare industry is evolving while grappling with several socio-economic and technological challenges along with the need to drive down HIT costs. A solution to this problem could be sought by moving to the Cloud [15].

Managing massive clinical data or EHRs requires heavy capital expenditure for sourcing and maintaining the IT infrastructure needed to store, transfer, retrieve, modify or print data and reports. At a state or a national level this could mean the storage and management of thousands of terabytes of data. All of this can be done more efficiently and at minimum costs if the data is moved into the Cloud.

The Cloud is a paradigm shift in HIT which enables stakeholders to focus more on their core competencies. In the case of the healthcare industry, it would involve the provisioning of healthcare products and services to patients by physicians, clinics, pharmacies, public health organizations, and payers. Providing a range of services across the entire spectrum of care would require the ability to scale application workloads, collaborate and share information and at the same time ensure that patient information is authentic and secured, and available anytime, anywhere. It would also mean the changing of business models, automating processes, streamlining workflows, and consolidating IT assets.

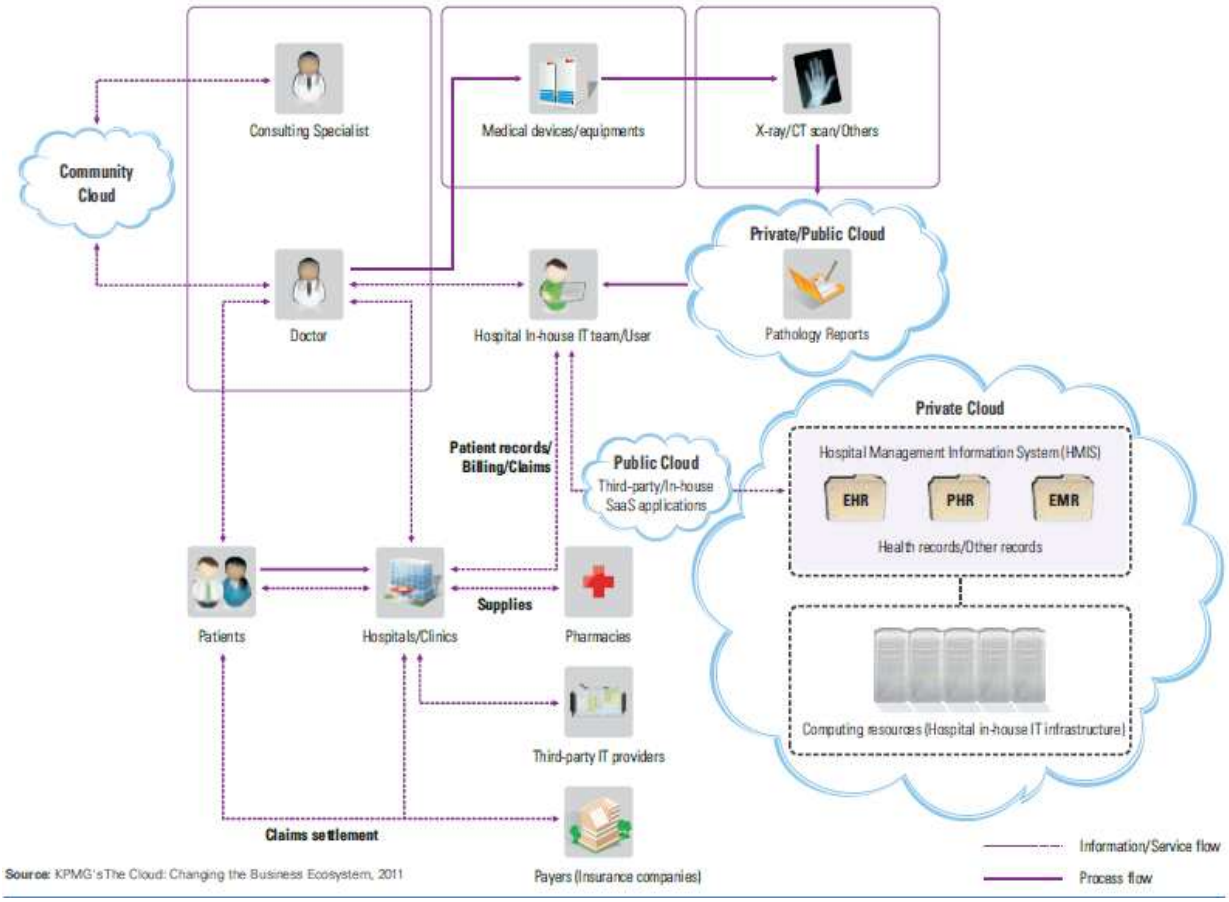

Figure 2.7 Paradigm shift in healthcare cloud ecosystem [15]

2.6.5. Benefits of Health Care Service in the Cloud

The Cloud is an IT deployment model that today's HIT departments could consider an investment towards developing a fully optimized health record and service management system.

Doctors or physicians could use medical appliances in their clinics to capture patient information and transfer it through a web-based SaaS application hosted in the Cloud (public or private) managed by the Cloud service provider. Applications would encrypt and de-duplicate patient information prior to transmitting the same into the Cloud. Patients and doctors could access the records securely by exchanging secure electronic keys or third-party security devices similar to the way secure credit card transactions occur over the internet.

In a private Cloud scenario, hospitals could transmit and store data in a secure fashion between their affiliated physicians or other member hospitals through Single Sign On (SSO)

access mechanism for easy and rapid access to information. In this way, hospitals can reduce their IT infrastructure burden and overall management cost.

In a public Cloud scenario, outpatient diagnostic centers can share results through the public cloud in a similar fashion like the private Cloud. Delivering services via SaaS applications in a public Cloud is also prevalent in physician offices. Similarly, drug manufacturers can make use of computing resources via cloud and reduce costs drastically using IaaS model. Every stakeholder in the healthcare ecosystem stands to benefit from the Cloud.

- **Pharmaceuticals/Drug manufacturers**- Drug manufacturing utilizes heavy IT infrastructure for its Research and Development (R&D) needs. The IaaS model could provide a drug manufacturer with On-Demand computing resources to perform drug research analysis, eliminating the need to retain computing capabilities and related IT expertise in-house.
- **Hospitals**- Using in-house or third party SaaS applications that are housed in the Cloud, patients an provide access to their health history and information so that hospitals can streamline the admissions, care and discharge processes. Hospitals can connect to their own web portals and access patient data stored in the Cloud.
- **Physicians**- With the Cloud, people can provide their health history and information to their physicians anywhere, anytime, including data uploaded from health and fitness devices, to help physicians make more informed decisions.
- **Pharmacies**- People can administer or manage their prescriptions and associated information such as dosage, amount and frequency, and provide this information to their healthcare provider.
- **Laboratories and imaging centers**- Patient's diagnostic results can be transferred via suitable Apps onto Cloud-based platforms, e.g. Google Health or Microsoft Healthvault. This eliminates the need for in-house storage and helps retain historic information in a systematic manner. Healthcare providers can access these results with the patient's permission, to help them make more informed health decisions.
- **Application Providers**- Health and wellness companies can design and deliver health and wellness solutions compatible with Cloud platforms to offer rich user experiences and ease of managing users' sensitive personal health information.

- **Device manufacturers**- Health and fitness devices can be designed to work with Cloud platforms and Apps, so users can upload device data and share it with their doctors and families.
- **Payers**- Health payers can offer their members with innovative tools compatible with their chosen cloud platform to provide value added services by giving members' access to more health information, and thereby increasing the effectiveness of their care management programs which can help reduce claims costs. Payers can enable plan members to add health data to their records in the Cloud and provide it to their healthcare providers.

In case of the adoption of the Cloud, the responsibility of managing the underlying IT infrastructure to provide the aforementioned benefits lies with the Cloud services provider.

2.6.6. Risks of health care services in the cloud

Though the Cloud in healthcare provides several benefits for all the stakeholders of the industry, it has its own set of challenges. Some of these include security, privacy protection, disaster recovery, regulatory, governance, and the reliability of the Cloud.

P**atient information security and privacy protection**

The primary reason the healthcare sector would offer resistance to making a move to the Cloud would be patient information security and privacy protection. Patient information across countries has been under the purview of legal frameworks e.g. the data privacy requirements legislated through HIPAA (Health Insurance Portability and Accountability Act) privacy rules in the US. HIPAA provide federal protection for personal health information. Similarly, the European Union has several directives pertaining to data protection. In many countries, the patient's Protected Health Information (PHI) cannot be moved out of the country of origin. Finally, the patients themselves would be concerned about the security of their personal data. The Cloud for healthcare would need to have a very strong data protection and privacy system in place to gain large scale acceptance / adoption in the marketplace. Therefore, the public Cloud environment may not be suitable for many healthcare applications. The Cloud's vulnerability to security breaches is similar to any traditional infrastructure environment. The adverse impact is, to a large extent, due to sensitivity of the information involved. A preferred solution to tackle the issue would be the use of a private Cloud coupled with secure access protocols and systems. Several Cloud

service providers have come up with data and privacy protection equipments and tools; however, the industry is still skeptical of their effectiveness.

Interoperability and standardization

The Cloud offers the ability to shift all data / information onto systems and storage platforms provided / managed by Cloud service providers. At times, it may so happen that health records of patient stored, in the Cloud by his personal physician, might be needed to be accessed by the hospital that the patient was referred to. In such cases, the hospital should be able to access a patient's health records stored on a different Cloud. At the same time, it is also expected that here would be a large number of software and applications that would exist in a Cloud. In order to ensure efficiency and optimum utilization of resources, it would be ideal if there is a high degree of interoperability and standardization between healthcare solutions for the Cloud.

Unifying the Cloud is an ideal state, but quite a distant goal to achieve, considering that there are several standards existing today. At the same time, there are also a number of Cloud standardization groups:

- Distributed Management Task Force (DMTF)
- Cloud Computing Interoperability Forum (CCIF)
- Open Grid Forum's 'Open Cloud Computing Interface Working Group' who is developing standards for managing the cloud.

Almost all industry majors like AMD, Broadcom, CA Technologies, Cisco, Citrix, Dell, EMC, Fujitsu, HP, Hitachi Limited, IBM, Intel, Microsoft, Novell, Oracle, Rackspace, Red Hat, and VMware are members of such groups and could accept one or the other standard. But it would be difficult to convince everyone in the business to accept a single interoperable / standardized system.

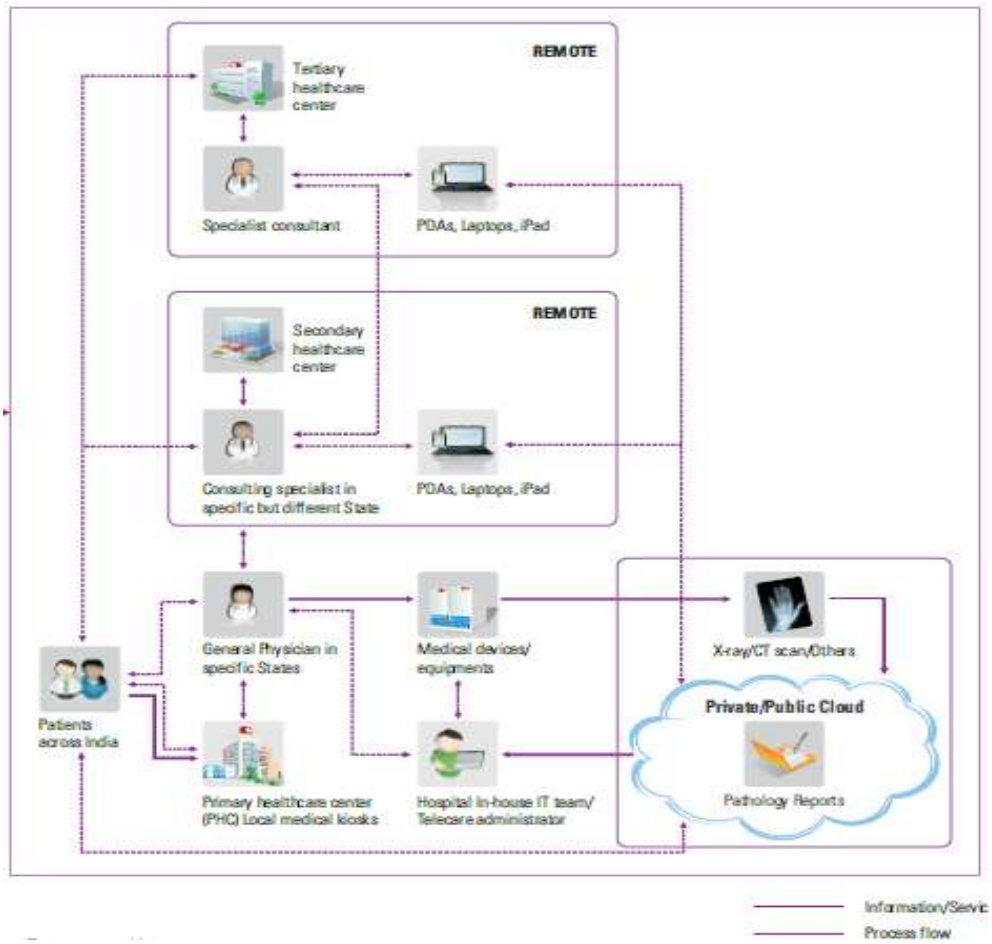

Figure 2.8 Illustrative model of the Tele-Cloud [15]

2.7. Cloud Computing for Medical Image Sharing

2.7.1. Medical Imaging

Medical imaging is a non-invasive technique used to create internal images of the human body for clinical or medical science purposes (i.e. “virtual dissecting” of the human body) [33]. It’s genesis for medical diagnostic purposes starts a century back, 1895, to the discovery of x-rays by a German physicist Wilhelm Konrad Roentgen. In conventional film radiography the radiographic film detects, stores and displays the radiographic information. That means radiographic film was the most important medium for the acquisition and archival of diagnostic images. In digital radiography X-ray detectors and computers perform the acquisition, archival and display of the radiographic information.

Today, in many settings clinical data and images are available from any location in the world right after the acquisition for the patient and healthcare professionals upon them being given the relevant entitlement. This is enabled by the digitalization of medical images and related data, common standards, secured data exchange platforms, and RIS, PACS and EPR integration [34].

2.7.2. Data and Workflow sharing

Data sharing in medical imaging enables entitled healthcare professionals, administrators and citizens to simultaneously and asynchronously access medical images and image related data, with this sharing not being dependent on the place or time.

2.7.2.1. Evolution of data sharing

Along with the development of interoperability standards in medical imaging the integration of databases evolved in consecutive stages. Data sharing between healthcare providers started with point-to-point integrations followed by simultaneously accessible central databases, and most recently, by many-to-many connections [35][36].

Point-to-point connection allows healthcare professionals located in one institution access to medical data collected and stored in another institution. In this example, two organizations would agree about the technical standards for data sharing, organizational and security rules, *etc*. There can be more organizations that are connected to the same database and use the data simultaneously. However, technical interoperability and contractual relations remain bilateral between two healthcare providers. Every new connection demands new agreements between collaborating parties.

To support simultaneous access to different databases, a more effective many-to-many approach is used [37]. This setting uses a central integration platform which communicates with different databases. Each healthcare organization has only one integration to the central platform. There is no need for multiple agreements between different healthcare providers and databases. All data exchange issues are covered using technical integration and by a contract between the healthcare provider and the integration platform.

Many-to-many database integration is achieved by using the Integrating the Healthcare Enterprise (IHE) standard profiles, particularly cross-organization data sharing profiles like the Cross Enterprise Document Sharing (XDS).

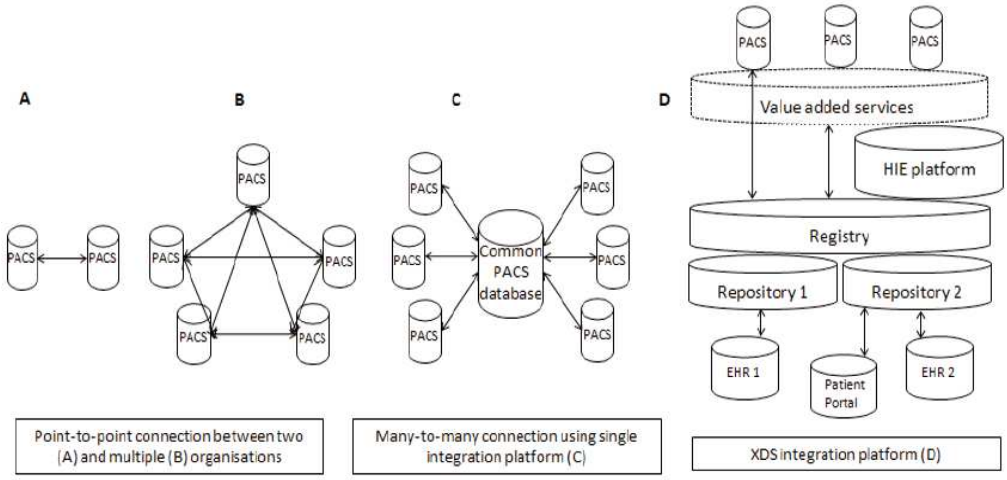

Figure 2.9.Evolution of database integrations. Database integration started from point-topoint connections followed by many-to-many connections. XDS integration profile allows sharing of different health related data all over the healthcare community [38].

2.7.2.2. Shared Workflow

Shared workflow is a healthcare process management model which allows a multi-site approach to the defined clinical or healthcare administrative process. Shared workflows utilize shared medical databases, standardized data and data exchange profiles, and related legal, security, financial and organizational rules.

Despite of the availability of shared databases, there are still two types of workflow settings in healthcare organizations – linear workflow and shared workflow. Workflow sharing is implemented either internally in the healthcare enterprise or across organizations. The focus of this paper is to explore and discuss cross-organizational workflow sharing.

Linear workflow

In linear workflow, the imaging and reporting is performed according to agreed and fixed actions along the reporting process. A reporting work list is pre-defined and images are assigned to the given radiologists or departments. The reporting process is built in consecutive steps and if the work list is fixed, the changing of it demands manual interference.

Cross-organizational shared workflow

In cross-organizational shared workflow settings, referral letters, images or reports originate from different organizations. They are organized according to agreed process rules and combined to create a virtual work list. Depending on the purpose, the work list is created either to fulfill the reporting service agreement, or to follow the availability of radiologists or even workload, *etc*. Compared to linear workflow it allows automatic capacity management (ACM) and forms a seamless and very effective reporting process.

Medical imaging shared workflow is set-up using many-to-many teleradiology settings and/or using global work lists. Global work list can be implemented on a many-to-many e-marketplace type of platform and supported by dynamic routing of images or relevant documents.

The global work list approach enables sharing of the workflow by implementing standardized software and platforms for sharing. It allows creation of global work lists which are extending the limits of a single healthcare enterprise. With a global work list in radiology, it is possible to avoid manual management of who reads what and where. Point-to-point connections which support mainly linear workflow can be replaced by matrix type of many-to-many connections.

Radiologists serving healthcare facilities can accomplish remote reading and reporting across different hospitals or large geographical areas. This is an excellent way to increase reporting quality or balance workload locally or regionally between sites with different RIS or PACS [39]. Manual workflow management can be replaced with ACM.

There are examples of the implementation of inter-organizational shared workflows and global work lists in different places in the World. In the Western Norway Health Care Region (Helsevest), the XDS-based communication platform was used to integrate 4 different RIS and 5 PACS solutions within 15 hospitals and several private radiology units [36]. In North America, similar shared workflow implementations are in commercial use. Companies like Telerays or Virtual Radiologic in the United States (USA) and Real Time Radiology in Canada integrate hospitals, imaging centers and radiologists to work together [40][41][42]. Also e-marketplace types of brokering services are evolving.

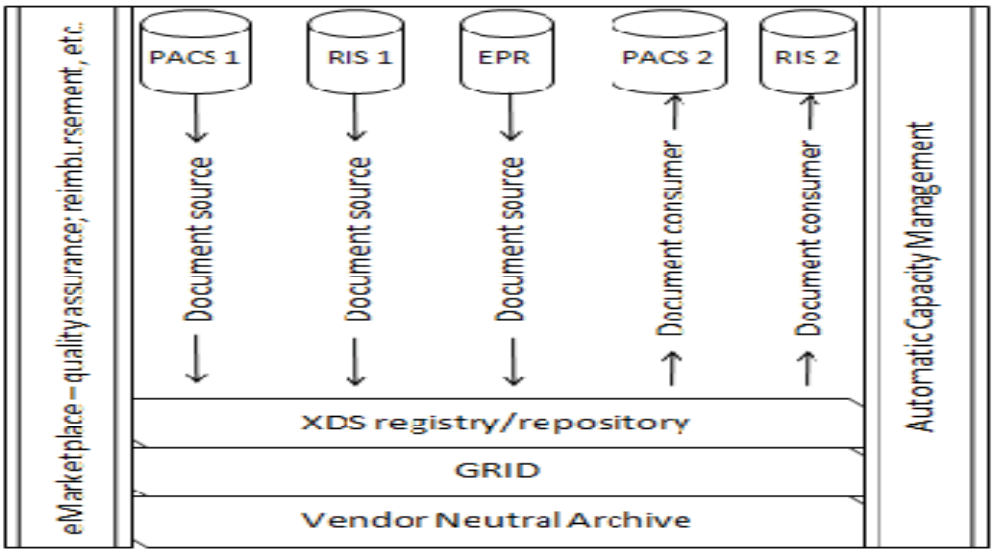

Figure 2.10 Shared workflow based on XDS profile and shared databases [38].

2.7.3. Benefits of Image Sharing

Any new method or model implemented in healthcare must provide clear evidence of benefits for a patient and/or public health [43][44]. It also has to be accepted by healthcare professionals. The main expectations are that the new proposed service increases safety, quality, accessibility and efficiency of the healthcare service and that the cost of the delivered service remains in the budgetary limits. In addition to the healthcare provider, the citizens and society must benefit from the innovation in healthcare, though the benefits frequently appear through different mechanisms.

2.7.3.1. Benefits for the radiology community

Pervasive and simultaneous access to the images, clinical data and processing functions increase the quality and effectiveness of reporting [45]. For the radiologist, medical data and image sharing across organizations opens simultaneous access to the relevant clinical data, referrals, prior images and reports, and current exam. This makes the radiologist more informed about the patient´s actual clinical situation. There is no longer a need to make repeated exams because images can be retrieved from other storages. The above-mentioned features support radiologists to make comprehensive interpretations of imaging findings.

Sharing of image information with other partners provides the opportunity for the radiologist to receive relevant feedback to the report or image quality and also share the best imaging practices with colleagues [46].

Use of dedicated tools over the Internet increases not only the diagnostic quality of radiologists' work, but these tools also help develop imaging interpretation skills and knowledge of clinicians, including improved communication with patient [47]. Image interpretation becomes a more integral part of daily clinical work along the patient care pathway.

2.7.3.2 Benefits for the healthcare provider

The benefits for healthcare institutions includes improving reporting capacity, shortening reporting times, using the opportunity for second opinions, and highlighting shared services as a reference for the hospital to attract patients.

The possibility to separate imaging from reporting leads to the consolidation of operations, especially regarding ambulatory imaging services and imaging in geographically remote areas. Both RIS and PACS services can be performed virtually allowing for new workflows based on sub-specialty, the availability of resources, urgency, or other clinical features. Searches of large, complex and distributed repositories of data can be completed locally and time efficiently.

From the economical point of view, shared databases and workflows lower exploitation costs through universal and centrally upgraded applications [48]. Also, scalability in a universal application guarantees high reliability. With shared databases and workflow, it allows the administration of healthcare providers to gain an overview of imaging methods and patient groups through the RIS, PACS and EPR and use this information to estimate the profile and cost
of imaging for specific radiology units or healthcare organizations.

2.7.3.3 Benefits for the society

Usually digitalization of the healthcare processes generates intangible benefits for the patient and community. An overall improvement in imaging management leads to a more informed and optimized use of imaging methods, thus decreasing overall healthcare costs. The benefits for the society also include benchmarking of healthcare providers leading to the

increase of effectiveness and quality, improved planning of resources and optimization of investments at the regional or national level. Benefits derived from the quicker access to imaging and treatment are: increased productivity, fewer disability and sick leave payments, more years of healthy life, quicker return to labor market, *etc*.

2.7.3.4 Benefits for the patient

For the patient, the most important change in using the shared database is the opportunity to become more involved in the imaging process [49]. A patient has access to their own medical data and images, collected and stored in different health care institutions during multiple visits to various physical locations [50]. This improves patient´s knowledge about their own health condition, previously performed exams and potentially avoids unnecessary radiation exposure of the patient caused by not needing to duplicate the taking of radiological images [49][51]. It also helps in planning of time and other resources in case an imaging procedure is needed.

Better informed and treated patients can return to their normal lives much faster. Consequently, in addition to improving the quality of patients' lives, this also has a positive economic effect on the state through increasing tax revenue while decreasing sick leave costs [39].

A referring physician is able to forward relevant referral letters and previous imaging results directly through the shared database, eliminating the need to see the patient in person.. The time needed to visit doctors will decrease as the number of required visits decreases due to the availability of shared information. It also has been shown that more transparent information flow leads to better communication between the patient and the physician [47].

2.7.4. Prerequisites for data sharing and shared workflow

2.7.4.1. Digitalization of medical images and related data

For data sharing and implementation of shared workflow, analogue film and text must be replaced by digital images, text and numeric data. This prerequisite is valid for every step of the clinical pathway. Lack of digitalization of all related images and clinical data leads to inefficiencies in the seamless flow of imaging data and hinders sharing of information [45][52]. Digitalization of medical images is achieved by converting analogue signals produced by different imaging modalities into computer processable digital values [53].

PACS is used to acquire, store, query, retrieve, display and process medical images and associated data originating from different imaging modalities. PACS integrates these sub-systems by digital networks and software applications [53]. It allows effective communication, for patient care, of DICOM and non-DICOM images. As a separate medical imaging technology, it is a prerequisite for image sharing and shared workflow. PACS provides a platform for a single point of access for images and related data and also integrates images from other healthcare information systems.

To achieve digitalization of the whole imaging pathway, digital images should be accompanied by patients´ digital data, including administrative data. For medical documentation, the most widely used interoperability standard is HL7. It provides a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical activity and the management, delivery and evaluation of health services [54]. HL7 covers a wide range of healthcare processes while DICOM concentrates mainly on medical imaging and the related exchange of data.

Today the integration of different healthcare information systems has evolved to the enterprise and cross-organizational level. For effective image communication, PACS installations now serve multiple hospitals and large geographical areas.

2.7.4.2. Standards and standard profiles

Standards in medical imaging specify values, rules and guidelines to achieve optimal, continuous and repeatable image processing results. Standards are approved by a recognized international or national standardization body and made available to the public [55]. In medical data sharing, the most commonly used standards are DICOM and HL7. These standards are used for image and health related data communication.

The two goals of standard profiles are to describe rules on:

1) How to use standards in a coordinated way for data sharing between different clinical databases; and
2) Implementation of the most optimal clinical workflows [56].

The IHE has become one of the main standard profiles used by healthcare professionals and the healthcare industry. It is the standard profile that uses DICOM, HL7,

Organization for the Advancement of Structured Information Standards (OASIS), security standards, *etc*.

Standards and standard profiles enable healthcare professionals from different healthcare domains or geographical regions to simultaneously use different databases and to share workflows to achieve the best clinical and administrative result.

2.7.4.3 Integrating the Healthcare Enterprise (IHE)

The IHE profiles were established to improve health related digital data sharing. IHE profiles were formed in 1997 by the common initiative of healthcare professionals and the healthcare industry. The IHE promotes the coordinated use of established standards to achieve specific clinical goals [56]. The aim is not to develop new integration standards but define integration rules that describe how to use and follow standards already in use [57]. The IHE does this via a description of technical frameworks for the implementation of established messaging standards. It is also a forum for coordinating and testing integrations of computer systems in healthcare.

IHE provides integration profiles, every one composed of several actors and transactions. The IHE actors and transactions are abstractions of the real-world healthcare information system environment. While some of the transactions are traditionally performed by specific product categories (e.g. HIS, Electronic Patient Record, RIS, PACS, Clinical Information Systems or imaging modalities), IHE intentionally avoids associating functions or actors with such product categories. For each actor, the IHE defines only those functions associated with integrating information systems. The IHE definition of an actor should therefore not be taken as the complete definition of any product that might implement it, nor should the framework itself be taken to comprehensively describe the architecture of a healthcare information system. The reason for defining actors and transactions is to provide a basis for defining the interactions among functional components of the healthcare information system environment.

In radiology, the IHE supports data exchange between different modalities and information systems according to defined clinical needs, workflows or planned services [58]. However, in addition to radiology, the IHE extends to many other clinical and operational fields and intends to support communication among different modalities, clinical subspecialties and healthcare user groups.

2.7.4.4 IHE standard profiles for Document and Image Sharing

As described above, to standardize the communication of images and related data across healthcare organizations, there is a need for system architecture and guidelines that specify conditions for data sharing. This issue is addressed by the following profiles, Cross Document Sharing (XDS), Cross Document Sharing for Imaging (XDS-I), Cross Community Access (XCA), Cross Community Patient Discovery (XCPD), Cross Document Workflow (XDW). Each profile is discussed in detain below.

Cross Enterprise Document Sharing (XDS) profile

It has been developed as an IHE information technology infrastructure profile that manages the exchange of documents that healthcare organizations have decided to share. From a single point of entry, XDS profile makes it possible to use patient medical data stored in different archives and managed by diverse applications.

The XDS profile defines a set of actors and transactions which allow documents to be registered in a single central registry, for them to be queried and also retrieved. It registers and shares documents between healthcare enterprises. The XDS allows the healthcare provider to share medical data without replacing the existing local or regional legacy information system or infrastructure [50].

The sharing of documents is limited to a defined group of organizations. This group of healthcare organizations is named the XDS Affinity Domain and is defined as a group of healthcare enterprises that have agreed to work together using a common set of policies and common infrastructure. This group does not follow any geographical or regional definition.

The XDS profile uses a document registry to capture the metadata about a document, including a pointer to the location of the document in a repository. It separates metadata and the actual content. This allows XDS to support a wide range of documents. Logical separation simplifies document exchange and enables existing information systems to use a wide variety of document formats (PDF, HL7 CDA, simple text documents) [57].

A healthcare IT system can act either as a document source or as a document consumer. In case of acting as document source, the provider archives a document in a repository in a transparent, secure, reliable and persistent manner, and registers it in the central document registry to allow for retrieval request. In case the healthcare organization is a document consumer, the healthcare organizations IT system queries the data about a

particular patient from the document registry, and according to the profiles describing the document properties, finds, selects and retrieves it from the repository where the document is archived [57].

To deal with patient privacy and consent issues, there is a Patient Care Coordination profile called Basic Patient Privacy Consents (BPPC) that enables XDS Affinity Domains to be more flexible in the privacy policies that it can support. BPPC provides mechanisms to record patient privacy consents, enforce these consents, and create Affinity Domain defined consent vocabularies that identify information sharing policies [59].

The XDS also demands the use of the IHE ATNA (Audit Node and Node Authentication) profile. The ATNA profile ensures that all transactions between involved servers are carried out securely and only with other trusted nodes in the network. It makes use of the Transport Layer Security (TLS) protocol to encrypt data being exchanged over an insecure network. The ATNA profile is responsible for the receipt and persistent storage of audit log events within the affinity domain. Audit events are required whenever an application imports, exports or queries protected health information [60].

Cross-enterprise Data Sharing for Imaging (XDS-I)

It extends the XDS to share images, diagnostic reports and related information across healthcare organizations. It is a profile that brings additional advantages to teleradiology networks. For example, a reporting radiologist has access to relevant imaging data stored in other healthcare institutions in the region [57].

The XDS-I profile specifies actors and transactions that allow users to share imaging information across enterprises. Images need to be indexed and published in a central document registry. The XDS-I defines the information to be shared, such as sets of DICOM instances (including images, evidence documents, and presentation states) and diagnostic imaging reports.

The XDS-I allows images to be located and retrieved remotely. The overall result is a three stage process for retrieval. The process starts with locating documents and reports for a patient in the registry. The next step is the retrieving of documents from the repository. Finally, a reference from the document or report to the image source is followed and the image is retrieved.

The XDS and the XDS-I reference a number of logical actors that are able to send and receive specified transactions.

The Cross-Community Access (XCA) profile

It is an IHE profile also defined under IT infrastructure. The XCA profile is developed to allow two or more registers to communicate with each other. It supports the means to query and retrieve patient-relevant medical data held by other communities. Such communities may have XDS Affinity Domains which define document sharing using the XDS profile, or it may be with respect to other communities, no matter what is their internal sharing structure [56]. The data query and retrieval from other communities is performed through the XCA initiating or responding gateway. Normally, there is only one gateway for a particular affinity domain. This one gateway will send requests to all external communities. Organizations may host any type of healthcare application such as EPR, patient health record (PHR), PACS, *etc*. A community is identifiable by a globally unique id (home Community Id). Membership of an organization in one community does not preclude it from being a member in another community. Such communities can share their domain documents using the XDS profile but they can also share documents with other communities with different internal sharing structure that implement the XCA profile.

The Cross-Community Patient Discovery (XCPD) profile

This profile complements the XCA profile by helping locate communities which hold a patient's relevant health data and by translating of patient identifiers across communities holding the same patient's data [61]. This profile is not relevant for domestic data exchange if the nation has one personal identification number. However, to communicate with healthcare information systems located in other countries, a regional or national information system with unique personal identifier should be compliant with the XCPD profile.

While the XDS-I profile supports the exchange of images and radiology workflows across healthcare organizations, it does not support the interchange of medical images between the communities. The XDS-I does not provide the framework and guidelines outside the XCA Affinity Domain. For example, to also share DICOM images, there is an extension of the XCA (like the XDS-I is for the XDS). The XCA-I allows query and retrieval of

medical images and related data from other communities because the current DICOM mechanisms are not sufficient to handle cross community access.

The Cross-Enterprise Document Workflow (XDW) profile

It enables participants in a multi-organizational environment to manage the status of documents involved in a clinical workflow [61]. The prerequisite for XDW implementation is that cross-organizational document sharing infrastructure (XDS, XCA) already exist.

The XDW uses a workflow document to track the different tasks related to the clinical event. The workflow document does not include any clinical information but contains information about the status of the particular clinical document in the workflow and maintains historical records of tasks. It uses the XDS document registry and repository to create and update the workflow document.

The XDW allows one to see if the document is either registered, the ordered service is booked, scheduled or completed, *etc*. [62]. This helps healthcare providers from different organizations to follow the status of diagnostic or the treatment process throughout the clinical event with relationship to one or more documents and can see who has made changes associated to the workflow. The XDW is not intended to support any specific workflow. On the contrary, it is workflow-independent interoperability infrastructure that facilitates the integration of multi-organizational workflows. It is also scalable up to regional and nation-wide settings.

2.7.4.5. Common semantics: Terminologies, Classifications and Vocabularies

It is the fifth prerequisite for medical image sharing. Beyond Digitalization, standards and standard profiles, IHE, IHE standard profiles for document and image sharing, common semantics is prominently necessary. Today, information about the health of an individual patient, public health or information used for the research purposes is processed and presented, in most cases, using computers. In addition to the standardization of health data and data exchange protocols, semantic interoperability is an important issue in data exchange. Semantic interoperability does not differ between digital and analogue set-ups.

To understand unambiguously the full meaning of a patients' medical data requires utilization of internationally or locally accepted clinical terminologies, vocabularies and classificators, and even more widely, the definitions of links and relations between them. For

clinical data representation there is a need for shared models that are linked to standard terminologies and classifications.

Standard representation of the full meaning of a patient's medical data requires integrating terminologies and classifications with models of context and other relationships (Healthcare Terminologies 2006). Terminologies and classifications form the foundations of information content in healthcare information systems [63].

In shared environments, semantic issues tend to be more visible because the data is more easily accessed and compared. Semantic interoperability is especially important in data sharing across organizations [48][50].

Terminologies and classifications have different uses. Terminologies are used to primarily capture clinical information while classificators are utilized for secondary data use. Terminologies are highly detailed and have substantial granularity allowing standardization of the recording of the patient's findings, events and circumstances [63]. They are mainly used to collect and present clinical information. In healthcare different healthcare systems and health related professionals have developed terminologies for their own purposes. The essential characteristic of terminology is a definition and an accurate specification of meaning. Terminologies must allow unambiguous communication of meaning across different healthcare areas and among health professionals and consumers.

Systematized Nomenclature of Medicine – Clinical Terminology (SNOMED-CT) is one of the most widely used systematically organized computer processable collections of medical terminology [64]. However, to use SNOMED-CT for radiology reporting requires additional work to aggregate large numbers of terms from different SNOMED-CT hierarchies into the form that is usable and to which radiologists, referring physicians and patients are accustomed. Using SNOMED-CT terms only makes the report too granular and structured while physicians and patients are still used to getting reports in a more colloquial form.

The IHE standard also uses multiple terminologies. They are integrated into software layers that provide access to and mapping among diverse terminologies stored in a database. Commonly used terminologies are useful in practical application of the XDS and XCA standard profiles. These include SNOMED-CT, Logical Observation Identifiers Names and Codes (LOINC), several HL7 vocabularies, some ISO standards and language codes [65].

Classificators are intended for quality of care measurement, reimbursement, statistical and public health reporting, operational and strategic planning, and other administrative functions. A classification system groups similar diseases or procedures and organizes related information for easy retrieval or other data processing purposes. They are hierarchical and provide guidelines and reporting rules for effective use.

ISO 17115 defines a classification as ‘an exhaustive set of mutually exclusive categories to aggregate data at a pre-prescribed level of specialization for a specific purpose’ [66]. Classification involves the categorization of relevant concepts for the purposes of systematic recording or analysis. The categorization is based on one or more logical rules. Coding rules must be incorporated in the classification. Coding indicates the source terminology for a particular code. However, the compliance to use classificatory in different clinical conditions is not always at an acceptable level. Today there are more than 20 comprehensive terminology and classification systems in healthcare facilities around the world. Additionally, there are a number of terminologies and classifications developed for a particular specialty or application.

To integrate different terminologies and classifications for shared information processing and shared workflows, different systems are mapped for simultaneous use of systematized lists. Mapping creates linkages between controlled content from one terminology or classification scheme to another. It enables data stored in different archives to be reused. Mapping reduces errors, increase consistency and reduces costs. It allows the retrieval of information from EPR, factual databanks, bibliographic databases, full-text sources and expert systems. However, these links are built according to a specific contextual basis and are unlikely to be 100% accurate

2.7.5. Recent Technologies to Support Medical Image Sharing

Exchange of large data sets over long distances and among different databases demands tools for secure, reliable and quick image transmission [67]. Recent technologies that use shared computing power and streaming of preprocessed data using Internet protocols allow data sharing and implementation of shared workflow. This is done in a manner that follows security and privacy rules, is carried out in a timely manner and is convenient for healthcare professionals.

Use of the current array of PACS products and image processing tools replaces dedicated, stand-alone PACS workstations with web-based PACS and RIS. These Web-based PACS and RIS communicate with other information systems throughout the healthcare domain [68]. Radiologists, radiographers and clinicians can use the same, single platform which provides them with diagnostic tools, advanced image processing methods as well as with remote meeting platforms on the web.

In this subsection, I try to discuss technologies that are implemented to enhance medical image sharing in healthcare providers worldwide. These technologies are widely used by many world leading companies in imaging field. These technologies are Streaming, Grid computing, and Vender Neutral Archiving (VNA).

2.7.5.1. Streaming technology

Streaming technology allows secure transmission of standardized, large data sets through low network bandwidths [48]. Streaming allows sending of portions of data from a source to a client for processing or viewing, rather than sending all the data first before any processing or viewing [67][48].

Medical imaging streaming is a valuable method to retrieve large volumes of image information over limited bandwidth or large geographical areas. It provides access to images and reports from different PACS archives and on a variety of client devices. Streaming creates vendor neutral applications: images are retrieved from PACS and can be viewed on any DICOM-viewer that is installed on client‘s standard computer or mobile device. Images are never stored outside the PACS but streamed only for viewing. In addition to PACS, VNA storage applications can be used as a source for image streaming.

Streaming methods can be categorized as raw streaming, intelligent downloading, or adaptive streaming of functionality. In healthcare settings, predominantly adaptive streaming and intelligent downloading are used [67].

In adaptive streaming, only frame-buffer views of the data or results of the data analyses are streamed. Using the power of the server, DICOM images are modified and processed. While the image is modified, this method does not send frame images from the server to the client each time the image properties are changed. Only final screen images are compressed and then transmitted to client devices in accordance with requirements regarding bandwidth usage, image quality, and interaction rates. This streaming method adapts to

changing conditions in order to meet these requirements [69]. The emphasis of the technology for adaptive streaming of functionality is to provide remote access to full system functionality, using the best combinations of local and remote processing of medical data.

Intelligent downloading is a form of streaming whereby only relevant portions of data set required for immediate viewing or processing are downloaded to a client. In general, processing of the data occurs locally at the client's. Additional downloading may occur in the background in anticipation of other viewing or processing requests [48][68].

2.7.5.2 Vendor neutral archiving (VNA)

Vendor neutral archiving is a term that is used to describe archiving applications that are free from vendor imposed limits on how, when, where and what a healthcare enterprise does with its digital documents and images [70]. VNA can be used not only to archive medical images but also to be a repository for other digital medical data.

VNA aims to allow healthcare enterprise to break the physical connection between the application and its content. It enables healthcare enterprises to own medical digital data and effectively share it across different organizations and clinical specialties. This is achieved by using vendor neutral middleware based on IHE standard profiles technical framework for context management.

Initially the trend in digital medical data archiving was towards disparate specialty or departmental repositories that were managed by vendor specific applications. This resulted in the creation of multiple data silos inside the enterprise. Communication between the silos required expensive and resource demanding integration [71]. Furthermore, the lifespan of archiving media, including PACS archives and software applications, is much shorter than the expectations of patients and clinicians regarding archiving media, or the demands made by clinical data retention policies. When digital data or image management applications become depreciated or are upgraded, the data is migrated from previous applications to new ones. Usually, this is a costly activity that also requires a temporary outage during normal working periods.

Vendor specific, fragmented archives in healthcare enterprises have the potential to compromise archived data by not providing access to the most accurate and relevant data at the point of care. Vendor neutrality requires the usage of widely accepted standards at all component interfaces [70]. The features that characterize VNA are tag mapping and

morphing, clinically-based information lifecycle management and universal viewer support, IHE compliancy, *etc*. [72]. VNA allows archiving any type of digital clinical content that can be associated with a patient or a study, including non-DICOM content such as PDF files, video files, sound files, JPEG, and TIFF images. The solution interfaces with other clinical information systems for communication of reports, results, workflow, *etc*., by way of HL7.

VNA enables use of different PACS applications from multiple vendors, integrates archived data sets into the virtual archive and avoids costly migration and re-indexing of data. The data ownership shifts from the archive vendor to the healthcare enterprise because the archived data can be managed using any standardized application independent of a particular vendor.

Consequently, healthcare organizations can implement and provide unique services to facilitate sharing of data, while maintaining different clinical assets under common patient records [73].

2.7.5.3 GRID Computing

Implementation of new e-services in healthcare requires coordinated use of heterogeneous information systems. Grid technologies aim to provide the framework to enable dynamic, flexible sharing of computational and storage resources through interoperable middleware based on open standards [54].

A computational grid consists of both hardware and software infrastructure that provides dependable, consistent, wide spread, and inexpensive access to high-end computational capability and storage resources [74].

A storage grid is storage architecture that employs multiple interconnected storage nodes so that any node can communicate with any other node. Distributed storage provides a high level of redundancy with almost no down time, evens out performance under conditions of fluctuating load and is highly scalable. It enables different healthcare organizations to integrate and share data across organizations [75].

A storage grid can interconnect different PACS archives and other storage media like vendor neutral archives. This concept allows special middleware containing meta-data indices with the full contents of each separate archive to be placed above the storages located in different enterprises [68].

Grid computing utilizes combined computer resources, connected via the internet, from multiple administrative locations. This allows additional computing resources to be achieved. It provides access to resources that are not subject to centralized control, uses standard, open, general purpose protocols and interfaces, and can deliver various levels of service. Grids consist of networks of computers, storage, and other devices that can pool and share resources [76]. To perform desired tasks, grid-enabled software is built on open, standard frameworks and protocols [77].

Though grid architecture was initially not intended to be used in the healthcare sector, it has now been well adapted to the public health information systems. It promotes an open, transparent, collaborative network that leverages open source software and infrastructures, enables continuing existence of legacy applications, supports a strong security model, uses standards and service-oriented architecture, allows distributed and federated database and web services access, and enables push and pull multi-directional data exchanges [74][78].

Grid technology can be deployed at the department level but the main value of it emerges when using grid in enterprise-wide or multiple enterprise settings. Grid computing and streaming of medical data and images gives powerful tools for data transmission and sharing in the healthcare environment. Grid-computing for electronic medical records is being enabled by the use of interoperability standards and standard profiles for integrating disparate systems and sources of data [68].

Health grids are evolving all over the world to solve increasing demand for data computing and analysis for healthcare and research purposes. One example is MammoGrid which has effectively demonstrated the viability of the grid by using its power to enable radiologists from geographically dispersed hospitals to share standardized mammograms, compare diagnoses and perform sophisticated epidemiological studies across national boundaries [79].

In radiology, the grid computing infrastructure is used to virtualize PACS services [78]. In accordance with the XDS-I profile, the registry containing the meta-data index to the full contents of each separate PACS or other archive, is placed above the various archives deployed in different locations. All meta-data are kept updated and synchronized across instances via various database features for maintaining data concurrency [68]. Virtualization of PACS services allows designing workflows based on different clinical purposes or client

needs [71]. It also supports multi-site installations and integration of disparate PACS archives. Grid computing architecture can be extended to also virtualize other healthcare services.

2.7.6. Barriers for data sharing and shared workflow

The challenges that arise when implementing cross-organizational data sharing and shared workflows depend on the level of data sharing [50]. These challenges include trust between healthcare professionals, trust between healthcare professionals and patients and issues related to service quality, cross-organizational interoperability, legal clarity and reimbursement.

Depending on the level of sharing, the interoperability issues are technical, organizational (including the seamless medical data exchange between different information systems), or semantic (including language). Barriers without crossing state borders tend to be mainly technical, organizational and financial. At the cross-border level, legal and language issues dominate [50].

Barriers for data sharing and shared workflow depend on the sharing models. The sharing model can be implemented within one organization, between organizations in one region or across country borders, or between a healthcare enterprise and citizen [50].

2.7.6.1. Inside the healthcare organization

In-house data sharing and in-house shared workflow still represent a majority of cases where images and workflows are shared. Although substantial research is done to define standards and profiles for cross-organizational implementation, most data sharing implementations are used for one organization's internal workload balancing. Implementation of image sharing and shared workflow decreases remarkably the time between image acquisition and the availability of the image's report in the healthcare environment.

Quick image sharing places higher demands for image quality and the image management process but does not require any additional legal measures as long as the images do not cross organizational borders [50]. However, administration of user rights and management of log files are new tasks for the organization and need complementary resources.

Still today, incomplete integration of imaging modalities, PACS, RIS and EPR, as well as partial digitalization of images and related data [57] is the main barrier for image and workflow sharing at the organizational level. Information sharing is not achieved in an effective manner where imaging standards and communication profiles are not fully applied. Absence of full digitalization of all images, lack of interfaces between RIS and imaging modality or PACS and EPR, *etc*., hinders the potential advantages of image and workflow sharing [80].

2.7.6.2. Between healthcare organizations

Sharing images and workflow between healthcare organizations creates new challenges regarding quality control, trust, legal issues, reimbursement, workflow management, and interoperability of EPR, RIS and PACS.

The most important challenge is to ensure that reporting of images outside the organization does not in any way reduce the quality of radiology services provided to the citizen. To achieve this goal, relevant healthcare organizations must work towards creating a professional, trustful relationship between clinical partners. Trust can be developed by on-site visits and familiarization with clinical radiology workflows at hospitals. Also, the appointment of one particular radiologist to act as the responsible person for inter-organizational teleradiology communication is needed [50].

Integration of EPR, RIS and PACS using IHE XDS standard profiles is still an exception rather than a rule. Using proprietary solutions for inter-enterprise health information system integration is a complex task and can be deployed mainly on a point-to-point integration basis. Consequently, this makes implementation of the real shared workflow a hard to achieve task. Implementation of XDS-I standard profile for sending and receiving images, which would allow image sharing between organizations, demands additional resources for upgrading software applications so that they are compatible with IHE standard profiles.

Transfer of image-related data outside the imaging facility requires additional identification, safety and security measures [80]. European Union (EU) Directives on the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector [81][82] specify a number of specific requirements relating to confidentiality and security that telemedicine and all other interactive on-line services have to meet in order to

safeguard individuals' rights. These legal acts also set-out requirements for providers of electronic communication services over public communication networks to ensure confidentiality of communications and security of their networks [83]. In Europe, in most cases, this is usually solved by bilateral contracts between the organizations addressing licensing, liability, accreditation and the registration of imaging services and professionals.

The reimbursement of tele-radiology services in inter-organizational workflow sharing is an issue that often causes difficulties and is seldom solved automatically with clinical set-ups [84]. Usually the financial software of the healthcare institution is not integrated with the clinical software, thus making the financial management of inter-organization tele-radiology difficult.

2.7.6.3. Across country borders

The basic issues that need to be addressed in an inter-organizational setting (quality and trust, interoperability, identification, security, legal issues) also apply to cross-border settings. However, the legal issues are more complex because of the differences in healthcare. EU legislation regulating tele-radiology services consists of multiple directives and legal documents, which makes the interpretation of the legal system in the EU extremely complex. Besides the EU directives, there are additional legislative documents which have to be considered in implementing tele-radiology services [50].

Additional issues to be addressed are semantic interoperability and language. In the Baltic eHealth and R-Bay projects, one of the main limiting factors for full deployment of cross-border tele-radiology services was the lack of commercially available radiology report translation software [67]. There is no professional and commercially available radiology report translation software [85].

2.7.6.4 Image sharing with citizens

Sharing digital images via the web with patients is a new feature in medical imaging management [86]. The main barrier to sharing digital images with patients is user identification security and secured access to electronic health record (EHR) and PACS. Usually, user identification and access rights to images in PACS are designed for healthcare professional. The identification of a particular citizen is usually done by using credentials for HER or PHR. In this setting, images are opened using a URL link between the EHR and PACS. Another limiting factor is a lack of citizen friendly viewers which can provide thin,

client applications and use low bandwidth networks. PACS' user interfaces are too complicated for the use of ordinary citizens [50].

Medical image viewing platforms for the patient are already in use in some countries. For instance, in Estonia the patient portal iPatient is used to give patients' access to medical images via the Internet. The access is secured by using a national ID-card. Patients can access their own images by using simple viewing platform which uses streaming technology. A similar concept is used by the Center for Diagnostic Imaging, USA. A patient is provided with a password protected account. Via the account, the patient obtains access to the booking service, receives preparation and appointment instructions, and can view his or her diagnostic reports and images [50].

2.7.7. Emerging Technology for Medical Image Sharing

2.7.7.1. Cloud Computing

As previously discussed literatures show, many organizations including healthcare are shifting their ICT paradigm from traditional data centers to cloud based services for the improvement of services with lower costs and better efficiency.

Radiology, early adopter of technology in healthcare, gives attention for cloud these days. This is because; production of medical imaging will continue to increase in the following decades. For instance, the PET-CT modality requires space for storing the PET images, the CT images and the outcome fusion images and, the same situation happens with the new modality PET-MRI. Furthermore, there is a new research trend of content-based image retrieval, where it is possible to discover and retrieve images based on the pixel data of the image. This content-based retrieval is enabled by models describe the image and these models also require store space. As result, the storing requirements of the medical imaging fields are demanding and will be even more demanding in the future. Therefore, new storage solutions with flexible business models are needed more than ever. The Cloud computing paradigm offers an elastic framework to allocate or release computational resources on-the-fly and enabling a more efficient usage and, as a consequence, reducing costs. Current PACS architectures, hospital oriented, with their own short-term and long-term archives with no or little interaction with other institutions or PACS are difficult to extrapolate to the cross-

institutional environment. XDS-I allied with XCA integration profile set the roadmap to enable the cross-enterprise medical imaging sharing. The conjugation of both integration profiles offers to the healthcare institutions flexible levels of inter-institutional coupling.

Researches by [87][88] proved that storing and/or distribute medical images and related exams using public Cloud providers is possible. Although, these solutions are interoperable within institution (since are DICOM compliant) at the cross-enterprise level they do not follow the transactions defined by the IHE. So, radiology departments can benefit from the potentials of cloud computing without compromising privacy and confidentiality of the PHI.

2.7.7.2. Strategy to adopt cloud for Medical Image Sharing

The broad scope and size of the cloud transformation will require a meaningful shift in how healthcare institutions think of IT. Healthcare providers that previously thought of IT as an investment in locally owned and operated applications, servers, and networks will now need to think of IT in terms of services, commoditized computing resources, agile capacity provisioning tools, and their enabling effect for their organization goal. This new way of thinking will have a broad impact across the entire IT service lifecycle – from capability inception through delivery and operations.

The researcher recommends the following adoption strategy, for healthcare organization when they decide to adopt cloud. The framework presents a strategic perspective for agencies in terms of thinking about and planning for cloud migration.

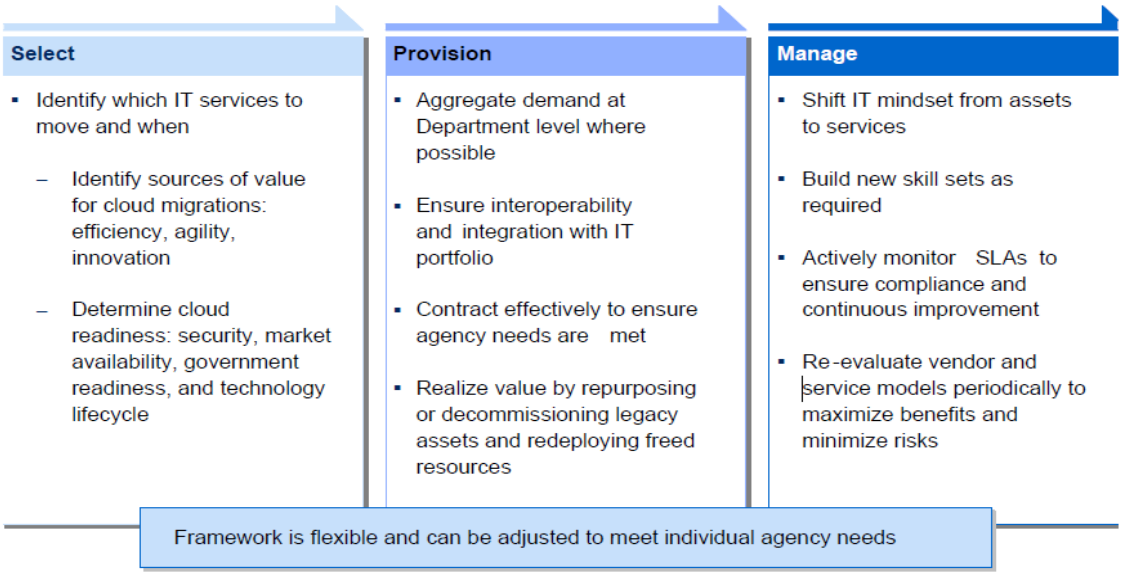

Figure 2.12: Decision Framework for Cloud Migration [88]

A broad set of principles and considerations for each of these three major migration steps is presented below.

1. Selecting services to move to the cloud

It is good for organizations to carefully considering their IT portfolios and developing roadmap for deployment and migration. These roadmaps prioritize services that have high expected value and high readiness to maximize benefits received and minimizes delivery risk. Defining exactly which cloud services an organization intends to provide or consume is a fundamental initiation phase activity in developing an agency roadmap.

The chart shown below uses two dimensions to help plan cloud migrations: *Value* and *Readiness*. The Value dimension captures cloud benefits in the three areas (i.e., efficiency, agility, and innovation).The Readiness dimension broadly captures the ability for the IT service to move to the cloud in the near-term. Security, service and market characteristics, government readiness, and lifecycle stage are key considerations. As shown below, services with relatively high value and readiness are strong candidates to move to the cloud first.

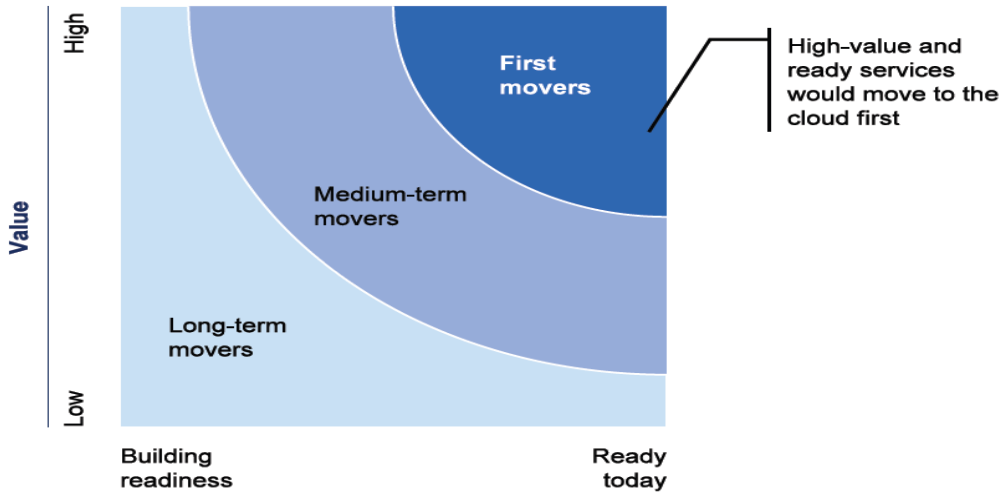

Figure 2.13: Selecting Services for Cloud Migration [88]

The relative weight of the value and readiness dimensions can be adjusted to meet the individual needs of agencies. Some agencies may stress innovation and security while others may stress efficiency and government readiness. However, the logic and structure of the framework should be applicable for all agencies.

Described below are a number of considerations for value and readiness that agencies may find helpful when completing this

Identify sources of value

As cloud computing provides three primary sources of business value: efficiency, agility, and innovation. Listed below are a number of considerations for each value category. Agencies should feel free to stress one or more of these sources of value according to their individual needs and mission goals. For instance, some agencies may place a higher value on agility, while others may stress cost savings brought about by greater computing efficiency.

Efficiency: Efficiency gains can come in many forms, including higher computer resource utilization due to the employment of contemporary virtualization technologies, and tools that extend the reach of the system administrator, lowering labor costs. Efficiency improvements can often have a direct impact on ongoing bottom line costs.

Agility: Many cloud computing efforts support rapid automated provisioning of computing and storage resources. In this way, cloud computing approaches put IT agility in the hands of

users, and this can be a qualitative benefit. Services that are easy to upgrade, are not sensitive to demand fluctuations, or are unlikely to need upgrades in the long-term can receive a relatively low priority.

Innovation: Agencies can compare their current services to contemporary marketplace offerings, or look at their customer satisfaction scores, overall usage trends, and functionality to identify the need for potential improvements through innovation. Services that would most benefit from innovation should receive a relatively high priority.

Determine cloud readiness

It is not sufficient to consider only the potential *value* of moving to cloud services. Agencies should make risk-based decisions which carefully consider the *readiness* of commercial or government providers to fulfill their needs. These can be wide-ranging, but likely will include: security requirements, service and marketplace characteristics, application readiness, government readiness, and program's stage in the technology lifecycle. Similar to the value estimation, agencies should be free to stress one or more of these readiness considerations according to their individual needs.

2. Provisioning cloud services effectively

To effectively provision selected IT services, agencies will need to rethink their processes as provisioning services rather than simply contracting assets. Contracts that previously focused on metrics such as number of servers and network bandwidth now should focus on the quality of service fulfillment.

Organizations that are most successful in cloud service provisioning carefully think through a number of factors, including: Aggregating demand, integrating services, contracting effectively and Realization of value.

3. Managing services rather than assets

To be successful, agencies must manage cloud services differently than traditional IT assets. As with provisioning, cloud computing will require a new way of thinking to reflect a service-based focus rather than an asset-based focus. Listed below are a few considerations

for agencies to effectively manage their cloud services. These are Shifting mindset from asset to service, actively monitoring according to SLA and periodic evaluation of the service.

2.8. Related Works

Cloud computing model provides a new way to solve foregoing problems. Some studies have been performed recently in an attempt to employ Cloud method in medical affairs. For instance, Rolim et al proposed a cloud-based system to automate the process of collecting patients' vital data via a network of sensors connected to legacy medical devices, and to deliver the data to a medical center's "cloud" for storage, processing, and distribution [89]. Nkosi and Mekuria described a cloud computing protocol management system that provides multimedia sensor signal processing and security as a service to mobile devices. The system has relieved mobile devices from executing heavier multimedia and security algorithms in delivering mobile health services [90]. Rao et al reported a pervasive cloud initiative called Dhatri, which leveraged the power of cloud computing and wireless technologies to enable physicians to access patient health information at anytime from anywhere [91]. Koufi et al described a cloud-based prototype emergency medical system for the Greek National Health Service integrating the emergency system with personal health record systems to provide physicians with easy and immediate access to patient data from anywhere and via almost any computing device while containing costs [92].

Some studies shows the successful application of cloud computing in bioinformatics research. For example, Avila-Garcia et al proposed a framework based on the cloud computing concept for colorectal cancer imaging analysis and research for clinical use [93]. Bateman and Wood used Amazon's EC2 service with 100 nodes to assemble a full human genome with 140 million individual reads requiring alignment using a sequence search and alignment by hashing (SSAHA) algorithm [94]. Kudtarkar et al also used Amazon's EC2 to compute orthologous relationships for 245,323 genome-to-genome comparisons. The computation took just over 200 hours and cost US $8,000, approximately 40% less than expected [95].

Furthermore in medical imaging field, the work in [96] introduces the concept of Medical Image File Accessing System on cloud computing. This uses the Hadoop platform to

solve the exchanging, storing, and sharing issues in Medical Images. While other research [88] Silva et al. proved that storing and/or distribute medical images and related exams using public Cloud providers is possible. Although, these solutions are interoperable within institution (since are DICOM compliant) at the cross-enterprise level they do not follow the transactions defined by the IHE.

So, my work takes this gap, IHE/XDS/XDS-I, compliance and it also works for both DICOM and non-DICOM. That means this paper focuses on how all types of image data can be archived and sharing by using IHE integration profile using cloud architecture. This feature makes my work novel.

Chapter THREE

3. Security, Legal and Compliance Issues in Cloud Computing

Introduction

The foundation of any good information security program is risk management. Organizations need to understand the following:

- What information is being stored, processed or transmitted
- What are the confidentiality, availability and integrity requirements of the information
- What are the compliance requirements of the information and penalties for failure
- How to implement people, process and technology controls to address the requirements

In a healthcare setting the protected health information (PHI) is the primary focus of information technology (IT) risk management practices [97]. Traditionally, sensitive health information has flowed through the organization via paper records. Maintaining and protecting these records relied heavily on people and processes. Risks to the unauthorized access, modification or destruction of information existed but the impact was typically only one or a handful of individuals on average.

With the increased adoption of technology in healthcare such as electronic medical records, health information exchanges, and networked medical devices, the risk to PHI increases in both likelihood of unauthorized disclosure and impact to the organization given the greater amount of data accessible.

In this chapter we try to discuss security issues (challenges, vulnerabilities, security goals and best practices on cloud security), Legal issues (Legal challenges, healthcare legal regulation) and compliance issues.

3.1. Security

In the psychology of security, Schneir argues that "*security is both a feeling and a reality. And they are not the same*" [98]. In this, Schneir means that, the reality of security is based on the probability of different risks and how effective the various mitigation strategies

are in place in dealing with the perceived risks. Security is also a feeling based on the psychological reaction to both the risks and the countermeasures.

Therefore, this means that, cloud computing need to appeal to the feelings of the clients and address the potential security risks in a manner that clients will feel safe and secure. By addressing security is this way clients will feel safer and secure and hence trust cloud service providers. This helps in identifying the gaps existing between the organizations compliance model, the security control model and the cloud model. By identifying the compliance requirement and where in the security model they are required or are fulfilled the organization can then link the appropriate security control to its appropriate cloud infrastructure.

The figure below shows an example of how a cloud service mapping can be compared against a catalogue of compensating controls to determine which controls exist and which do not — as provided by the consumer, the cloud service provider, or a third party. This can in turn be

compared to a compliance framework or set of requirements such as PCI DSS, as shown.

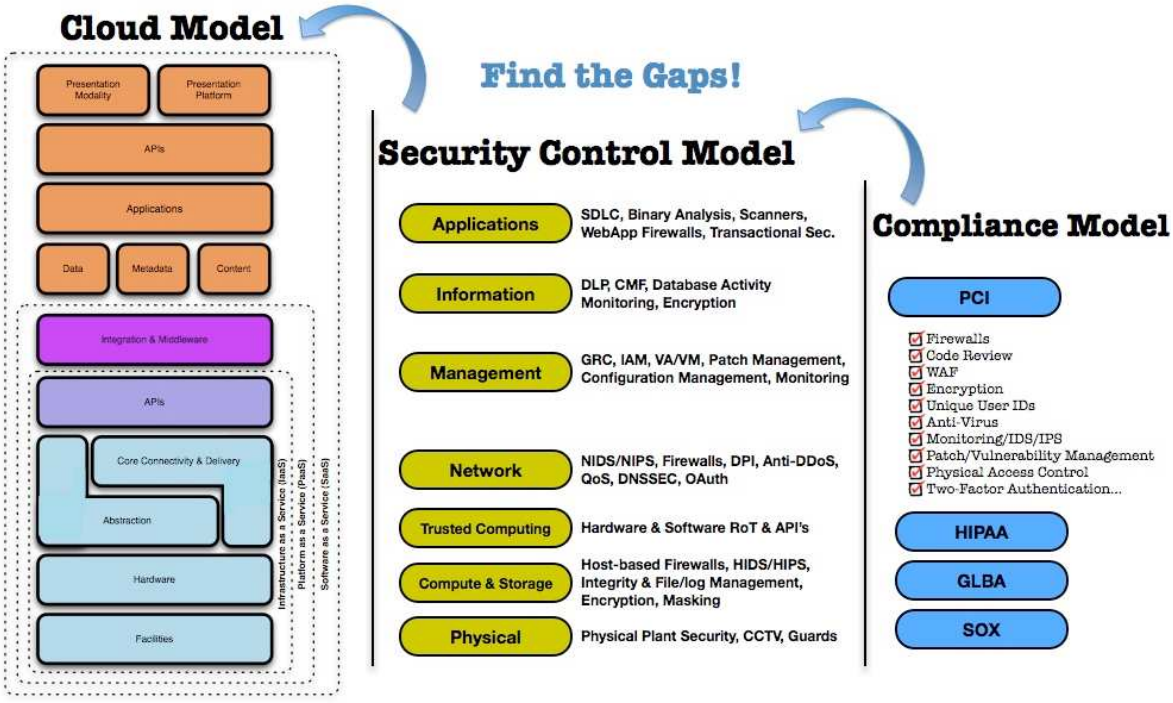

Figure 3.1: Mapping Cloud model to Security and Compliance Model [99]

Once this gap analysis is complete, per the requirements of any regulatory or other compliance mandates, it becomes much easier to determine what needs to be done in order to feed back into a risk assessment framework; this, in turn, helps to determine how the gaps and ultimately risk should be addressed: accepted, transferred, or mitigated.

3.1.1. Security challenges in cloud computing

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties [99]. Considering these challenges before moving the clinical data or components of the IT infrastructure to the cloud is not a task that should be forgotten. Cloud computing and cloud service providers need to address a number of challenges that affects security in the cloud. What are these challenges, how these challenges can be addressed and how the mitigation plans are put in place is crucial in ensuring that clients trust cloud computing environment. These challenges are discussed in detail as follows:

Loss of governance

By using cloud services the client passes control to the provider. This passing off, of control to the provider, results in loss of control over a number of issues which in turn may affect the security posture of the client data and applications. This is aggravated by the fact that SLAs may not tender commitment on the part of the provider, and thus widening the security cover gap. The terms of use policies also contributes as can be exemplified by Google App engine terms of use which require the user to *"agree that Google has no responsibility or liability for deletion or failure to store any Content and other communications maintained or transmitted through use of the service"[100]*.

Amazon is another example where their terms of use for their Amazon Web Services, makes it clear that they have no liability to any unauthorized access, use, corruption, deletion among other thing to the clients data or applications [101]. This poses challenge to customers

as to how to ensure security of their data and applications which may be hosted in the cloud by a third party.

Consumer lock-in and bankruptcy

Currently there are tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. Consumer lock-in and bankruptcy of the Cloud provider are two serious risks and both have a similar consequence, which is losing control of the data trusted by the cloud consumer to the cloud provider [87].

Consumer Lock-in may be performed at two different levels: data lock-in and vendor lock-in. Trusting valuable data to a single provider may lead to opportunistic reprising, where the provider uses the held data at its data centers to blackmail the costumer and rise prices while renegotiating contracts. Vendor lock-in is more subtle type of consumer lock-in. Due to the fact that each Cloud provider offers, to its customers, a unique development API which turns the applications specific to the Cloud provider. Therefore, the consumer is locked-in with the Cloud provider since migrating the applications to other Clouds means recoding the applications following the new cloud API. As a result, the cost of migration does not compensate the eventual competitive prices of other Clouds. As it was mentioned before, other risk that could lead to losing control of the consumer's data is the bankruptcy of the Cloud Provider. Cloud Providers are companies and companies may go bankrupt. The obvious question that arises is what happens to the consumer's data and applications if such scenario becomes a reality? Migrating data (e.g. images or documents) probably would be less demanding than migrating applications developed with specific PaaS API. As a result, the lack of interoperability at the PaaS may turn the migration process extremely difficult, requiring the refractor of the majority of the source code. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

Privacy and confidentiality

The privacy and confidentiality of the data placed on the Cloud are the main barriers that delay Cloud's general acceptance. The World Privacy Forum (WPF) released a report spelling out the risks to privacy and confidentiality posed by Cloud computing. The report unveils concerns regarding Cloud's current state: what happens to the data after the consumer uploads it to the Cloud and how its confidentiality will be protected. The answer to this question is somehow disappointing. In the current state of Cloud computing it does not ensure privacy or confidentiality of the stored data. The simple fact of uploading data to the Cloud makes that data more suitable for disclosure or unauthorized usage. The WPF published several privacy advices in order to aware the cloud consumers:

- Read the Terms of Service before placing any information in the cloud. If the Terms of service are not understandable, a different cloud provider must be considered.
- Information in the cloud is legally easier to access through the Cloud than by seizing a private computer. Therefore, sensitive information should not be uploaded to the Cloud.
- In the Term of Services one must notice if the Cloud provider reserves rights to use, disclose, or make the uploaded information public.
- Read the Privacy Policy before placing any information in the cloud. If the Privacy Policy is not understandable, a different cloud provider must be considered.
- Beware if the Cloud provider retains rights over removed data by the consumer.
- Beware if the cloud provider notifies their consumers when the Terms of Service or Privacy policy change.

Furthermore, WPF extends its advices to companies or governments that are considering the upload of data or the migration of the IT infrastructure to the Cloud:

- Caution on ad-hoc Cloud computing is advised. Organizations should have standardized rules for employees to know which data they may (or not) upload to the cloud.
- Sensitive information that is of the interest of the organization to keep away from the government, other competitive organizations or other governments should not be uploaded.

- Information disclosure of cloud's data should be considered before uploading the actual data.
- Hire professional support for understanding the Terms of Service or Privacy Policies of the Cloud provider.

Interoperability and standardization

Although some efforts towards reaching standardization among for Cloud Computing, such as the Cloud Computing Interoperability Forum (CCIF) or the European Telecommunications Standards Institute (ETSI), the reality is that cloud standardization is far from being achieved and at some levels maybe it never will, as a consequence, the lack of interoperability inter-cloud provider is a resilient issue. If it is possible and relatively easy to guarantee cloud interoperability at the IaaS level even without standardization (e.g. DeltaCloud [102] accomplishing interoperability between the several PaaS is a more demanding task. Not only due to possible economical interest of the Cloud providers, but as well at the technical level.

PaaS APIs abstract the complexity of the IaaS and provides the developers with embedded functionalities (e.g. automatic scaling) that at the IaaS level have to be implemented from scratch . This facilitated API of PaaS is more convenient for the developer but less flexible at the same time [103]. PaaS automatic features turn the standardization or interoperability efforts more complex. Each Cloud provider follows its unique IT architecture - especially above the IaaS level (PaaS or SaaS). If some features are easy to accomplish in some cloud architectures, the same features could be extremely difficult to achieve at other architectures. This heterogeneity of features and architectures may push back standardization, and turn full interoperability above the IaaS level extremely difficult.

Geographical distribution

The Cloud providers are private companies adjudicated to a country obligated to follow the countries laws [87]. However, they compete with each other on a global market, ignoring countries borders. Enabled by the Internet, a Cloud provider from the USA may easily offer its Cloud services to a consumer from Singapore or Australia. At the same level, a Cloud provider may have several data centers around the world. For instance, one of the major expenses of a data center is the energy consumed for refrigerating the machines and, if the data center is placed in a cold natural geographical location (e.g. Alaska) the cooling

costs will be much lower and the Economics of Scale enhanced. However, this cross-border logistics of the Cloud business model may aggravate liability and jurisdiction risks, due to the fact that cross-border litigation is typically more complex and high-staked than litigations within borders, and is not clear which court have jurisdiction over the Cloud where the illegality occurred: would it be treated in the jurisdiction of the consumer, the provider or the vendor?

3.1.2. Security Vulnerabilities of Cloud Computing

Cloud computing environment apart from creating challenges to security, it also increases the vulnerability and attack surface. The vulnerabilities and threats that cloud computing need to address among others are as follows [2]:

- Poor authentication, authorization and accounting system.
- User provisioning and de-provisioning; the ability of customer to control the process.
- Remote access to management interface.
- Hypervisor vulnerabilities such as virtual machine based root kit.
- Lack or weak key encryption.
- Lack of standard technologies and solutions.
- Poor key management procedures.
- Inaccurate modeling of resource allocation.
- Mis-configuration.
- Lack of forensic readiness, sanitization of sensitive data.

This list is not intended to be exhaustive but it shows the importance of addressing security issues for trust to be built for cloud computing customers. As for the threats, the Cloud Security Alliance (CSA)[103] has identified what it calls the top threats to cloud as follows:

- Abuse and nefarious use of cloud computing.
- Insecure interfaces and application programming interfaces (API).
- Malicious insider.
- Shared technology issues.
- Data loss or leakage
- Account or service hijacking.

- Unknown risk profile.

Though the threats identified are representative of all the possible threats that can occur in the cloud, nevertheless they portray the necessity of security to appeal to the feelings of the clients. This is because without security addressing the reality of these risks and providing for mitigation plans, clients trust for cloud services will be hard to build.

4.1.3 Security and cloud computing (Standards and Best Practices)

With all the fears surrounding information security and cloud computing in particular, in this sub-section a review of a number of security standards and best practices that have been developed and used in conventional computing is done. The review aims to identify and see how these standards and best practices can be used in ensuring cloud computing security and build trust.

ISO 27001 (BS ISO/IEC 27001:2005, BS 7799-2:2005)

This standard which was formerly was known as BS 7799-2, is intended to "*provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS)"* [104]. The standard defines how a business or an organization can organize it information security, based on it needs, objectives and security requirements. The standard also can be used by both internal and external parties in assessing the security posture of an organization; this has led to certifications showing that an organization meets the standards requirement for information security. The certification is an indication that the organization has implemented information security in the best possible way. However, certification for cloud computing may not very useful. This is because the client and vendor security requirements and practices may differ which will still require vendor to adjust their practices to meet clients' needs. Nevertheless, vendor certification is still important as an indication that they are committed to ensuring security and use of security best practices.

The standard prescribes how information security can be managed through ISMS. The management system has four phases which are: the Plan phase which is dealing with the planning of organizations' information security; sets objectives for information security and selects the appropriate security controls. The standard contains one hundred and thirty three (133) possible controls. The second phase is the DO phase which executes all that which was

planned in the planning phase. The third phase is the check phase. This phase supervises how the ISMS functions and monitors to see if the results meets the set objectives. The fourth phase is the Act phase, which is concerned with taking of corrective measure for anything that was identified in the previous phase as not meeting the objectives. Figure 3-2 shows how these phases are related.

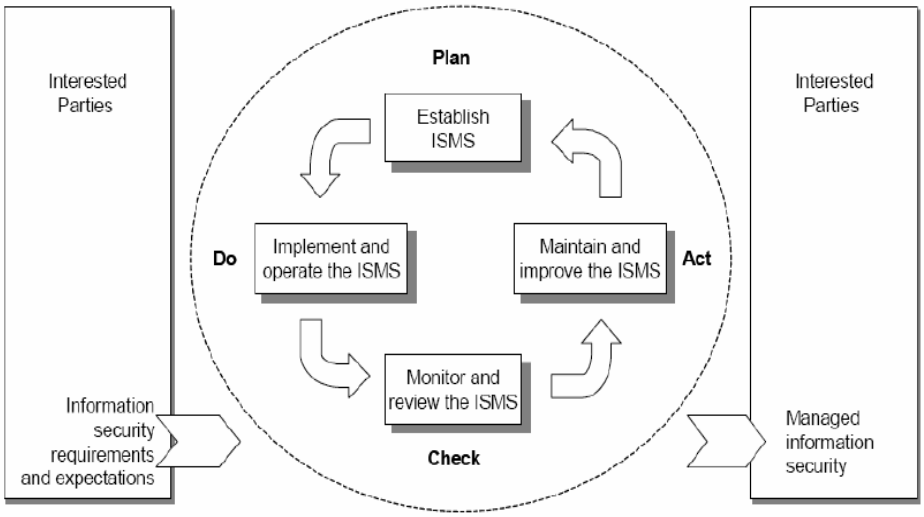

Figure 3.2: The four phases of ISO 27001 [105]

The standard also requires a set of documentations to be produced as a result of complying with the standard. These documents are: the scope of the ISMS, the ISMS policy, procedures for document controls, internal audit , and procedures for corrective and preventive measures, documents relating to the selected security controls, risk assessment methodology, risk assessment report, risk mitigate ion plan and records. However, the amount and complexity of the document will depend on the size of the organization and the complexity of the ISMS.

In order to address security and trust issues in cloud computing adoption, we propose that, vendors and clients should work together in the whole process of developing and implementing ISMS. This will enable both parties to understand the security requirements and capabilities of the vendor in providing the required security and hence will facilitate and foster t rust.

ISO 27002 (BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005)

This standard is an auxiliary standard to ISO 27001. It establishes the "*guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization*" [105]. It purpose is stated as "*provide general guidance on the commonly accepted goals of information security management*" [105].

The objectives and controls in this standard are expected to meet the requirements identified during risk assessment when implemented. The standard can be used by an organization as a basis for developing organizational security practice guidelines and security standards that will be vital in fostering inter organizational trust. The standard covers areas such as data security, data processing, data transmission, computers, information exchanged, risk management , access control , information system acquisition, incident response and business continuity.

By using the guidelines outlined in this standard, the cloud vendor and client need to work together to identify how the different ISMS requirements can be implemented in adopting cloud computing services, and how issues related to access control , incident response and business continuity will be tackled. This collaboration between service providers and clients in the process of developing and acceptable security posture is important in facilitating trust and adoption of cloud computing. Therefore, by leveraging the ISO 27001 and ISO 27002 information security standards and by working in collaboration with clients in developing a set of transparent security principles vendors can build customer trust and thus enhance the adoption rate of cloud services.

Therefore, through collaboration and the use of these different security standards, clients and vendors can manage to establish security policies and best practices to govern their relationship. It is through collaboration a structured security and trust framework can be developed that can be useful in assessing the security requirements of the user and the ability of the vendor to meet those requirements.

Control Framework for Information and related Technology (COBIT)

This is a "*framework for IT governance and control, it supports toolset that allows managers to bridge the gap between control requirements, technical issues and business risks*" [106]. As a governance and control framework COBIT provides two procedures one for defining an IT strategy and the second for managing third party services. It also provides

a maturity model that can be used to assess the maturity of the IT governance processes in an organization.

For cloud computing clients, by using the COBIT procedure the client will be able to determine what should be done before and after selecting a cloud vendor or solution. COBIT will also help, in monitoring the value that is to be gained by adopting cloud computing, the level of risk exposure and in deciding who will be responsible, accountable, consul ted and informed during the cloud adoption project.

The maturity model will help an organization in determining the level of maturity of its IT governance, and whether the maturity level is acceptable for the move to cloud computing. Therefore, by using COBIT organization can institutionalize good practices which will ensure that IT investments produce business value [107]. And in this case it will help in ensuring that the move to cloud solutions will result in better business value without compromise. Figure 3-3 shows the overall COBIT 4.1 framework

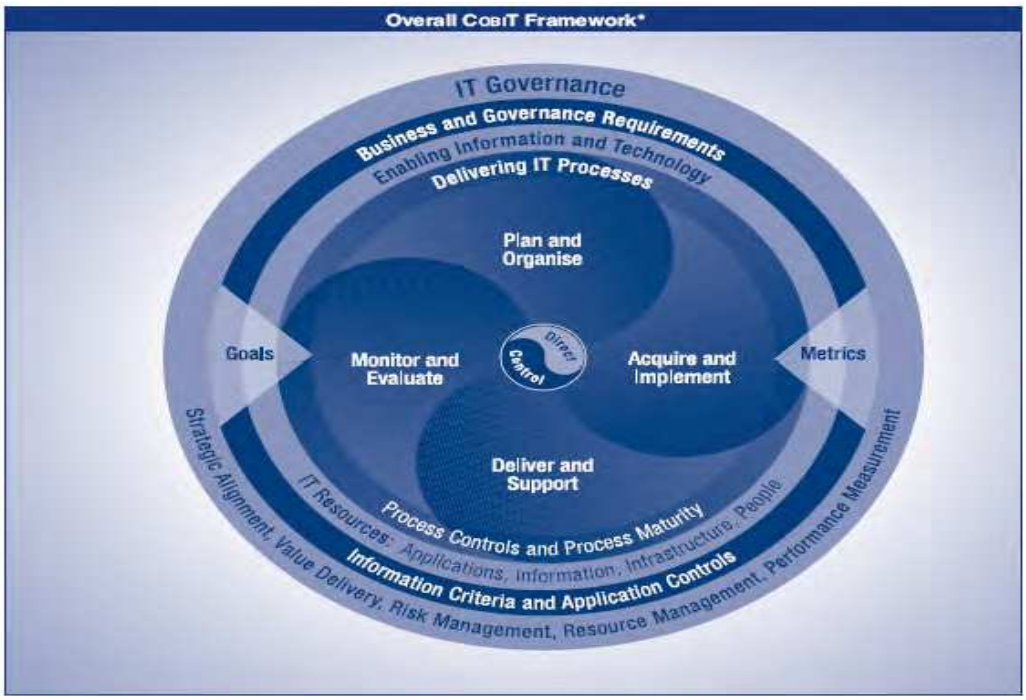

Figure 3.3: Overall COBIT 4.1 Framework [107]

By using this framework a healthcare organization can try to answer questions related to governance and best practices and determine whether the organization is capable of IT governance in the cloud.

Open Security Architecture (OSA)

The standards and best practices discussed so far pre-dates' the cloud computing error. The cloud computing pattern developed by the open architecture is an attempt at addressing the different security and migration challenges facing cloud adoption. The open security architecture-cloud computing patterns have combined different possible aspects of cloud use and how these can be managed and monitored. The pattern also provides mapping of the different aspects of security and management to ISO standards and COBIT best practices for IT governance. The pattern also identifies different stakeholders and their respective responsibilities.

Standardized security framework for cloud computing

As it have been shown, the biggest problem with cloud computing security is lack of transparency of cloud vendors about their security capabilities, and lack of standard or framework for security. As a result of this different organizations are currently working in developing different security frameworks for cloud security. Frameworks in development [108] include: A6, Trusted cloud initiative, Common Assurance Maturity Model (CAMM) and Federal Risk and Authorization Management Program (FedRAMP).

A6 (Automated Audit, Assertion, Assessment, and Assurance API) working group

The effort is known also as Cloud Audit, and is under the leadership of Chris Hoff of Cisco Systems.

Trusted Cloud Initiative

This initiative is under the Cloud Security Alliance; it is chaired by Liam Lynch eBay security strategist. The objectives of the initiative are to provide a reference framework for implementation and enable end-to-end security platform.

Common Assurance Maturity Model (CAMM)

This is a consortium of made up of 24 members. Most of the members are vendors, but it also includes the European Network and Information Security Agency (ENISA). It was launched initially as an assurance framework metric. The initiative is planning a formal release in November 2010.

Federal Risk and Authorization Management Program (FedRAMP)

This is an initiative by the US government for continuous authorization and security monitoring of shared IT resources or services of the federal government departments and agencies when they contract or outsource their IT services including outsourcing to cloud computing.

3.2. Legal Issues

With data and application hosted by a third party, the cloud service provider; issues of ascertaining the legal and compliance impact to participating parts is difficult. Issues related to data protection, privacy, jurisdiction of storage and processing and e-discovery raise. It also raises the issue related to the responsibility of the aforementioned issues.

These differences in regulations and government interferences poses challenges to businesses as they seek to adopt cloud computing. For example a business located in Europe may be jeopardized by using cloud services which hosts its data in a country where there is no data protection laws or where there is legislation.

Therefore, these differences calls for business managers and chief information officers to understand how local data protection requirements of different countries may impact their business in terms of complying to their privacy and data protection legislation in country of origin.

For the cloud providers, an understanding of local data protection requirements impact on their clients' data is of importance as it will help in providing their clients with accurate and sufficient information and also help in tailoring their offerings to meet their clients' requirements. How vendors respond to these legal and compliance challenges have impact on how trustworthy the vendor is/will be perceived by customers in handling legal and compliance requirement and needs of the customer.

3.2.1 The Legal framework

For cloud service customers and providers in Europe (EU), the EU Data Protection Directive 95/46 is more relevant [103]. For those in the United States of America (US) there is no specific directive or law but a number of regulations have bearing on their businesses [109]. For other parts of the world may have national regulations or no regulations at all for data protection. All these differences pose challenges for both cloud customers as well as

vendors in deciding whether to use cloud services for the case of a customer and where to locate the cloud in the case of a vendor.

The EU directive clearly defines the obligations which are mandatory and binding to all who process personal data [110][111]. Therefore, the directive is applicable for cloud service whenever personal data processing is involved and falls within the EU jurisdiction, the case is not much different in the US only that the vendor or customer may have to comply to different laws and regulations.

The EU directive articles 6 and 17 shows that cloud computing services are not exempt from compliance to data protections laws which provide for individual privacy and personal data protection. The articles provide for the security obligations of the data controllers and data processors with the responsibility for both technical and organizational measures that ensures privacy. They also limit how personal data can be collected and processed to the purpose for which they were initially collected. These two articles apply to cloud computing in that they limit how cloud vendors or customers can collect, and process personal data.

3.2.2. Legal regulations relevant to eHealth

The domain of healthcare and consequently healthcare IT systems is subject to a great variety of laws and regulations almost like none other [32]. This sub section describes the most notable sources of regulation relevant to healthcare IT systems. The Laws and regulations are concerning healthcare IT systems are both numerous and far reaching. Both properties account for the complexity of developing healthcare IT systems and ensuring they are compliant with the corresponding regulations.

Several causes are responsible for the large amount of regulations. For one thing, many laws were put into effect when development of healthcare products was hardly internationally coordinated and normed, therefore numerous country-specific regulations. Furthermore, some regulations apply to healthcare IT systems that initially only targeted non-computerized medical products. These laws were partly and gradually adapted to also cover IT aspects or amended by new additional laws. Lastly, federalism like in the European Union delegates certain regulatory authority to its member countries, thus creating local regulations that may have to be taken into account.

ISO Standards

International Organization for Standardization (ISO) and International Electro technical Commission (IEC) provides best practice recommendations on information security risks, management and controls through its ISO/IEC 27000-series standards. The standards cover the fundamental requirements of information management systems, provide guidelines and principles for the implementation of such systems. Among the standards, ISO 27799:2008 and ISO/TR 27809:2007 meant for health informatics. The former provides guidelines for designing health sector specific information management systems following ISO/IEC 27002. The later provides control guidelines for patient safety within such systems.

ISO/IEC Joint Technical Committee 1 (JTC1) deals with all matters of Information Technology including develop, maintain, promote and facilitate IT standards by enterprises and users concerning the security of IT systems and information.

Health Insurance Portability and Accountability Act (HIPAA)

The US congress promulgated HIPAA in order to ensure security and privacy of individually identifiable health information. HIPAA deals with security and privacy through the HIPAA privacy rule (standards for privacy of individually identifiable health information) and the HIPAA security rule (security standards for the protection of electronic health information).

HIPAA Privacy rule

The privacy rule protects the following individually identifiable health information held or transmitted by the covered entities.

- Common identifiers (e.g. name, address, birth date, social security number);
- Past, present or future physical and mental health or condition;
- Provision of health care to individuals;
- Past, present or future payment provision for health care.

However, there are no restrictions to use or disclose health information that cannot identify an individual in any way. The covered entities are permitted to use or disclose the health information for the specific purposes (e.g. treatment, payment etc.). The entities can

disclose health information for research or public interest withholding certain specified direct identifiers.

HIPAA Security rule

The security rule protects all individually identifiable health information that the covered entities create, receive, maintain or transmit in electronic form. The security rules cover the following aspects.

- Ensuring authorized disclosure, integrity and availability of all personally identifiable health information;
- Identify and protect against anticipated threats to the confidentiality, integrity and availability;
- Protect against impermissible use and disclosure of information.

The security rule demands administrative safeguards that include both the security management processes and personnel. Proper admission control to facilities and devices should be maintained. The rule advocates for technical safeguards by including access control, audit control, integrity control and transmission security.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) extends the scope of security and privacy protections available in HIPAA and the act was signed into law in 2009. In the health care industry so far HIPAA has not been rigorously enforced, HITECH provides legal liability for non-compliance. Apart from enforcing the HIPAA rules, HITECH takes into care the notification of breach and access to electronic health records. HITECH Act requires that any unauthorized use and disclosure would generate a data breach notification for example patients be noticed of any unsecured breach. The Act provides individuals with a right to obtain their electronic health records and they can also designate a third party to receive this information.

3.2.3 Legal challenges

A number of challenges emerge relating to cloud computing. These challenges may be categorized under various names and titles. For example Sotto, et al [2010] identifies some of the challenges as Privacy and security laws issues, service provider restrictions, state

Information security laws, EU regulatory issues, International data transfers and legal base for processing data in the cloud. Dr. Widmer identifies the challenges as commercial, open issues on data protection, and contractual issues. In this section the challenges are identified as; the role of the cloud service customer/provider, the applicability of EU laws, trans-border data transfers, ensuring data protection. We see these challenges covering most of the legal aspects of using cloud services.

The first challenge: the cloud service customer/provider role

The EU directive puts on the shoulders of data controllers most of the obligations for ensuring privacy and data protection of the individual, with few on the data processors [110]. In the case of cloud computing it is hard to pin cloud providers as data controllers though they process data entrusted to them by the data controller according to the directive. Therefore it is imperative that the role played by cloud vendors and customer be clearly defined to ensure compliance to the directive.

The third challenge relates to trans-border data flow.

For instance The EU directive demands that data should not be transferred outside the EU. Transfer can only take place to countries with adequacy level of protection. It also demands for contracts and notifications in case of transfers taking place. Like EU directive, when countries national regulation may affect the cloud provisioning.

The fourth challenge is that of ensuring the protection of data.

The challenge here is to ensure that both data controller and data processor have effective means of protection for data.

3.3. Compliance issues

Nature of cloud computing environment puts at risks industry and/or regulatory requirements. This is because of the difficult to force providers to comply with these regulations or industry standards. For example in using public clouds infrastructure it entails failure to comply with certain requirements such as PCI DSS, Federal Information Security Management Act (FISMA) of 2003, Gram-Leach_Billey Financial Services Modernization Act of 1990 and the European Data Protection Act of 1990 among others.

This is made difficult because these acts and regulations were not prepared with cloud computing in mind. They focused of physical asset protection (Hamilton). Compliance is also made difficult as vendors are not necessarily industry specific. This means that vendors may not be required to comply with any industry specific legislation or standard. Another aspect is that vendors may be offering their services to customers from different industry with different compliance requirements.

CHAPTER FOUR

4. Cloud Service and Provider Selection

Introduction

There are a wide, and increasing, number of providers of "Cloud", and it is open to debate whether a particular offering comprehensively matches the set of characteristics that NIST, Gartner, or any other organization might use to distinguish a "pure Cloud" offering from some technology simply rebadged to appeal to a new audience. The entity purchasing the Cloud services needs to decide what the required features are, and try to ignore the overarching labeling. It is apparent, however, that the commoditization of software, software development and systems can offer alternative ways of doing "traditional" activities. Indeed, for some, IaaS, PaaS and SaaS could be used to replace a significant majority of extant IT systems – entire businesses could run "in the Cloud".

This section provides an overview of market-leading providers of technologies that, in common parlance is either considered "Cloudy" in terms of what they provide, or relate to providing Cloud for organizations.

As discussed in chapter 2, cloud computing can refer to several different service types (SaaS, PaaS, and IaaS) and different deployment models (private, public, community, and hybrid cloud). Each service type or deployment model has its own benefits and risks [106]. Therefore, the key considerations in contracting for different types of services or deployment models should be different. In this chapter the researcher focus on identification of service and deployment models appropriate for sharing medical images in the cloud.

4.1. Cloud Services Selection

It is good for organizations to carefully considering their IT portfolios and developing roadmap for deployment and migration. These roadmaps prioritize services that have high expected value and high readiness to maximize benefits received and minimizes delivery risk. Defining exactly which cloud services an organization intends to provide or consume is a fundamental initiation phase activity in developing an agency roadmap.

4.1.1. Software as a Service (SaaS)

SaaS enables users to access applications running on a Cloud infrastructure from various end-user devices (generally through a web browser). The user does not manage or control the underlying Cloud Infrastructure or individual application capabilities other than limited user-specific application settings.

In SaaS users (healthcare professionals, patients and researcher) can access different software from the cloud:

- Messaging and collaboration System
- Electronic health records (EMRs)
- PACS
- RIS
- Patient portal systems
- Customer Relationship Management (CRM)
- Enterprise Resource Planning

4.1.2. Platform as a Service (PaaS)

With **Platform as a Service**, **PaaS**, the cloud provider hosts applications developed by the user, or on behalf of the user, using the cloud provider's operating system. In other words, the service provider offers a software platform and protocol stack on which a customer's application can run. For example, a hospital-licensed application could be managed in the cloud utilizing a MySQL or Oracle database instance offered by the PaaS provider. Image archiving is one example of using cloud services to offset the effects of the exponential growth in data and in requirements for on-demand storage.

Using the cloud, radiologists, physicians and patients do not need to physically install any specific services, solution stacks or databases on their machine. It provides the images to the users where they can simply select these images and use them on a machine provided in a cloud.

- Services
- Solution Stacks
    - Java
    - PHP
    - .NET
- Storage
    - Databases
    - File Storage

4.1.3. Infrastructure as a Service (IaaS)

In this model, the cloud user outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The provider owns the equipment and is responsible for housing, running, and maintaining it. The user typically pays on a per-use basis.

The benefits of IaaS include rapid provisioning, ability to scale and pay only for what you use. By moving your infrastructure to the cloud, you have the provision to scale as if you owned your own hardware and data center (which is not realistic with a traditional hosting provider) but you keep the upfront costs to a minimum.

Cloud Based Medical Image Archiving and Sharing (CMIAS) delivers different infrastructure at one place. It provides a platform (internally no physical infrastructure) virtualization environment in the hospitals and imaging centers. Using this, radiologists and physicians need not to set up any specific physical infrastructure for image processing, sharing and other work. CMIAS provides the following services for infrastructure as a service.

- Compute
    - Physical Machines
    - Virtual Machines
    - OS-level virtualization
- Network
- Storage

4.2. Selecting Cloud Service Providers

Once ISV has decided to adopt cloud computing (here we consider only the public cloud case), the next step is to choose a suitable cloud platform. In this section we describe three major public cloud platforms, namely, Amazon AWS, Microsoft Azure and Google AppEngine. We emphasize properties that are likely to affect the decision. For example, we describe supported languages and frameworks, runtime environment restrictions, platform-provided services and features, and pricing models.

Choosing a proper cloud provider is the most important part of the implementation plan. Different providers may offer different service models, pricing schemes, audit procedures, and privacy and security policies. Healthcare providers have to compare different offerings. Also, it needs to evaluate the provider's reputation and performance before it signs a contract.

Identification and selection of Clouds is started by analyzing the cloud service provider (CSP) that can best provide Infrastructure as a Service (IaaS), since it is the most appropriate layer to deploy the framework. In this research world-class software company's cloud offering for medical records services are candidates. These are Amazon Web Services (AWS), Microsoft's HealthVault and Oracle's Exalogic Elastic Cloud. In the following sub sections, we try to discuss services (compute, storage), price models and service level agreements of each provider.

4.2.1. Amazon Web Services

Amazon Web Services (AWS) represents a set of online services that form together a cloud computing platform. Amazon has built large-scale, reliable and efficient IT infrastructure where customers can host their applications. Currently Amazon has data centers in five regions: US East (Northern Virginia), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), and Asia Pacific (Tokyo). Besides REST based APIs, AWS has recently released a set of direct language-integrated APIs to access the cloud services.

Compute Services

Amazon Elastic Compute Cloud (EC2) service allows renting virtual machines to run custom applications on Amazon's data centers. Virtual machines or "instances" function as virtual private servers. Instances have different CPU resources, available memory, local storage space, and I/O performance, depending on the instance size. The consumers are free to choose any size and deployment region for their virtual machines. In order to instantiate a virtual machine, a user should boot Amazon Machine Image (AMI) that contains operating system with required middleware and configuration settings. It is possible to create custom AMIs or choose available preconfigured images. EC2 is very flexible and supports many operating systems, a lot of middleware, and any development platform or programming framework.

EC2 does not have built-in scaling. The users can manually change the number of instances through administration console or provided APIs. Another possibility is to use Auto Scaling service. Auto Scaling can scale applications up or down dynamically without an extra management effort.

Storage Services

Amazon Web Service offers various durable and scalable storages for different purposes.

Simple Storage Service **(S3)**: provides primary data storage for any type and amount of data. Data is stored in special "buckets" that can be located in a specified region to reduce latencies or cost. Moreover, AWS has a content delivery service for even better data distribution. The provided authentication mechanism allows the protection of sensitive information. Also, S3 has built-in redundancy support, but there is an optional Reduced Redundancy Storage (RRS) service at a lower price.

Amazon SimpleDB*:* is another service used for storing and querying over non-relational emistructured data. This storage service has a built-in replication, indexing and performance tuning features. Https endpoints ensure a secure, encrypted communication with this service. Developers can take advantage of *Amazon Relational Database Service* (RDS) to set up and operate a relational database in the Cloud. RDS provides capabilities similar to ordinary databases. In addition to that, it has an automatic replication and backup support. However,

developers can still install standard Oracle Database or Microsoft SQL Server on EC2 instances.

Pricing model and Service Level Agreements

The pricing model for AWS is quite complex. EC2 compute is billed per active instance hours. The price depends on the type and configuration. The users can optionally reserve instances. In this case they get a reduced hourly rate but have to pay in advance. Data storage is charged per GB per month. Data transfer is charged per GB in and GB out. Usually the price is lower within the same region and free within the same Availability Zone. Also, there are additional costs per transaction for some services. Prices vary across different regions.

AWS service level agreements guarantee 99.95% availability of EC2 service, 99.999999999% durability and 99.99% availability of S3 storage, and 99.99% durability and 99.99% availability of RRS. Availability time is calculated for one year period. More detailed information about the pricing model and SLAs is available on the official web site [11].

4.2.2. Google AppEngine

Google AppEngine is a PaaS offering for developing and hosting web applications on Google managed infrastructure. One of the biggest advantages of AppEngine is Google's technologies and services available for custom applications. Developers can use standard language-integrated APIs to access most of these services. A set of SDKs and an Eclipse plug-in enable full local development support. SDKs can simulate AppEngine environment on a local machine.

Compute services

AppEngine provides a secure environment where applications can be deployed. It currently supports Java, Python and Go runtime environments. Each environment provides standard protocols and common technologies for a web application development. However, regular AppEngine instances have many limitations. For example, access to other computers on the Internet is allowed only through the provided URL fetch and email services; there is a write protection for a local file system; code can be executed only in response to a web

request or a task; request has a 30 second limit. In addition to regular instance, developers can use Backends. The *Backend* is an AppEngine instance running in the background. Also, it is more flexible than a regular instance (e.g. it has a higher computational capacity limit and no request deadlines). AppEngine takes care of load balancing and scaling. Applications are scaled based on the load while data is scaled based on the size.

Storage services

AppEngine offers several options to manipulate data.

The *Data store* is used for non-relational data with high read and query performance, auto scaling and transaction support. Unlike relational databases, it supports "schemaless" entities with properties. Datastore offers two types of storage with different availability and consistency.

The Blobstore is another storage service. Developers should use the *Blobstore* for large data objects. These objects stored in Blobstore are called “blobs”. Blobs are usually created by uploading a file through an HTTP request.

Pricing model and Service Level Agreements

Google AppEngine is free for the users up to a certain level of consumed resources. But in general, resources like CPU, storage and bandwidth are billed based on the consumed amount similar to AWS. However, compute services charge per CPU circles but not “per deployment hour”. Since developers do not have a full control over the application scale, Google AppEngine

has a preconfigured cost limit of the application. SLA is currently only in a draft version that offers 99.95% availability of custom applications. If Google fails to fulfill SLA, customers receive credits for future AppEngine usage.

4.2.3. Microsoft Azure

Microsoft Azure is a relatively new PaaS offering in the cloud market. It has data centers in six areas: North and Central America, North and West Europe, East and Southeast Asia. Azure platform consists of Compute, Networking, Storage and Identity services. Figure 5.1 shows detail view of the cloud services with each category.

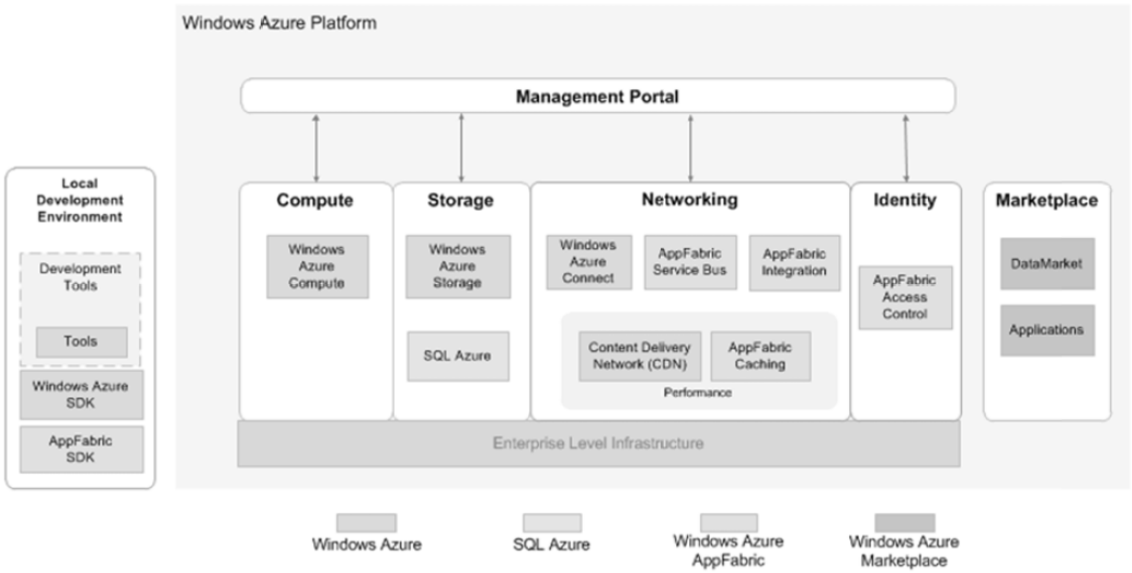

Figure 4.1: Windows Azure Platform Products and Components

Microsoft Azure provides SDKs and tools for VS2010 to enhance local development. SDKs can emulate a cloud environment on a local machine where developers can run, test and debug applications before moving to the public cloud. Azure extensively uses existing Microsoft tools and technologies like ASP.NET, NET MVC, ADO.NET, Visual Studio IDE, and Microsoft SQL. So developers can use existing experience to migrate or develop cloud applications for Microsoft Azure.

Compute Services

Azure Compute provides a special execution environment for hosted services. Services can be build from different roles. Each role represents a component with unique functionality running inside a virtual server. Azure supports three types of role: Web Role, Worker Role and Virtual Machine Role.

The Web Role is intended to run frontend web applications. It has preconfigured Internet Information Services (IIS) 7. IIS7 simplifies the hosting of applications based on web technologies like ASP.NET or WCF. It is also possible to run unmanaged code of virtually all languages including Java or PHP.

The Worker Role serves for more general purposes. It is designed to run a variety of code mostly to perform long running tasks or background processing for a web role. For

example a Web Role can be used for uploading images while a Worker Role does image processing.

The Virtual Machine Role is designed to run user-customized OS images, giving more control over the runtime environment. However, Azure supports only Windows Server 2008 R2 operating system. In contrast to Web and Worker roles that are running inside a virtual machine. VM roles are actually virtual machines. VM Role is useful when moving entire on-premise Windows Server applications to Windows Azure.

Any hosted service is usually represented by a combination of different roles; Roles can communicate with each other directly or by using Storage Services. It is possible to use different capacities for different roles instances, since every role runs in its own virtual machine.

Microsoft Azure has a built-in load balancer. It distributes the load across Web Roles to achieve better performance. Furthermore, the platform is constantly monitoring roles to provide a high level of availability. If any instance fails, a new one is reinitialized automatically. Moreover, applications have no down time during upgrades. Microsoft suggests having at least two instances of each role to achieve offered availability.

Storage Services

Azure storage provides scalable, persistent, durable storage in the cloud. It is exposed as a REST-based service. Data stored in Azure Storage can be accessed from Azure Compute of from anywhere on the Internet through HTTP. The users can configure access policies using built-in authentication. There are four storage abstractions supported by Azure Storage: Blob Storage, Table Storage, Queue Storage and Windows Azure Drive.

The Blob storage is unstructured storage that resembles a regular file system. It provides an interface for storing any named file along with its metadata. It supports a hierarchical structure, similar to a file system. File size as well as the number of files are not limited.

Pricing model and Service Level Agreements

The pricing model of Microsoft Azure is similar to other cloud offerings. The users pay only for consumed resources without any upfront investments. Though, different subscriptions are possible. Compute services are charged according to the VM instance size on hourly basis.

Compute hours is the amount of clock hours the application is deployed (regardless CPU utilization). Both staging and production deployments are counted. Storage services are charged per GB/month and a number of transactions. Storage capacity is calculated as average space used by Blob, Table, Queue, and Driver storages during the billing period. That means 30 GB used only for one day is billed as 1GB/month.

Microsoft offers a set of SLAs for services including Windows Azure Compute, Windows Azure Storage, Windows Azure CDN, etc. Most service level agreements guaranty minimum service availability and, in some cases, performance. Availability of compute services is 99.95%, of storage services – 99.9%. If these rules are violated, customers receive service credits in compensation.

Cloud Computing Providers efforts for HealthCare

Microsoft HealthVault

Microsoft developed a platform to store and maintains health and fitness information, called **HealthVault** []. It is a cloud service that helps people collect, store, and share their personal health information. HealthVault's data can come from providers, pharmacies, plans, government, employers, labs, equipment and devices, and from consumers themselves. Access to a record is through a HealthVault account, which may be authorized to access records for multiple individuals, so that a mother may manage records for each of her children or a son may have access to his father's record to help the father deal with medical issues.

Google Health

Meanwhile, Google provides a personal health information centralization services, known as **Google Health** [3]. The service allows Google users to volunteer their health records, either manually or by logging into their accounts at partnered health services providers, into the Google Health system, thereby merging potentially separate health records

into one centralized Google Health profile. Volunteered information can include health conditions, medications, allergies, and lab results. Once entered, Google Health uses the information to provide the user with a merged health record, information on conditions, and possible interactions between drugs, conditions, and allergies.

In general, HealthVault and Google Health serve as Cloud health information storages and operate separately. As consumers of different Cloud applications rely on Cloud Providers (CP) to supply all their computing needs (process, store and analyze huge sensor data and user generated data) on demand, they will require specific QoS to be maintained by their providers in order to meet their objectives and sustain their operations. To solve the problem of Cloud interoperation, an Unified Cloud Interface (UCI) standardization has been proposed.

Amazon's Cloud computing based Healthcare efforts

At an invitation-only event sponsored by Harvard Medical School and Amazon Web Services, a few dozen experts convened in Boston for a day to ponder the possibilities of cloud computing in their work. Participants included health care IT leaders, academics, biomedical researchers, medical and scientific consulting firm representatives, and officials from vendors like Amazon, Oracle, and Hewlett-Packard [54]. For its part, Amazon in recent weeks unveiled the AWS Hosted Public Data Sets, or "Public Data Computing Initiative," which provides on the cloud a "hosted-for-free, centralized public repository" for data -- such as United States census and human genome research data -- useful to researchers,

As we observed in this section, cloud platforms are unique in many ways. They not only represent different layers of the cloud stack, but also have specific services and provided features. Consequently, cloud platforms are suitable for performing the migration of existing applications in different ways.

AWS is similar to a virtual private hosting where users can control almost the entire software stack. It gives great flexibility for developers, but makes it difficult to offer automatic scalability, load balancing and failover [5]. Nevertheless, AWS has a variety of integrated services for that. A web service interface makes Amazon's offering really platform and language independent. With its level of flexibility and interoperability, AWS is suitable for the majority of existing applications.

Google AppEngine offers a high level domain-specific platform, targeting traditional web applications. AppEngine looks much like a cloud application framework. It allows automatic load balancing, elasticity and integration with other Google services, but puts applications into a very limited environment. AppEngine is a good choice for building new applications, but the migration of existing systems is likely to require significant re implementations.

Microsoft Azure intermediates between AppEngine and AWS. It resembles a lower lever application framework, providing a language-independent managed runtime with certain possibilities to control the environment. Weak points of Azure are the lack of monitoring capabilities and no built-in scaling support. Thus, the users have to purchase external tool/services or develop their own. In general, Azure fits well for the systems based on Microsoft technologies and tools. A consistent development experience is an additional advantage in this case.

Cloud-enabled systems are likely to have similar cost and performance across the platforms. However, there are some distinctions they might have. For example, Microsoft Azure tends to be slightly more expensive, but it shows considerably better I/O performance. Also, the scaling speed differs across platforms. The average time to provision an additional instance is about ten minutes in Azure, and only about one minute in AWS. However, it is highly dependent on the configuration (e.g. Windows OS boots much slower than Linux OS).

4.3. Pilot Proposed Services of the Cloud

4.3.1. Database Development Service

Using the cloud, database developers can create databases; link different databases from diverse locations implement and maintain relational databases, and retrieve information using Structured Query Language (SQL) with PHP to connect the databases in the Internet. IBM Clouds offers a database solution by providing DB2 images in their available instances which represents the OS. Healthcare software developers could to create their databases using DB2 images. DB2 images give the ability to set three different access levels: the owner, administrator, and user. The password should be entered for each access level.

Windows Azure also has another solution which provides a database solution with a user friendly interface. Building a database using Windows Azure is started with creation of

a subscription followed by creating the server with the access levels and their passwords. Then the databases are created using a .NET framework after connection of the .NET to the created server.

4.3.2. Operating Systems Service

Operating Systems is one of the most beneficial service from Cloud Computing since most of CSPs who provide platform as a service (PaaS) are providing a variety of operating systems in image form. So, healthcare providers can utilize the many OS options provided as a service and can test how the platform is done.

4.3.4. Information Management Systems

Various information systems (e.g. Personnel management system, Enterprise Resource Planning systems, Customer relation management system, hospital scheduling system) will be deployed and used by cloud users. Relevant Information Systems will be placed in the cloud and authorized users from different healthcare service providers would access it, instead of deploying the information system for each institution that costs the no of institutions times unit price of the system.

4.4. Toolkits/Frameworks For Simulate Cloud Computing

4.4.1. CloudSim

It is a toolkit for a novel framework to simulate the infrastructures and the Cloud Computing management services. CloudSim is an open source and extendible simulation, allowing users and developers to do experimental studies on Cloud Computing infrastructure for different data center models, scheduling, and allocations policies [107]. In addition, it allows use of either the time sharing or space sharing allocation. CloudSim simulates the creation and deploys the VMs on a simulated node of any virtual data center which can be used to ensure the Service Level Agreement (SLA) and the Quality of Service (QoS) for user requirements [108]. Furthermore, it allows the migration of VMs to guarantee reliability in keeping the automatic scaling feature and the bottleneck discovery.

4.4.2. GreenCloud

GreenCloud is a simulator built to reduce the power consumption in Cloud Computing data centers which the Cloud's infrastructure designer can use to direct them. It is a tool to reduce the power consumption by applying different typologies until it finds a

suitable one with an acceptable level of energy consumption with accepted QoS. GreenCloud intends to indicate the consumed energy by the data center components, such as servers and switches. It allows utilizing the power by voltage and frequency scaling, and dynamic shutdown on all data centers' components, especially the computing and networking components which consume the power primarily. The energy consumption analysis is visualized in Graphical User Interface (GUI).

4.4.3. OpenNebula

OpenNebula is the open-source industry standard for data center virtualization, offering the most feature-rich, flexible solution for the comprehensive, complete management of virtualized data centers to enable on-premise IaaS clouds in existing infrastructures. OpenNebula interoperability makes cloud an evolution by leveraging existing IT assets, protecting your investments, and avoiding vendor lock-in.

4.4.4. Aneka

Aneka is a platform for deploying Clouds developing applications on top of it. It provides a runtime environment and a set of APIs that allow developers to build .NET applications that leverage their computation on either public or private clouds. One of the key features of Aneka is the ability of supporting multiple programming models that are ways of expressing the execution logic of applications by using specific abstractions. This is accomplished by creating a customizable and extensible service oriented runtime environment represented by a collection of software containers connected together.

CHAPTER FIVE

5. Cloud Based Services for Medical Image Archiving and Sharing

5.1. Building the Framework

The current enterprise imaging environment has created the demand for a scalable archive environment, robust imaging application architecture, and the ability to access image studies based on a patient centric view of data. Imaging has moved beyond the domain of radiology and has become pervasive throughout healthcare enterprises. However, the pervasiveness of imaging does not mean that healthcare organizations have yet been able to fully integrate these new technologies with their existing systems to improve patient care. As a result, healthcare organizations must pursue a scalable, high performance and reliable medical imaging and interoperability architecture to meet these needs.

After analyzing the environment of medical imaging in detail, the researcher tries to develop a cloud base framework that meet the challenges hospitals and imaging centers face in creating integrated and highly interoperable image management systems. The response to these challenges by the researcher is Cloud base Medical Image Archiving and Sharing Framework (CMIAS). The goal of the CMIAS framework is to enable healthcare providers and research organizations to provide complete and timely access to critical imaging/diagnostic information at the point of care, regardless of the source, age or location of the information.

The presented framework namely Cloud based Medical Image Archive and Sharing (CMIAS) contains five layers (User Interface, SaaS, PaaS, and IaaS) and three modules (User log database, system security, and service management): Based on the identified services and selected Clouds, the researcher proposed a Cloud Computing framework Ecosystem for healthcare providers.

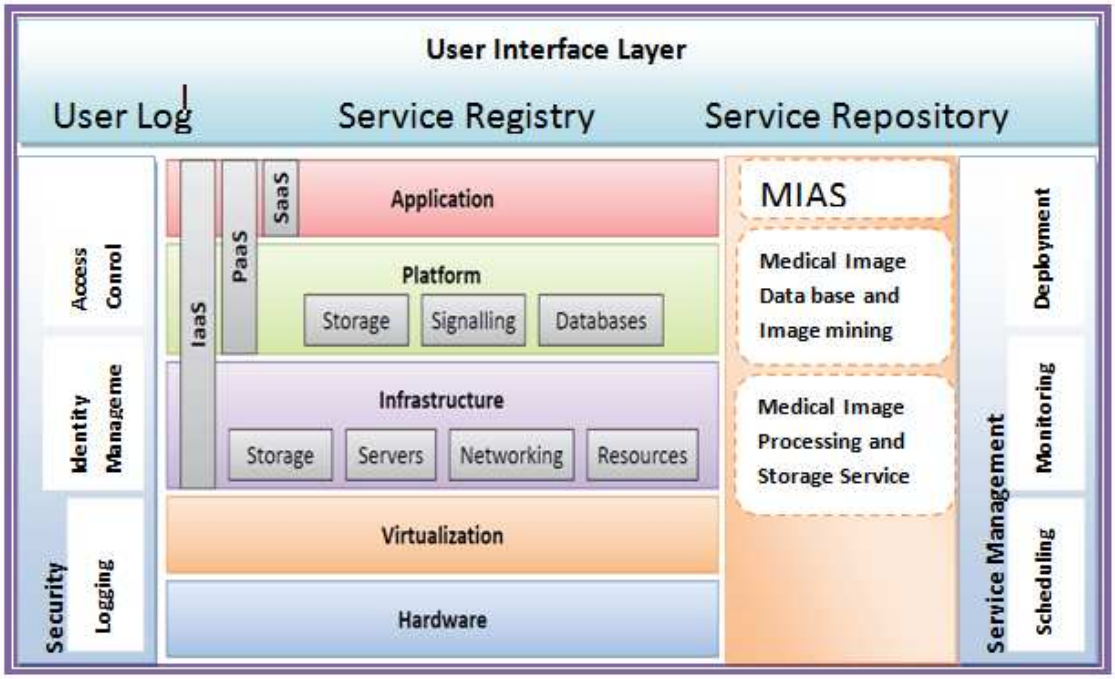

Figure 5.1: The Virtual Model of Medical Ecosystem for Users on Cloud Computing (author)

5.1.1. User Interface Layer

Because applications and data are hosted outside of the organization in the cloud computing environment, the cloud service provider has to use Authentication and Authorization mechanism. Authentication means that each user has an identity which can be trusted as genuine. This is necessary because some resources may be authorized only to certain users, or certain classes of users.

Authentication is the mechanism whereby systems may securely identify their users. Authentication systems provide answers to the questions:

Who is the user? Is the user really who he/she represents himself to be?

Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. Authorization systems provide answers to the questions:

Generally, in order to accomplish the above tasks, the layer has the following modules

- **User Portals**: provide an access path to specific web applications or services since everything is located on the web and can be accessed using a network connection.

- **Service Catalog**: contains different types of services with detailed information about the additional access information, such as what layer the service is located and who can access this specific service.
- **Service Repository:** composed of different services like EMRs, DICOM viewers, categorized and arranged depending on the service name and access level which may be in one of the three other layers (SaaS, PaaS, or IaaS).

5.1.2. Clinical Application Tier: (SaaS) Layer

The second layer in CMIAS is the Clinical Application layer. This layer provides access to hosted clinical application software in the cloud. The main service as a software in CMIAS is delivering medical imaging management solution to authorized users. In addition this layer provides the following clinical application software as a service, PACS, RIS, EMR and other clinical systems. Furthermore it provides also a web based DICOM image viewer solution.

The SaaS model is deployed over the internet or behind a firewall on a local area network. The vendor typically provides a license to use an application either as a service on demand through a subscription, or in a "pay-as-you-go" model. So, the framework enables the solution to be delivered as a service to any connected healthcare provider anytime and anywhere by any device (Smart phone, PDAs, Laptop). It is part of the utility computing model where all of the technology is in the "cloud" accessed over the internet as a service akin to the electricity grid, where end users consume power without needing to understand the component devices or infrastructure required to provide the service.

As healthcare organizations need to focus on their core competencies, the SaaS model is the most suitable in meeting clinical imaging needs and to deliver on the corporate objectives in most instances, be it improving the efficiency and driving down costs, or being agile and flexible to bring product to market faster.

In the analysis of different literatures, I choose getting medical image archiving solution as a service (SaaS) is the optimal model for healthcare institution. As it is the best model the researcher also proposed a framework how these medical imaging solutions should be designed, design framework. The framework encompasses state of the art standards and integration profiles on the industry. Figure 5.2 shows design framework of cloud based medical imaging solution.

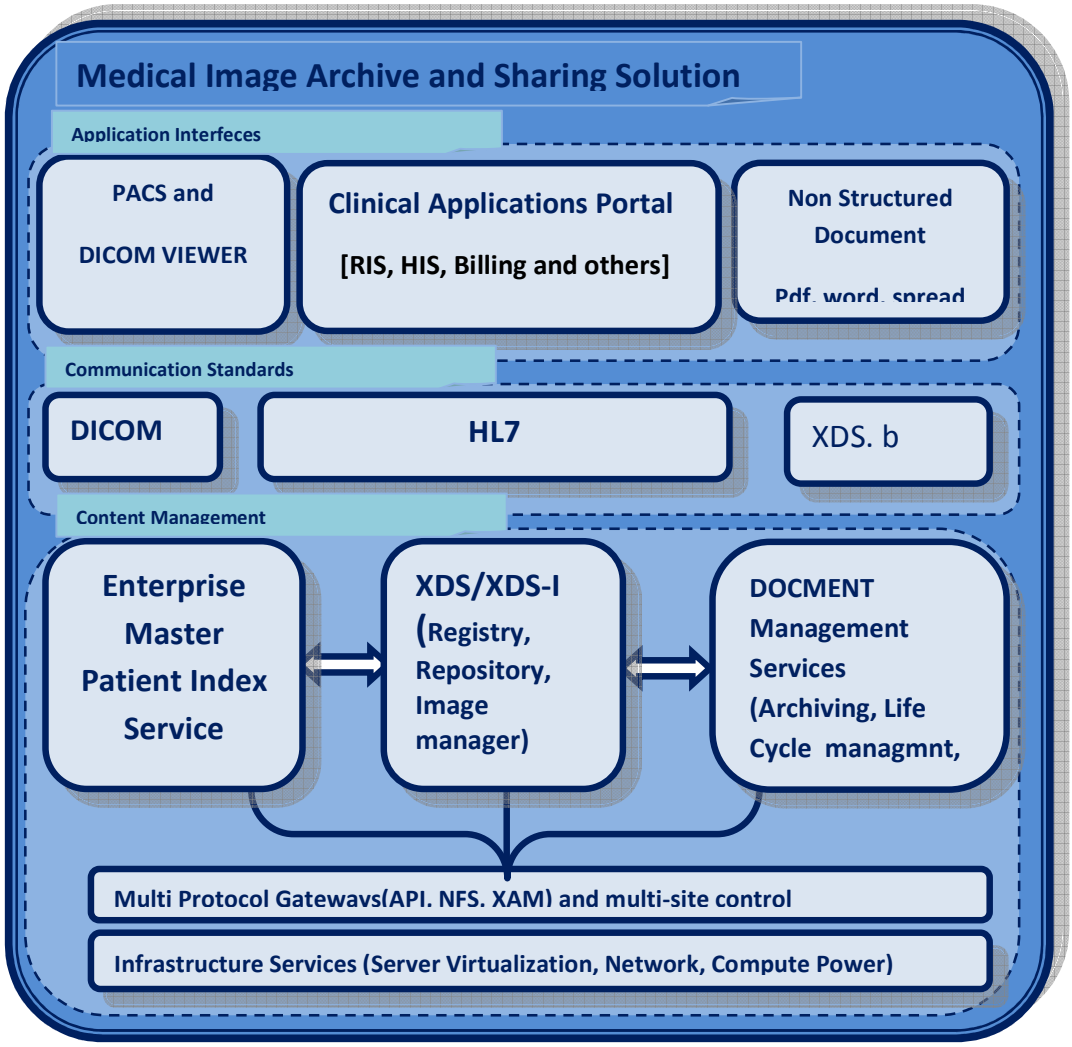

Figure 5.2: Design Framework for medical image management solutions on the cloud [author]

Components of the proposed framework

The proposed cloud based solution, medical image archiving and sharing solution, has three main tiers, application tier, standardization tier and content management tier. The details of each tier are discussed in brief as follows.

Application Tier

This tier is a gateway of different imaging related systems (such as PACS, Picture Archive Communication Systems) to utilize the solution, as a Long Term Archive to archive medical images and imaging related information. It is also a gate to unstructured data systems (.doc, xls, pdf and other files) in order to integrate them to other patient data records and images. Generally this interface allows different patient record systems to use the solution provided.

Communication Standards Tier

After different imaging related systems are interfaced by the application layer, it is time to filter them according to the data each system handles. Then the data is received by the appropriate communication standard. For instance if the system needs to upload image related report, RIS, on the Cloud, then the report is received by HL7 messaging protocol.

Content Management Tier

As shown in the framework, many tasks are done on this tier. It is a tier where images are organized according to the state of the art image sharing standard, XDS-I, the radiology tailored implementation profiles of the IHE. In addition to this, this tier also provides enterprise wide master patient index service and image management service. The combination of these Services provides key functions, such as DICOM Store & Query/Retrieve interfaces, IHE XDS/XDS-I storage and query, classification of patient data according to its content, application of differential management rules and routing of different data to different locations and to storage infrastructure components appropriate to data content. Data transformation services are also provided to match the requirements of the various clinical systems which utilize the archive, such as using the Electronic Master Patient Index (EMPI) to transform image data to a retrieving facility's local patient identifier scheme on retrieval from the archive. Each of these three Services is described below in greater detail.

Master Patient Index Service

Because imaging studies require services from multiple organizations for every patient encounter, there is an increasing need to provide patient-centric image access,

independent of where the images are stored. This increases the relevance of enterprise master patient index (EMPI) services for health information systems. Healthcare organizations rely on multiple systems handling various different data processing needs, from laboratory to billing, or from ADT *[DEFINE: HL7 Admission Discharge and Transfer (ADT) messages are used to communicate to episode details (typically inpatient episode details but may also be used for emergency details) to external applications]* to Image Manager. In today's world, each system will likely have its own patient database and its own proprietary identification schemes. When data must be transferred or correlated across domains, the ID numbers across those domains may be different. Additionally, the same ID may exist in multiple domains but identify different people, preventing access or raising the possibility of mismatched data. Errors in patient identification and variations in medical record numbers can undermine the system, leading to fragmented, inaccurate information or overlay of patient information. Such situations may cause failure to bill a patient or payer properly or mistreatment of a patient which could result in a loss of life. An EMPI is a database that contains a unique identifier for every patient in the enterprise. This would include the medical center, outpatient clinics, practice offices and rehabilitation facilities. All registration systems look to the EMPI to obtain patient information based upon several identifiers. An EMPI acts as a record locator service to facilitate access to a single source of truth for patient care data, provider information, medical records and billing information. This record locator service (RLS) eliminates redundant and inaccurate information, yielding gains in internal efficiency, as well as improving clinical and financial outcomes.

Through standards-based implementation of the EMPI, this tier creates a patient centric architecture to provide seamless access to patient data residing on multiple systems and physical locations.

The EMPI service is fully IHE compliant, built upon well-defined industry standards and protocols, such as Patient Identifier Cross-Referencing (PIX), Patient Demographics Query (PDQ), and Cross-Enterprise Document Sharing (XDS). PIX allow all enterprise participants to register the identifiers they use for patients in their domain. Participants retain control over their own domain's patient index. PIX support domain systems' queries for other systems' identifiers for their patients. The advantages offered by PIX are great. PIX allow system architects to maintain all systems' identifiers for a patient in a single location. It

allows for the use of any encapsulated algorithm to find matching patients across disparate identifier domains. It also allows for a lower cost of synchronizing data across systems, since there is no need to force identifier and format changes onto existing systems. Critically, PIX leverages standards and transactions already used within IHE.

IHE PDQ enables on-demand patient-centric access to image data across diverse systems and devices. It allows quick retrieval of a patient list including common patient names, identifiers, contacts, and visit information. It also enables selection of the correct patient when full identification data may not be available, while limiting access to only a subset of demographic and visit information.

Cross Document Exchange (XDS/XDS-I) Service

The CMIAS framework leverages IHE infrastructure profiles to integrate healthcare information within and across care delivery organizations. The framework will accept open standard systems that can provide an IHE compliant set of assets that include an industry leading XDS Registry, and XDS and Audit Repositories. These assets enable centralized search functions across distributed environments from any patient care location. This is achieved by using the XDS and XDS for imaging (XDS-I) protocols to store a brief description of clinical data and related images in a centralized database called the registry. In turn the registry then accesses patient documents and images from either the XDS repository or from source systems that feed the repository and return the integrated information to the requesting application or user.

IHE XDS enables sharing of images, reports, and other clinical data across multiple clinical departments/disciplines in multi-vendor environments. The solution automates complex routing and retrieval protocols to and from heterogeneous storage devices. Images, diagnostics reports, and evidence documents derived from the processing of images represent important components of a patient's medical record. However, they are managed and archived on a variety of imaging information systems such as RIS and PACS over the course of diagnosis and treatment.

XDS-I extends XDS by sharing, locating and accessing DICOM instances from an image manager, e.g. for radiologists or oncologists. Moreover, XDS-I may be useful for sharing cardiology and other imaging documents.

Document Management Service

The Document management service is the Service that provides the image management and workflow functions within the CMIAS. The document manager not only provides the traditional DICOM services but is also tightly integrated with the other components of the MIAS framework. It uses the industry standard PIX/PDQ interface to associate DICOM studies with the master patient ID for patients. It also acts as an XDS Source, storing Manifests within the XDS Registry and Repository and serves ups images and imaging related information to requesting applications and users.

The Document Management Service is an advanced image management software solution that facilitates an open DICOM infrastructure for any PACS or imaging environment. The DICOM Manager brokers communication between single and multiple PACS vendors, modalities, and other systems allowing federated searches across imaging systems. Built on a collaborative and extensible Cloud computing and SOA model, the Service features a flexible architecture that can aggregate and federate DICOM objects and query results, as well as virtualizes and replicate storage assets via tight integration with the Storage Virtualization Tier.

The Document management Service incorporates a content-aware router that dynamically caches, queues with priority, compresses and encrypts data through an automatic yet tightly controlled batch interface to trigger efficient packet movement to in-network storage. It is highly scalable, able to achieve truly massive storage requirements, in a centralized or fully decentralized (but centrally managed) storage environment that is not based upon any central instance. Through this robust set of functionalities and characteristics, the CMIAS's Document Management provides timely access to all imaging throughout the enterprise, regardless of application, storage or location, over the long term.

Storage sub tier

The storage sub tier is responsible for the long-term management, security and protection of the CMIAS's integrated clinical information, mainly, medical images and related reports. The selected Cloud provider storage architecture should enable logical separation of imaging and other clinical application from the storage infrastructure. Thus, it enables healthcare enterprises to extract additional utility from its existing storage

investments, or alternatively, maximize its utility from any future storage upgrades. Since it is on cloud the solution allows the entire enterprise storage infrastructure to be centrally managed like a single storage network, so that storage capacity can be automatically allocated wherever needed as it becomes available. More specifically, it exhibits best in class functionality in four areas:

1. Provides an enterprise storage platform for all of the MIAS's documents, reports and images across all applications, enterprise sites and storage tiers (e.g. disk, tape, maid, vtl)
2. Ensures uptime and availability of the MIAS applications via real time failover and automated re-synchronization and self healing functions.
3. Protects data for life via digital fingerprint and proactive data verification technology.
4. Automates storage administration functions such as replication, backup, hardware related migration and storage expansion.

4 5.1.3. Platform as a Service (PaaS) Layer

This layer provides access to different platforms- programming language, distributed systems, net-centric systems and similar platforms. At this layer healthcare system developers can easily got a developing platform and can run and test their software with resource efficient environment. Furthermore, it helps to host there the application. Another application at this layer for healthcare sector is for students of radiology department. For them it can be a platform to host legacy systems and practice their course work properly.

5.1.4. Infrastructure as a Service (IaaS) Layer

The IaaS level gives more flexibility when dealing with the Hardware layer but through virtualization. At this layer servers are configured from virtual machines and use for storage and computation purpose. The most widely used application of this tire is storage of large size of data like medical images and storing of heavy video files for media industry. Some prominent cable television stations are using Amazons EC2 storage service for their data.

In healthcare the utilization of this service is more focused on the use computational power of the unlimited resources of Cloud providers for analyzing biomedical data. In biomedical Cloud's fast computing power is used for short time genome comparison. For this purpose Cloud computing demonstrates its attractiveness properly. In other words the

experiment shows it has a significant improvement in cost and time compared to the in house IT infrastructure usage.

5.2. Proposal for Implementation Medical Image Archive and Sharing on a Hybrid Cloud

The proposed framework, Cloud based Medical Image Archiving and Sharing (CMIAS) is a hybrid cloud-based service to archive and manage clinical imaging and associated report content from any picture archiving and communication system (PACS), Radiology Information System (RIS) and other related systems. When the framework is adapted to healthcare providers, it helps any authorized user of a medical imaging application to store, search, publish and access the data regardless of the PACS vendor source. It also offers flexible solutions for hospitals and medical imaging facilities to allow clinicians to quickly access patient imaging data across multiple PACS systems at the point of care.

Hybrid Cloud is one of the Cloud Computing deployment models. It provides the ability to access, manage, and use third-party (vendors) resources from multiple CSPs and combines them within in-house infrastructure (private Cloud). Using such a model allowed us to avoid lock-in and was blocked with one CSP by allowing mix and match services from different CSPs. In addition, it will give us the ability to secure the institution's critical application and data by hosting them on the private Cloud without having to expose them to a third-party. With a hybrid Cloud model, the institution has more control of their system since part of the infrastructure is under their control. For this model, the research needs software which manages the complexities and the heterogeneity of this distributed data centers. So, the first step will be building private cloud, the next sub section discuss about how healthcare organizations can utilize their in-house infrastructure using cloud computing model.

5.2.1 Building Private Cloud

Private Cloud is a virtual IT infrastructure that is securely controlled and operated by the organization. Private cloud computing offers the controls and security of today's data center with the agility required for business innovation. Because it can be extended to affiliated organizations as part of a federated or community cloud, a private cloud can connect healthcare providers, and clinical labs that all may play a role in a patient care episode. In order to implement hybrid cloud, there is a need to choose a tool that orchestrates

the in-house infrastructure, which is used as a private cloud. So the researcher try to professionally select compare the different open source cloud infrastructure manager tools. The contest is among Apache VCL, Nimbus, OpenNebula, Eucalyptus, Enomaly, and OpenQRM.

From the platforms described above, OpenNebula stands out as the best all rounder, it supports Xen, KVM and VMware as its virtualization back ends and can use them simultaneously if care is taken to mark each virtual machine template with the appropriate hypervisor requirement. On the interface side, it features an RPC2 interface on top of which other interfaces are implemented such as part of the EC2 and OCCI interfaces.

In-house Infrastructure Orchestration by OpenNebula

It is an IaaS implementation that orchestrates network, storage and virtualization technologies to supply a single service to its end users. OpenNebula is able to orchestrate datacenter resources, as well as remote resources according to allocation policies. It is part of the Resources and Services Virtualization without Barriers (RESERVOIR) project, a European Union project that aims to enable massive scale deployment and management of complex IT services [109].

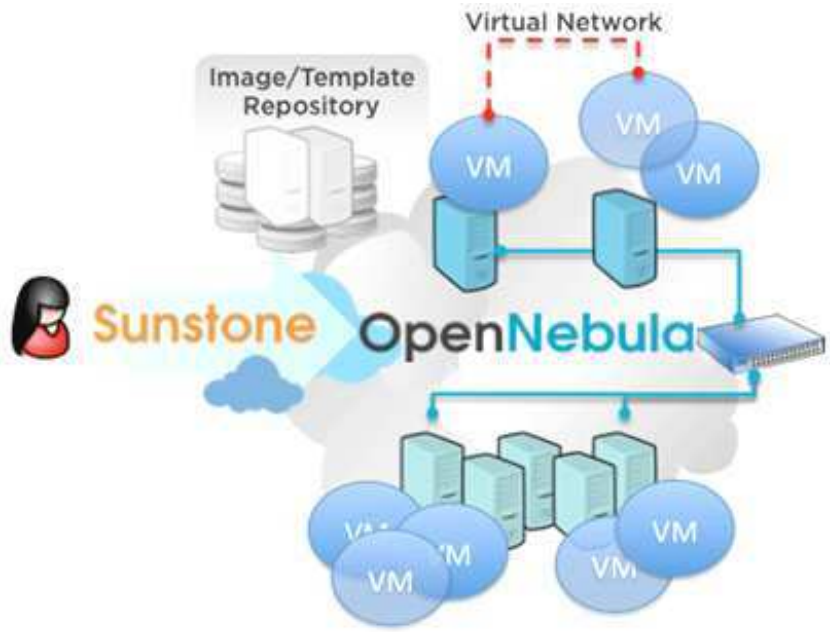

Figure 5.3: overview of OpenNebula

OpenNebula enables the creation of private and hybrid clouds, allowing any existing deployment to grow beyond existing physical resources. This is a major advantage in the event of an unexpected load peak.

Some of the main principles which guided the design of OpenNebula are full openness of architecture and interfaces, adaptability to various hardware and software combinations, interoperability, portability, integration, stability, scalability and standardization. Its main features include data-center or cluster management with Xen, KVM or VMware virtualization. It leverages the most common cloud interfaces Amazon AWS, OGF OCCI and VMware vCloud, and provides user management with authentication, multiple user rolling, secure multi-tenancy and quota management.

In the scope of cloud management a rich set of storage, virtual image, virtual machine and virtual network management features is provided. It supports cloud-bursting with Amazon EC2, simultaneous access to multiple clouds, and cloud federation. Standardization and interoperability are supported through abstraction from infrastructure and modular approach. Standard APIs includes Ruby, Java and XMLRPC. Security concerns are addressed with internal and external SSL communication and LDAP integration.

OpenNebula EcoSystem adds a set of tools, extensions and plug-in to OpenNebula Cloud Toolkit components enabling integration with existing products, services and management tools for virtualization, clouds and data centers. Telecom and hosting market and respectable scientific organizations like CERN adopted OpenNebula.

Components of Open Nebula

- Interfaces & APIs: OpenNebula provides many different interfaces that can be used to interact with the functionality offered to manage physical and virtual resources. There are two main ways to interface OpenNebula: command line interface and the Sunstone GUI. There are also several cloud interfaces that can be used to create public clouds: OCCI and EC2 Query. In addition, OpenNebula features powerful integration APIs to enable easy development of new components (new virtualization drivers for hypervisor support, new information probes, etc).
- **Users and Groups**: OpenNebula supports user accounts and groups, as well as various authentication and authorization mechanisms. This feature can be used to

create isolated compartments within the same cloud, implementing multi-tenancy. Moreover, a powerful Access Control List mechanism is in place to allow different role management, allowing a fine grain permission granting.

- **Networking**: An easily adaptable and customizable network subsystem is present in OpenNebula in order to better integrate with the specific network requirements of existing datacenters. Support for VLANs and Open vSwitch are also featured.

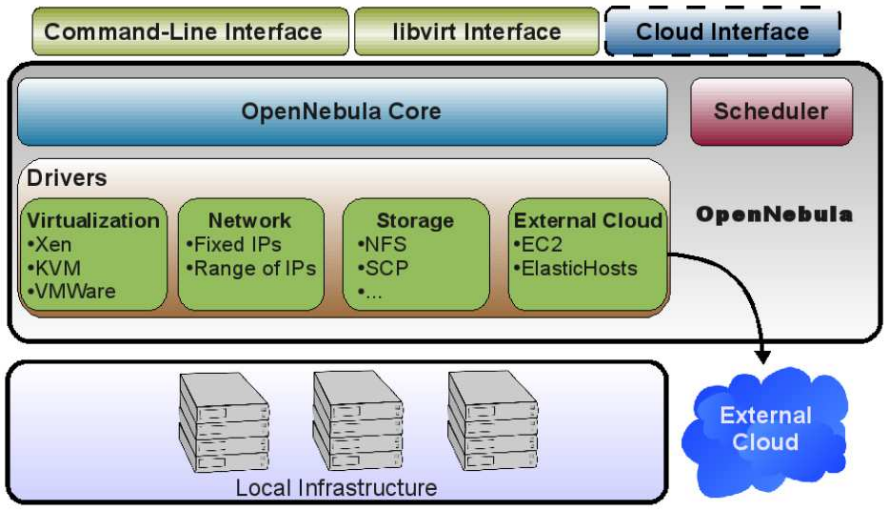

Figure 5.4: Different Services of OpenNebula

- **Hosts and Virtualization**: Various hypervisors are supported in the virtualization manager, with the ability to control the lifecycle of Virtual Machines, as well as monitor them. This monitorization also applies to the physical hosts.
- **Storage and Images**: OpenNebula aims to be flexible enough to support as many different image storage configurations as possible. The Storage subsystem can be configured to support non-shared and shared file systems, as well as a broad array of different arrangements of the image servers.

Using Aneka for Platform Development

Aneka [110], which is being commercialized through Manjrasoft, is a .NET-based service-oriented resource management platform. It is designed to support multiple application models, persistence and security solutions, and communication protocols such that the preferred selection can be changed at anytime without affecting an existing Aneka ecosystem. To create an Aneka Cloud, the service provider only needs to start an instance of

the configurable Aneka container hosting required services on each selected desktop computer. The purpose of the Aneka container is to initialize services and acts as a single point for interaction with the rest of the Aneka Cloud. Aneka provides SLA support such that the user can specify QoS requirements such as deadline (maximum time period which the application needs to be completed in) and budget (maximum cost that the user is willing to pay for meeting the deadline). The user can access the Aneka Cloud remotely through the Gridbus broker. The Gridbus broker [111] also enables the user to negotiate and agree upon the QoS requirements to be provided by the service provider.

An enterprise Grid [112] harnesses computing resources of desktop computers (connected over an internal network or the Internet) within an enterprise without affecting the productivity of their users. Hence, it increases the amount of computing resources available within an enterprise to accelerate application performance. This capability can be combined with other dedicated resources in the enterprise to enhance the overall system capability and reliability.

To support scalability, the Aneka container is designed to be lightweight by providing the bare minimum functionality needed for an Aneka Cloud node. It provides the base infrastructure that consists of services for persistence, security (authorization, authentication and auditing), and communication (message handling and dispatching). The Aneka container can host any number of optional services that can be added to augment the capabilities of an Aneka Cloud node. Examples of optional services are indexing, scheduling, execution, and storage services. This provides a single, flexible and extensible framework for orchestrating various application models.

As our framework uses OpenNebula as a base of the hybrid Cloud to orchestrate hardware, it uses Aneka on top of OpenNebula and create a platform for application development and database system storage. On other word, we use Aneka to deliver platform as a service using our internal resources. Aneka provides software infrastructure for scaling applications using broad collection of APIs for the developers to design and implement applications. Aneka gives developers the ability to run their application on a local or remote distributed infrastructure which supports the hybrid Cloud deployment model. Transferring the current system or platform to be managed and accessible within Cloud technology is a very hard task. Therefore, it needs lots of planning, preparing, testing, and changing of the

current layers and architecture of the platform to be compatible with the Cloud- based educational environment; furthermore, the need for a flexible, extensible, and accessible solution for developing and deploying the proposed framework is raised. The Aneka platform met the listed requirements mentioned above which made it one of the best solutions in our case. The Aneka platform [113] provides a flexible and configurable platform which supports multiple programming languages and gives the ability to develop and deploy the applications either on private or public Clouds as the following figure

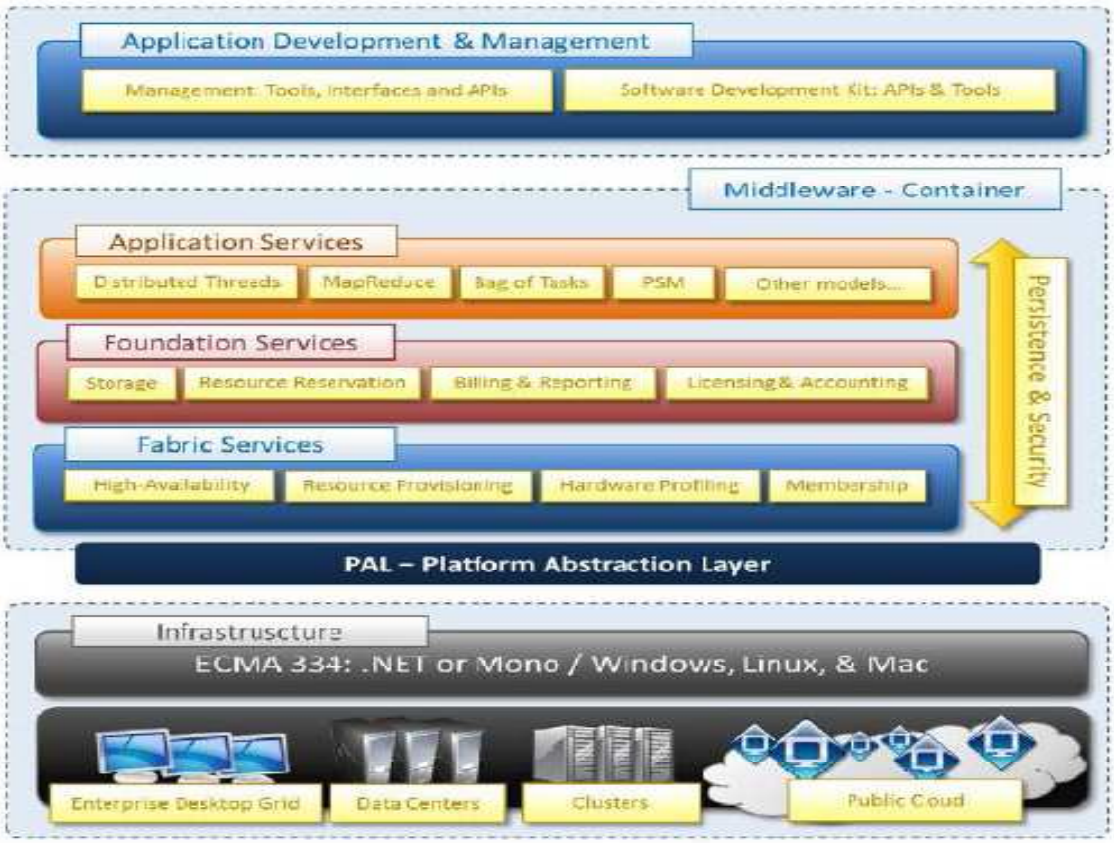

Figure 5.5: Typical Aneka Cloud deployment [113].

As shown in the above layers corresponding to the basic service layers of the Cloud Computing easily integrated with the external Cloud. Aneka enables the execution of the application on its runtime environment by using the underlying Cloud infrastructure for either private or public Clouds. It provides management tools; administrators can easily start, stop, and deploy any application. The Aneka platform contains three classes of services which characterize its middleware layer:

1. Execution Services: Their primary responsibility is scheduling and executing deployed applications.
2. Foundation Services: They represent the collection set of management services, such as metering applications and resource allocation and updating the service registry whenever needed.
3. Fabric Services: They present the lowest level of middleware services classes. They provide access to Cloud resource management to enable resource provisioning which will scale the allocated resources to the applications to achieve the required QoS.

To sum up, the proposed system stores the Medical images in the cloud and hospitals, imaging centers, consulting physicians, senior radiologists and researchers can access those details via virtual private network (VPN) and public Internet access. Fig.5.6 is the proposed construction of cloud-based MIAS. The health department establishes interface to store and manage important information such as computer-based patient records, etc.

This framework is easy to realize by adding a network module or control center just attached to existing systems. The network module is to connect within the cloud, and can use the resources in cloud to achieve hardware, software and data-storage according to the need. Using this method to optimize and reduce existing MIAS gradually, thus obtains adjustable flexible structure. It's very affordable to use cloud computing in medical IT services, many hospitals can share the infrastructure formed by connecting large number of systems together, thus the hospitals can become more efficient, and construction costs can be reduced.

At small hospitals like township hospitals, most business can be processed within the cloud, so as to get rid of the heavy burden of complete construction and management. They only need to complete the patient’s information collection and result display, the others that including management, storage, maintenance, and even disease diagnosis can be achieved in the central servers. Also large hospitals reduce its costs from this flexible and extensible framework.

Mostly scanned images are sent manually or by land mail as DVDs. Sometimes, images are sent over slow FTP connections that takes significant time and streamlining at send/receive ends. These methods are quite disconnected also. A Cloud based Image

exchange could help resolve such issues and streamline to provide physicians with 24 * 7* 365 access to medical imaging studies, easily accessible through Internet.

Furthermore, a number of small and medium size hospitals and imaging centers mostly having CT or MRI modalities are constrained to have their own internal PACS infrastructure in terms of the costs and IT resources needed to run and maintain it. An on-demand cloud based medical imaging exchange solution could help obviate such needs and can provide a model for such entities to connect their modalities and rent such services without the need to invest upfront on the PACS infrastructure and then the resources to run and maintain the PACS related IT operations.

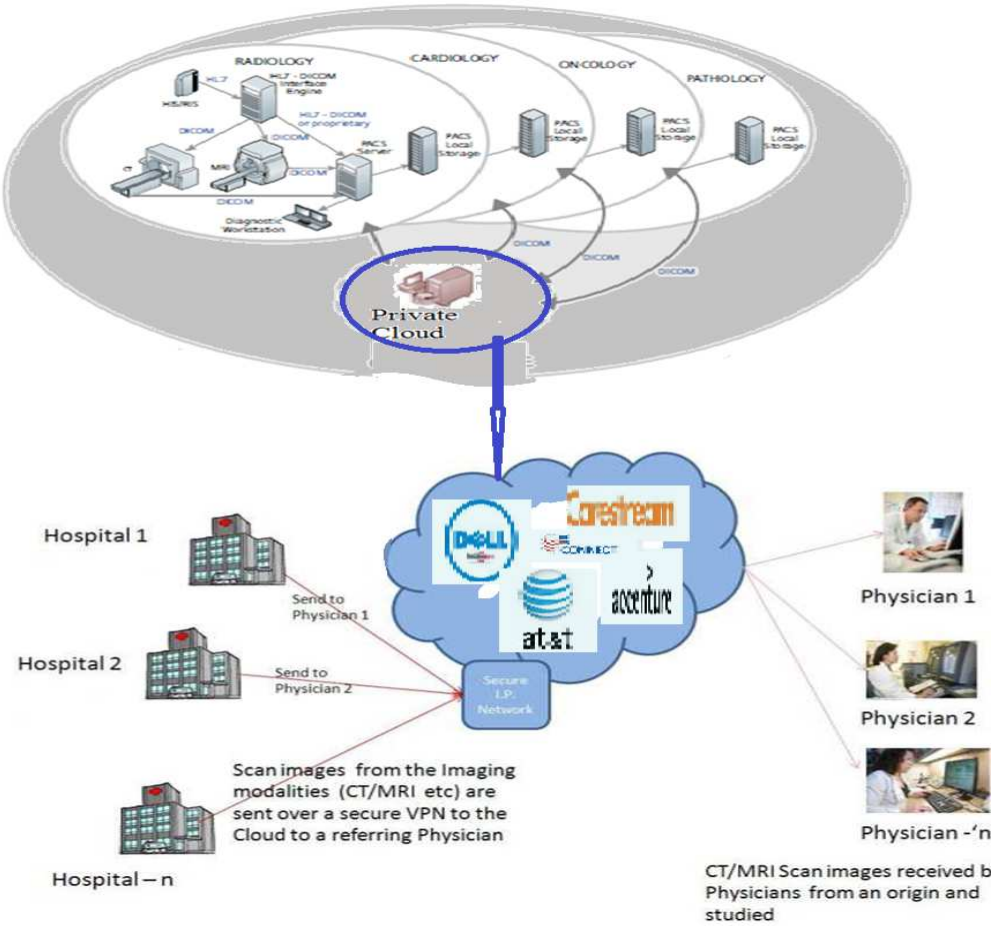

Figure 5.6: Proposed Cloud service for Medical Image Exchange and Management.

Essentially, the Cloud based solution is a PACS on-demand facilitating a DICOM imaging exchange between Hospitals/Imaging centers and Physicians. In figure 5.6 the following workflow will take place when a doctor wants the patient information.

- A Scalable Cloud Image exchange service is run. It is available on-demand and can connect with multiple medical Image producers (Hospitals or Physicians) and Image consumers (Physicians). They can be located anywhere. From Hospital 1the medical images are sent to Physician1 for studies in a secure manner.
- Physician1 connects to the Cloud service through the Internet to receive and access the images for studies and reporting.
- From Hospital-2, medical images are sent to Physician 2 for studies.
- Physician2 connects to the Cloud to receive and access the images for studies and reporting.

In this scenario, the medical images can be optionally stored and managed securely in scalable cloud storage for later studies or for disaster recovery. This scenario also applies well to large healthcare institutions having multiple imaging and medical centers spread out across the geographical locations.

CHAPTER SIX

6. MIAS Design Framework Evaluation

Introduction

This section of the study presents a synthesis of the expert survey conducted with 15 experts around the world and from amongst physicians, healthcare IT specialists and health information consultants. The survey is conducted through e-mail, web seminar discussion. Most of the respondents are members of health informatics forum.

Several respondents prefaced their remarks with a cautionary note, which amounted to a qualification in design and migration of different medical data repositories towards standard, shareable formats. Currently information like medical images is stored into data repositories that are vendor and/or system specific and make the sharing of the medical information between organizations and systems difficult or impossible within the region. This creates significant expense when integrating systems within and between organizations. It also creates significant expenses when migrating medical applications as medical data is stored in a vendor specific way and difficult to migrate to new medical applications. Since design frameworks play a great role in this context, it seems that their evaluations highly concentrate on this context.

The walkthrough of the framework is done layer by layer. That means the key summaries of respondents on each layer is presented. In each layer the respondents mention their views on the strong and weak features of the framework. Comments, if incorporated in the future, that enable the framework in its best ease are presented at last.

Clinical Application Interface layer

Respondents recognize that a good medical image archiving and sharing solution framework must have interfaces to integrate with information systems of several caregivers, such as hospital information systems, PACS, administrative tools of insurance companies, national data center. Most respondents agree on proposed design framework that, large proportion of which satisfies this requirement. The following are the observation and comments from respondents on the application interface layer.

According to Dr Shabbir, who works as a project manager of various Health IT projects like TrEHRT, LabPush and Sana-Swazi in Taiwan “the framework provides

complementary capabilities to traditional RIS/PACS integration- allowing documents, patient records, prescriptions, invoices and other unstructured content to be easily accessed via secure, virtual and federated repository". When he reason out this is because it had different interfaces to different healthcare related information systems.

Meghan Genovese, Senior Associate Director, Health Informatics Program School of Information / School of Public Health University of Michigan, attributes the interface of the framework by saying " it aggregates and reconciles all content types in a patient-centric archive". He further adds "Patient-centric view on all imaging information, DICOM or non-DICOM, available in the enterprise, independent of the source system or originating department, imaging center or hospital is very important, one of the good features this framework had".

Dr. Mohamed Khalifa, Consultant & Director, Medical & Clinical Informatics in Saudi Arabia, states his view like this " Linking data with metadata creates a user-friendly clinical data repository, which delivers greater value to the healthcare organization and ultimately the referring physician and his or her patient". So, this design framework enables to achieve this goal.

"This framework enables a scalable, vendor-neutral repository that collects and receives images and data from a variety of systems such as imaging exams, lab and pathology data, video files, JPEG images and others to create a cohesive patient portfolio", is the view of Chris Paton, health informatics consultant & honorary Senior Research Fellow in New Zealand when he state the multi interfaces the framework had.

Communication Standards (Integration and Interoperability) layer

The following are the observation and comments from respondents on the communication standards layer:

According to Francisco J Grajales, doctoral fellow in Health Care Technology in Canada, "Adherence to Industry Standards is Critical in Complex Multi-site Environments, the framework enriches this feature". When he further explains, "An intense interaction is taking place between DICOM, Health Level 7 (HL7), and their respective frameworks. This is demonstrated by a significant synergy between the RIS and PACS markets, consolidation in the industry, the development of integrated RIS-PACS solutions, and high rates of RIS/PACS integration in the market".

Werner van Huffel, healthcare IT specialist in Singapore states his view on the framework at this layer by saying “it captures unstructured data and medical imaging using HL7, DICOM and XDS standards, this makes the framework more compatible”. When he emphasizes the advantage he says “Leveraging open standard message formats to reduce the expensive point-to-point integrations that are typically required”.

Bob Hoyt, director, Medical Informatics, University of West Florida replied in this way “acceptance of connections through DICOM, HL7 and XDS.b is the optimal way.” He further explains the use of these standards by giving example, in the following way “structured reports to process HL7 notification messages regarding procedure scheduling, procedure updates, patient information updates to process DICOM modality performed procedure.”

Chris Paton also gives his view on the advantages of using open standards stating by the following way “The open architecture and standards-based connectivity support all major standards to integrate and exchange information between separate stakeholders and systems.” Since this framework uses commonly used medical data standards he states “the framework enables integration and interoperability among medical image solutions”

Content Management Layer

The following are the observation and comments from respondents on the content management layer planning phase.

Robert Nadler, Software Manager, Healthcare Informatics in USA expresses his view on the framework at this layer in the following way “Images (and other data) can be distributed at multiple sites outside the physician’s office or the health center, though there should be one source of truth for patient information that can draw from a federated information system.”, so to minimize incompatibility between different healthcare systems “Storage of any type of documents and metadata in a non-proprietary format is the task that should not be forgotten.” He expresses his positive outlook to the framework “having this feature makes this framework more attractive.”

The view of Francisco J Grajales in this layer is “unified handling of arbitrary file formats and “-ologies” (e.g., radiology, cardiology, pathology, endoscopy, oncology, urology, ophthalmology) is the immediate need medical imaging.” So, one of the great successes of this design framework is “managing these heterogeneous data together”.

Werner van Huffel is also expressing his view on management layer. As he states "actively manage data throughout its life cycle based on clinical, legal or business is one of the requirements in good framework."

Meghan Genovese, Vivian Vimarlund and John Poikonen are those who gave great emphasis on the framework since it incorporates master patient index which helps for patient-centered image access. Their view can be summarized by the expression of John as "since EMPI service is fully IHE compliant, built upon well-defined industry standards and protocols, such as Patient Identifier Cross-Referencing (PIX), Patient Demographics Query (PDQ), and Cross-Enterprise Document Sharing (XDS), providing seamless access to patient data residing on multiple systems and physical locations becomes easy." Vivian also adds in master patient index in the following way "It manages patient IDs from different sites and resolves metadata discrepancies."

Most of the respondents argue that, since the framework data management uses the industry standard PIX/PDQ interface to associate DICOM studies with the master patient ID for patients, it makes integration and availability in a good ease. They also agree on its role as an XDS Source, storing manifests within the XDS Registry and Repository and serves ups images and imaging related information to requesting applications and users.

"One of the interesting features of the framework", as stated by Bob Hoyt is "utilization of XDS framework." He reasoned out his view by "due to that, it functions as a registry, communicating with other systems such as the RIS or HIS, which are enabled through their support for DICOM, HL7, and other IT standards." Finally he continues, "The result is a centralized repository, archiving data from multiple information systems across the enterprise."

The last observation on this layer is Chris's, "unified management of clinical data, storage pools, system resources and access rights can be possible at this layer, which makes it more usable." He ends up his comment, "I am happy by seeing this feature on the framework."

The respondents reviewed the design framework and found that the framework to be useful and effective for developing medical image solution. The process of using the framework in real project highlighted a number of issues. Since the solution is cloud based it further improves medical imaging inefficiencies in a good manner, however, the respondents

also identifies areas and issues that further improves the framework in its best ease. These issues are summarized as follows:

- Incorporating advanced reporting tools that allows current and prior exams to be automatically compared. Advanced post-processing tools support analyses in such studies as cardiac and coronary CT, vessel segmentation, and PET/CT.
- Maintaining DICOM private tags should be given more emphasis. They argue this since it helps to transforms private tags to DICOM presentation states and structured reports.
- Grayscale Presentation States (GSPS) to specify presentation of images as gray scaling, zoom, text and graphical annotations should be specified in the framework.
- Key Objects (KO), To specify a particular selection of images for a specified reason and with an attached note is another feature that should be incorporated in the framework according to the view of the respondents.
- In the current situation, there may be a need of changing proprietary datasets for each PACS system by department who wants to change PACS. In this case there should be software conversion to standard neutral format. If the framework would have this feature as one component in addition to new design, migration and integration will be near.
- In addition to the image archiving and sharing services, extending it to various other archiving needs is advantages. For instance offering interfaces to utilize for example Web Services and Java technologies will make the framework more usable by many.

The results and recommendations from this walkthrough and review of literature (section 2.7.4.2, 2.7.4.3, 2.7.4.4, 2.7.4.5, 2.7.6, 2.7.7) support the hypothesis put forward. For this research it was hypothesized that: by using the developed framework, healthcare and IT managers will have a better understanding of the different key issues in designing medical image archiving and sharing solution that utilize cloud computing. The walkthrough and literatures analyzed (section 2.7.4.2, 2.7.4.3, 2.7.4.4, 2.7.4.5, 2.7.6, 2.7.7) have demonstrated that the framework is a useful tool for understanding different issues and as a tool for designing medical image solution that can be delivered as a service to both technical and business managers.

CHAPTER SEVEN

7. Conclusions and Future Work

Successful adoption of cloud computing is key for realization of benefits promised by cloud computing environment. As healthcare organizations are faced with the need for high processing capabilities, large storage capabilities, IT resource scalability and high availability, at the lowest possible cost, cloud computing becomes an attractive alternative. However, the nature of cloud computing pose challenges to organization as they consider adopting it. Issues such as security, legal and regulatory compliance become more prevalent.

The aim of the research was to investigate the challenges facing cloud computing adoption and synthesize a framework which will provide healthcare organizations with guidelines for successful cloud computing adoption by addressing the challenges identified. With the framework an evaluation survey was done that measures the adherence level to the proposed framework.

Contributions to the Body of Knowledge

The drivers and the challenges facing cloud computing adoption for medical image archiving and sharing were identified in this research. The motivation for this is the slow adoption of cloud computing by many large organizations such as healthcare organization, financial institutions and state or government agencies. Following this, a roadmap for successful adoption of clouds computing and its tools, provisioning models and design framework was synthesized. The motivation for development of the roadmap being the need to address the identified challenges and provide organizations with a tool for guidance in adoption cloud computing.

In order to achieve this, an extensive literature review on cloud computing, trust and security issues related to cloud computing, legal and compliance issues and organizational challenges for cloud adoption was conducted. The objective was to understand how healthcare organization perceives cloud computing despite its promised benefits. An extensive exploration of trust models, security standards, regulations on privacy and data protection were done. The literature revealed that most of the trust and security issues raised originate from the traditional computing environment, while those related to legal and compliance issues related to the complex nature of health data must be addressed uniquely.

Based on the findings from literature review, a survey was prepared which aimed at investigating the main concerns of issues in adopting cloud computing. The targeted survey respondents were physicians, radiologists, IT strategists, healthcare IT specialists and consultants and academicians around the world. The survey revealed that the greatest concerns were inter- operability, integration, availability, security, privacy, SLA and vendor lock-in. Other concerns were regulatory compliance, application portability and lack of standards.

The aim of the research was to develop a framework that would assist healthcare organizations in leveraging cloud computing through successful adoption. Using the results from literature review and survey, the roadmap that provides helpful guidance for successful adoption of cloud computing was developed. The framework helps healthcare providers in adopting cloud computing successfully for medical image archiving and sharing. This is in two ways, the first is provision of tools, provision models and services of cloud computing for medical imaging and in addition the design framework of medical image archiving and sharing solution identifies critical issues when developing cloud based solution. The framework was evaluated by physicians, radiologists, IT strategists, healthcare IT specialists and consultants and academicians and proved to be applicable in medical imaging context.

Following the evaluation of the framework, recommendations were drawn, that are key to successful cloud computing adoption and improvement of the framework.

Even though expert survey was limited, the results obtained reflect the positive effect of using the framework for ensuring successful adoption and development of medical image archiving and sharing in cloud computing model.

Experimentation, Evaluation and Limitation

The survey conducted as part of this research aimed at investigating advantages, challenges facing cloud computing adoption for medical imaging. The survey was conducted in two phases, for investigation and evaluation.

It was possible to synthesize the framework by the results obtained from the survey by those obtained from other researches and the findings from the literature review.

Following the results from literature review and survey a framework (utilization and design framework) were developed. The framework was then evaluated by experts and recommendations for its improvements were given.

Future Work & Research

Although the technologies underlying cloud computing have existed for nearly sixty years, cloud computing as a computing paradigm has existed for just a few short years. As a result the scope for further research is broad. This section provides some starters for future work and research. In addition healthcare providers are in infant age in adopting cloud computing in general and even for medical imaging.

There is need for more case studies to evaluate the framework. This is because in this research it was not possible. These case studies will be in enterprise to cross enterprise level. This will help to improve the framework. Another area for further research is that of assessing the social-technical impacts of cloud computing in healthcare organization.

Social-technical impact: the impact of migrating to cloud computing and its effects on the organizational culture, people and their relationships, work performance and system affordances. Research in this area should seek to answer questions such as: how does migrating to cloud affect the current work practices? Will system affordances change and how will they change?

References

[1]. Prasad, R., Ranjan, M., Chandra, S. Design and Implementation of a Cloud based Rural Healthcare Information System Model, UNIASCIT. 2012; 2 (1): 149-157.

[2]. Khmelevsky, Y., & Voytenko, Cloud Computing Infrastructure Prototype for University Education and Research. Proceedings of the 15th Western Canadian: Conference on Computing Education. Kelowna, Canada: ACM. 2010.

[3]. Katzan, H. The Education Value of Cloud Computing. Contemporary Issues In Education Research. 2010.

[4]. Behrend, T. S., Wiebe, E. N., London, J. E., & Johnson, Cloud computing adoption and usage in community colleges. Behaviour & Information Technology 2011.

[5]. http://www.ubuntunet.net/ethernet (retrieved on May 20, 2012)

[6]. Gartner, Top 10 Predictions, 2009

[7]. Image sharing and archiving, Simens white paper, available at http://www.usa.siemens.com/healthcare (accessed on June 15, 2012

[8]. Gupta, V., cloud computing in healthcare, 2011.

[9]. IBM Systems and Technology Solution Brief, Scalable, vendor-neutral image archiving solution from IBM and Acuo, 2011

[10]. *Zhang, R., Liu, L.*, Security Models and Requirements for Healthcare Application Clouds

[11]. Executive Summary: Moving Toward Multimedia Electronic Health Records: How Do We Get There? 2011.

[12]. Integrated medical image storage solutions from Comport improve patient care and trim storage costs, Solution brief, available at www.comport.com (accessed on august, 2012)

[13]. Client Computing Strategies for Healthcare Organizations, available at http://www.intel.com/about/companyinfo/healthcare/index.htm, accessed on may, 2012

[14]. AT&T Medical Imaging and Information Management, security overview, Available at www.att.com/healthcare/miim (Retrieved on March, 30 2012).

[15]. The Cloud Changing the Business Ecosystem, a publication of KPMG International Cooperative, 2011.

[16]. Jonas, A. Strategic use of IT in Radiology: A comparison between Sweden and the USA, 2005

[17]. Vaquero, L. M. A Break in the Clouds: Towards a Cloud Definition. *Computer Communication Review,* 2-5. 2009.

[18]. SHEFF, D. Crank it up; wired.com, www.wired.com/wired/archive/8.08/loudcloud_pr.html, 11/06/2010, 2003

[19]. KEPHART, J. O. & CHESS, D. M. The Vision of Autonomic Computing. *Computer Magazine.* January, 2003.

[20]. Autonomic Computing: IBM's Perspective on the State of Information Technology; IBM; 22, 2001.

[21]. LOHR, S. Google and I.B.M Join in 'Cloud Computing' Research. *The New York Times.* 2007.

[22]. GRANCE, T. The NIST Cloud Definition Framework. NIST, 2010.

[23]. Valentina, P. Cloud Computing and the Regulatory Framework for Telecommunications and Information Society Services, 2012.

[24]. Neil, R., Lorenzo V., Jonathan C., Tony S. The Cloud Understanding the Security, Privacy and Trust Challenges, technical report by RAND Corporation, 2011.

[25]. CHELLAPA, R. Intermediaries in Cloud-Computing: A new Computing Paradigm. *Cluster: Electronic Commerce*, 1997.

[26]. BUYYA, R., YEO, C. S. Cloud computing and emerging IT platforms: Vision, Hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25**,** 599 – 616, 2009.

[27]. WANG, Y. D. & EMURIAN, H. H. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21***,** 105-125, 2005.

[28]. Daryl Plummer, *Experts Define Cloud Computing: Can we get a Little Definition in our definitions"* (Gartner Blog Network, 27 January 2009) <http://blogs.gartner.com/daryl_plummer/2009/01/27 /experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/> accessed 7 January 2012

[29]. DUSTIN A., ANDREW DE A., JOE, A., JAMES B., RICHARD B. Cloud Computing Use Cases White Paper. Version 3.0, Cloud Computing Use Case Discussion Group, 2010.

[30]. Felix, N. Customer Profiling Using a Service-Oriented Architecture, 2010

[31]. WANG, L. & LASZEWSKI, G. V. Scientific Cloud Computing: Early Definition and Experience. *10th IEEE Conference on High Performance Computing and Communications.* Dalian, IEEE, 2008

[32]. Christian, N., Andreas P., Mohammad, M. R. Survey on healthcare IT systems: Standards, Regulations and Security, 2011.

[33]. Luís S. Ribeiro, Carlos, C., José, L. Current Trends in Archiving and Transmission of Medical Images, 2011.

[34]. Ng K, Rehani M X ray imaging goes digital. Digital imaging brings benefits but also demands changes in ways of working. BMJ. 2006 October 14; 333(7572): 765-766. doi: 10.1136/bmj.38977.669769.2C, 2006.

[35] RxEye http://www.rxeye.net/ (last accessed 10/04/11). 2011

[36]. Størkson, S., Aslaksen, A. Six months of experience with a XDS-based communication platform for radiology in the Western Norway health care region. International Journal of Computer Assisted Radiology and Surgery Volume 4, Supplement 1, 2009, 168-170, DOI: 10.1007/s11548-009-0321-2, 2009

[37]. R-Bay http://www.r-bay.org/ (last accessed 10/04/11), 2009.

[38]. Peeter R. Data Sharing and Shared Workflow in Medical Imaging, TUT Press, 2011

[39]. Saluse, J., Aaviksoo, A., Ross, P., Tiik, M., Parv, L., Assessing the economic impact/Net benefits of the Estonian Electronic Health Record System (digimpact), 2010.

[40]. Telerays http://www.telerays.com/ (last accessed 10/04/11), 2011.

[41]. Virtualrad http://www.virtualrad.com/ (last accessed 10/04/11), 2011.

[42]. Real Time Radiology https://www.realtimeradiology.com/ (last accessed 10/04/11), 2011.

[43]. Geenhalgh, T., Stramer K., Bratan, T., Byrne, E., Russell, J., Mohammad, Y., Wood, G., Hinder, S. Summary care record early adopter programme, 2010.

[44]. Winblad, I., Hämäläinen, P., Reponen, J. What is found positive in healthcare information and communication technology implementation? - the results of a nationwide survey in Finland. Telemed J E Health. 2011 Mar;17(2):118-23.

[45]. Thrall, JH. Reinventing radiology in the digital age: part I. The all-digital department. Radiology. 2005 Aug; 236(2):382-5

[46]. Thrall, JH. (2007a) Teleradiology. Part 1. History and clinical applications. Radiology 2007; 243:613-7

[47]. Fridell K, Aspelin P, Felländer-Tsai L, Lundberg N. The effect of PACS on the practice of orthopaedic surgeons. J Telemed Telecare. 2011, Jan 26.

[48]. Pohjonen H, Ross P, Blickman J. Extending the radiological workplace across the borders. Medical Imaging and Informatics. Lecture Notes in Computer Science, 2008, Volume 4987/2008, 12-17, DOI: 10.1007/978-3- 540-79490-5_3.

[49]. Castro, D. Explaining international IT application leadership: Health IT. The Information Technology & Innovation Foundation. Policy Issues. 2009, September 22. http://archive.itif.org/index.php?id=291 (last accessed 10/04/11)

[50]. **Ross P**, Pohjonen H. Images crossing borders: image and workflow sharing on multiple levels. Insights into Imaging, 2010; 2(2): 141-148

[51]. Kenny LM, Lau LS (2008) Clinical teleradiology - the purpose of principles. Med J Aust 2008; 188: 197-198

[52]. Thrall JH (2007b) Teleradiology. Part 2. Limitations, risks and opportunities. Radiology 2007; 244:325-8

[53]. Huang, H. PACS and Imaging Informatics: Basic Principles and Applications. John Wiley & Sons. Inc., Hoboken, New Jersey, USA, 2010.

[54]. HL7 Health Level Seven International (HL7), 2011 (last accessed 10.04.2011). http://www.hl7.org/.

[55]. Directive 98/34/EC (1998) Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations. http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:204:0037:0048:EN:PD F (last accessed 10/04/11)

[56]. IHE (2011c) Integrating the Healthcare Enterprise (IHE). http://www.ihe.net/ (last accessed 10.04.2011)

[57]. Fernandez-Bayó J IHE profiles applied to regional PACS. Eur J Radiol. 2010 Jun 24. doi:10.1016/j.ejrad.2010.05.026

[58]. Siegel EL, Channin DS. Integrating the Healthcare Enterprise: a primer Part 1. Introduction. Radiographics. 2001 Sep-Oct;21(5):1339-41.

[59]. ACC, HIMSS and RSNA (2009). Integrating the Healthcare Enterprise. IHE IT infrastructure technical framework supplement 2007-2008. Basic Patient Privacy Consents (BPPC). Copyright 997-2007:ACC/HIMSS/RSNA http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Supplement_BPPC_TI_2007_08_15.pdf

[60]. Lugnegard, H. Technical White Paper. XDS-I - Cross-enterprise document sharing for imaging. DOC-HEJM-7BR92U-2.0 ©2010 Sectra Imtec AB, 2010.

[61]. IHE Integrating the Healthcare Enterprise. IHE IT Infrastructure Technical Framework Supplement: Cross-Community Patient Discovery, 2008. Copyright © 2009: IHE International. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Supplement_XCPD_PC_2009-08-10.pdf

[61]. IHE b IHE IT Infrastructure (ITI) Technical Framework Supplement. Cross-Enterprise Document Workflow (XDW). Draft for Public Comment. Copyright © 2011: IHE International, Inc. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XDW_Rev-1-0_PC_2011-06-03.pdf (last accessed 10/04/11)

[62]. Pariso C, Saccavini C, Zalunardo L, Cocchiglia A (2010) Cross-enterprise Document Workflow (XDW) Detailed profile proposal and development plan. Arsenal IT, Veneto´s Research Centre for Health Innovation. IHE 2010. ftp://ftp.ihe.net/IT_Infrastructure/iheitiyr9-2011-2012/Technical_Cmte/Profile_Work/XDW/XDW_Flyer.pdf (last accessed 10/04/11)

[63]. Healthcare Terminologies. Healthcare terminologies and classifications: An action agenda for the United States. American Medical Informatics Association and

American Health Information Management Association Terminology and Classification Policy Task Force. 2006

[64]. IHTSDO (2011) International Health Terminology Standards Development Organization (last accessed 10.04.2011) http://www.ihtsdo.org/.

[65]. IHE Integrating the Healthcare Enterprise (IHE). 2011c. (last accessed 10.04.2011) http://www.ihe.net/

[66]. ISO 17115:2007. http://www.iso.org/iso/iso_catalogue.htm (last accessed 10/04/11)

[67]. Pohjonen H, **Ross P**, Kamman R, Blickman J. Pervasive access to images and data – the use of computing grids and mobile/wireless devices across healthcare enterprises. IEEE Transactions on Information Technology in Biomedicine. 2007 Jan; 11 (1):81-6 17249406

[68]. Wang KC, Filice RW, Philbin JF, Siegel EL, Nagy PG Five levels of PACS modularity: Integrating 3D and other advanced visualization tools. J Digit Imaging. 2011 Feb 8. PMID: 21301923

[69]. Medical Insight Adaptive streaming – overview of concept and technologies, 2009. Copyright © 2009 by Medical Insight A/S. (last accessed 10/04/11) http://www.medicalinsight. com/images/stories/pdf/ medical_insight adaptive_streaming.pdf

[70]. DeJarnette W. What is a Vendor Neutral Archive? Copyright © DeJarnette Research Systems, Inc., 2009. (last accessed 10/04/11) http://www.himss.org/content/files/ DeJarnetteWhitePaper _WhatVendorNeutralA rchive.pdf

[71]. Benjamin M, Aradi Y, Shreiber R (2009) From shared data to sharing workflow: merging PACS and teleradiology. Eur J Radiol. 2010 Jan;73(1):3-9. Epub 2009 Nov 14

[72]. Werb S, Sitka L. Vendor neutral archive. VNA – Whitepaper. © 2011 - Acuo Technologies®. http://www.acuotech.com/pdf/VNA_Whitepaper- 2011.03.15.pdf (last accessed 10/04/11), 2011.

[73]. Tera Medica (2011) Vendor neutral archive. Copyright © 2001 - 2011, TeraMedica Inc. http://www.teramedica.com/solutions/vendor-neutral-hyperarchive. html?showall=1 (last accessed 10/04/11)

[74]. Foster I, Kesselman C, Tuecke S (2001) The anatomy of the grid: enabling scalable virtual organizations. Int J High Perform Comput Appl. 2001;15(3):200- 22

[75]. Erberich G (2007) Globus MEDICUS – Federation of DICOM medical imaging devices into healthcare grids. From genes to personalized healthcare: Grid solutions for the life sciences. N Jacq et al. IOS Press, 2007

[76]. Berman F, Fox G, Hey AJG (2003) Grid computing: making the global infrastructure a reality. New York: John Wiley and Sons; 2003

[77]. Sharma A, Pan T, Cambazoglu BB, Gurcan M, Kurc T, Saltz J (2009) VirtualPACS--a federating gateway to access remote image data resources over the grid. J Digit Imaging. 2009 Mar; 22(1):1-10. Epub 2007 Sep 18

[78]. Faggioni L, Neri E, Castellana C, Caramella D, Bartolozzi C (2010) The future of PACS in healthcare enterprises. Eur J Radiol. 2010. doi:10.1016/j.ejrad.2010.06.043

[79]. The Healthgrid White Paper (2008) Integrated roadmap II. 2008. TSHARED6.2TTT. http://eu-share.org/about-share/ (last accessed 10/4/11)

[80]. Pechet TC, Girard G, Walsh B (2010) The value teleradiology represents for Europe: a study of lessons learned in the U.S. Eur J Radiol. 2010 Jan; 73(1):36-9. Epub 2009 Dec 23

[81]. Directive 95/46/EC (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri= CELEX: 31995L0046:EN:HTML (last accessed 10/04/11)

[82]. Directive 2002/58/EC (2002) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

[83]. Health Information Technology (2010) Nationwide health information network: Overview. The Office of the National coordinator for Health Information Technology. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1142&parentname =Co mmunityPage &parentid=4&mode=2 (last accessed 10/04/11)

[84]. Lundberg N, Wintell M, Lindsköld L (2010) The future progress of teleradiology-an empirical study in Sweden. Eur J Radiol. 2010 Jan;73(1):10-9. Epub 2009 Dec 22

[85]. Pohjonen HK, Ross P, Blickman JG, Christensen L (2006) The status of structured reporting in imaging: special focus on remote reporting. ECR 2006, Book of abstracts. European Radiology Supplements 2006; 16(1):166

[86]. Winblad I, Hämäläinen P, Reponen J (2011) What is found positive in healthcare information and communication technology implementation? - the results of a nationwide survey in Finland. Telemed J E Health. 2011 Mar;17(2):118-23

[87]. Ribeiro, L. S., Blanquer, I., Costa, C. & Oliveira, J. L. (2011). On demand ihe xds document registries on the cloud, *international Journal of Computer Assisted Radiology and Surgery*, Springer, pp. 297–298.

[88]. Vivek, K. Federal Cloud Computing Strategy, February, 2008

[89]. Rolim CO, Koch FL, Westphall CB, Werner J, Fracalossi A, Salvador GS. A cloud computing solution for patient's data collection in health care institutions. 2010.

[90]. Nkosi MT, Mekuria F. Cloud computing for enhanced mobile health applications. In: Proceedings of the IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom), 2010.

[91]. Rao GSVRK, Sundararaman K, Parthasarathi J. Dhatri: a pervasive cloud initiative for primary healthcare services. In: Proceedings of the 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN). New York, NY: IEEE; 2010

[92]. Koufi V, Malamateniou F, Vassilacopoulos G. Ubiquitous access to cloud emergency medical services. In: Proceedings of the 2010 10th IEEE International Conference on Information Technology and Applications in Biomedicine (ITAB). New York, NY: IEEE; 2010

[93]. Avila-Garcia MS, Trefethen AE, Brady M, Gleeson F, Goodman D. Lowering the barriers to cancer imaging. In: eScience 2008: IEEE 4th International Conference on eScience. New York, NY: IEEE; 2008.

[94]. Bateman A, Wood M. Cloud computing. Bioinformatics 2009;25(12):1475

[95]. Kudtarkar P, Deluca TF, Fusaro VA, Tonellato PJ, Wall DP. Cost-effective cloud computing: a case study using the comparative genomics tool, roundup. Evol Bioinform Online 2010;6:197-203.

[96]. Chao-Tung Yang; Lung-Teng Chen; Wei-Li Chou; Kuan-Chieh Wang; Implementation of a medical image file accessing system on cloud computing On page(s): 321 – 326, 2010.

[97]. How Trend Micro's innovative security solutions help healthcare organizations address risk and compliance challenges, Trend Micro Healthcare Compliance Solutions, 2011.

[98]. SCHNEIR, B.The Psychology of Security. schneir.com, 2008.

[99]. http://incubator.apache.org/deltacloud/

[100]. Michael Armbrust, Above the clouds: A berkeley view of cloud computing, *Technical Report UCB/EECS-2009-28*, EECS Department, University of California, Berkeley, 2009.

[101]. CSA: Top Threats to Cloud Computing V1.0; Cloud Security Alliance, 2010; 14.

[102]. BSI b BS ISO/IEC 27001:2005/BS 7799-2:2005: Information Technology-Security Techniques-Information Security Management Systems-Requirements. British Standards Institution, 2005.

[103]. ISACA COBIT Framework for IT Governance and Control; ISACA, http://www.isaca.org/Knowledge-Center/COBIT/pages/Overview.aspx, 2010, 2/4/2010.

[104]. HUSTINX, P. (2010) Data Protection and Cloud Computig under EU law; Panel IV: Privacy and Cloud Computing: in. *Third European Cyber Security Awareness Day*. BSA, European Parliament, European Parliament

[105]. ROBINSON, N., GRAUX, H. [Technical Report] Review of the European Data Protection Directive; Information Commissioner's Office; TR-710-ICO, 2009.

[106]. Sotomayor, B., Montero, R. S., Llorente, I. M. & Foster, 'Virtual Infrastructure Management in Private and Hybrid Clouds ', IEEE Internet Computing, September/October 2009

[107]. Bahsoon, R, 'Green Cloud: Towards a Framework for Dynamic Self-Optimization of Power and Dependability Requirements in Cloud Architectures', WSRCC-2 Papers Software Research and Climate Change A blog for community building, (2010).

[108]. Buyya, R., Ranjan, R. & Calheiros, R. N. 'Modeling and Simulation of Scalable Cloud

Computing Environments and the Cloudsim Toolkit: Challenges and Opportunities', Proceedings of the 7th High Performance Computing and Simulation Conference, Leipzig, Germany, (2009) .

[109]. Simões, T., Architectures for cloud computing based information systems, 2010.

[110]. X. Chu, K. Nadiminti, C. Jin, S. Venugopal, and R. Buyya. Aneka: Next-Generation Enterprise Grid Platform for e-Science and e-Business Applications. In *Proceedings of the 3th IEEE International Conference on e-Science and Grid Computing (e-Science 2007)*, Bangalore, India, Dec. 2007.

[111]. S. Venugopal, R. Buyya, and L. Winton. A Grid Service Broker for Scheduling e-Science Applications on Global Data Grids. *Concurrency and Computation: Practice and Experience*, 18(6):685-699, May 2006.

[112]. A. Chien, B. Calder, S. Elbert, and K. Bhatia. Entropia: Architecture and Performance of an Enterprise Desktop Grid System. *Journal of Parallel and Distributed Computing*, 63(5):597-610, May 2003.

[113]. Vecchiola, C., Chu, X., Mattess, M. & Buyya, 'Aneka-Integration of Private and Public Clouds 'In: Buyya, R., Broberg, J. & Goscinski, A. Cloud Computing: Principles and Paradigms, (2011).

APPENDIX

Questioners in order to asses issues related to adopting cloud computing for medical image archiving and sharing

1. What are the challenges of medical imaging in the current healthcare scenario?
2. What are the advantages and disadvantages of image sharing?
3. Do you think sharing medical images will have a positive impact on quality of care? If yes, in what way?
4. Who are the beneficiaries when medical images are shared (physicians, radiologists, patients, healthcare organizations or others)? Please specify each in detail with their benefit
5. What things should be done, prerequisites, or required for effective medical image sharing?
6. In your opinion, what are the technologies used currently for sharing medial images?
7. What are the challenges in using these technologies?
8. Could you believe cloud computing has the potential to enhance medical image archiving and sharing? If yes in what way?
9. Could you describe the derivers and inhibiters of cloud adoption in medical imaging?
10. Do you believe a road map is required in order to adopt cloud for medical purpose?
11. What do you think the most challenge of adopting cloud computing for medical imaging?
12. Cloud you list services, tools, provisioning models and providers appropriate for medical imaging?
13. Which provisioning model (private, hybrid, community, public) is better for medical image archiving and sharing?

Expert Survey Questioners

1. How do you see the framework's clinical application interfaces, where medical image archiving and sharing solution will request and provide information to other systems that are typically reside at the point of patient care?
    a. Do you feel in the interfaces are enough? If not mention to be added?
    b. What are the positive and negative impacts of these interfaces on provisioning of quality medical image solution
    c. What are the impacts of these interfaces on the framework?
2. Do you feel that the communication standards used in the framework are appropriate in support of information exchange between systems implemented in a large variety of development environments (technical) and communication environments?
    a. Does the framework used most recognized communication standards/
    b. Do the standards support variety of data formats (image, metadata and unstructured data)?
    c. Have you noticed new feature in this framework in the utilizing more standards?
    d. Do you feel there is an excluded standard that must be incorporated? If yes please specify.
    e. Do those standards enable to safely and effectively share information across a disparate and heterogeneous healthcare enterprise?
3. What is your view on the third layer, content management layer?
    a. Do you satisfied with the way the framework handles DICOM Store & Query/Retrieve services?
    b. Does the framework consider providing reliable access to patient data across the enterprise?
    c. Does the framework's application of differential management rules and routing of different data to different locations and to storage infrastructure components appropriate to data content?
    d. Do you think there is missed feature that must be added? If so, please specify.

4. What is your opinion on providing this solution as a service (SaaS delivery model) through cloud computing?
    a. Does this make an impact in letting healthcare professionals to only focus on their task, rather than IT issue? Please specify it.
    b. Do you believe cloud computing is attractive for medical image management? In what way?
5. Do you believe this design framework will be help full for developing integrated and interoperable medical image archiving and sharing solutions?
6. Do you think the presented framework provides a viable solution to the problem in medical image archiving and sharing?
7. If you feel something uncovered about this framework, please let me know?