Asian Journal of Science and Applied Technology
ISSN: 2249-0698 (P) Vol.2 No.1, 2013, pp.20-29

DOI: https://doi.org/10.51983/ajsat-2013.2.1.743

A Secure Approach for Storing and Using Health Data in a Private Cloud Environment

K. Pullarao[1] and K. Thirupathirao[2]

[1]Lakireddy Bali Reddy College of Engineering, School of Computer Science, Mylavaram - 521 230,
Andra Pradesh, India

Email: pullarao@outlook.com

(Received on 13 February 2013 and accepted on 28 May 2013)

Abstract – **Cloud computing is an upcoming technology in the field of IT industry. Cost reduction, speed processing, simple accessibility and scalability are the important features of cloud computing. Cloud is robust authentication and more secured technology and it spread in many areas like healthcare sectors in which storing patient information securely more important. The major issues involved in the cloud computing is data confidentiality, data sharing among geographical locations, storing data. This paper provides survey on privacy, security issues and a brief summary about opportunities in cloud. Also it provides a start-up of traditional medical scenario, problems in the current scenario, benefits by adopting cloud in e-health sector and issues arising during adoption of cloud in e-health domain. A methodology of private cloud Iaas is proposed for storing patient and health data in cloud environment.**

Keywords: **Patient Data, Data Confidentiality, Data Sharing, Data Storage, Multi Cloud, Hybrid Cloud, Private Cloud.**

I. Introduction

To make the right and effective decisions at right time in the field of health care, the hospital information system must be high quality, relevant reliable, accurate and high quality. The information is made available, updated, stored to different persons as physician, nurses, professors, researchers, health insurance personnel, [8] [9]etc., involved in health care. The patient information is of type text, images, and multimedia data etc.., this data useful to patient care [7], administrative and business management, monitoring and evaluating medical care services, epidemiological and clinical research, and planning of medical care resources. Important functionalities of health care information are quick, simple access of patient data. So this access having (i) effective and complete (ii) independent of geographical locations.

II. Related Work

As cloud computing is an emerging and new technology researchers are interested to do research in this area. Only some of researchers are worked in the field of cloud computing and e-health. Lejiang *et al.* (2010) research aimed to present the defects of traditional hospital patient management system. Authors conclusion is that cloud computing is best platform for improving efficiency in use of medical records. Gottlieb *et al.* (2005) said that easy and quick access of medical records would helpful in patient's emergency situations. Ajay *et al.* (2011), has been proposed model based framework to implement cloud computing and presented problems faced by developing countries in e-health care systems. osterhaus *et al.* (2010), has explained the cloud computing technologies, privacy issues in cloud, the impact in health care systems. Hans *et al.* (2010) explained general problems in e-health care systems; provide a solution for privacy of sensitive data and usability of e-health systems. All of above authors discussed the problems arises in traditional hospital patient management systems, what are the current problems faced in e-health care systems, the solutions to overcome those problems, the challenges faced in e-health systems, how cloud is an idle solution for privacy, quick access of medical records for fast treatment.

III. Present Scenario

The present health care record management system is shown in figure 1. [13] It is a paper-based system. Main drawbacks of this system don't allow easy access of records, time consuming, and lack of availability geographically.

The health care industry takes minimal use of computers and databases to store patient data [12]. In this traditional way patient keep the personal health record (PHR) with him every time whenever go to checkups.

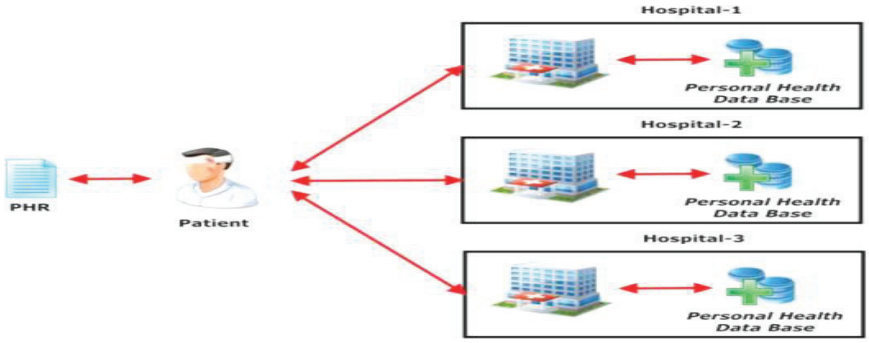

Fig. 1 Health care record management system

A. Problems in traditional health care systems.

(i) The quality and storage of electronic files is limited to hardware devices. (ii).speed of systems is depend on bandwidth used by internet. (iii). In traditional systems backup mode is very limited, so the issues security and long term usage of medical records is compromised.(iv). the sharing of resources [10] are not possible as traditional systems don't use the advantages of cloud computing. For to overcome these type of Issues related to medical field [11] we need to adopt cloud based services.

B. Benefits of adopting cloud computing in e-health systems.

1. Scalability: Hospitals reduced the cost of unused hardware and servers with adoption of cloud. Hospitals need to pay what type of services they use. The maintenance cost of hardware like upgrades are made easy.

2. Data Storage: Different type of data like video tutorials, health records and hospital data are stored on servers. The sensitive information as personal details are not maintained because they will maintain remotely on global servers and shared by different hospitals. Video files are also stored in cloud but the accessibility of video files may be low, because it is commonly shared by multiple users. Quality storing of data depends on how much we are able to invest in companies for connection on cloud. The main problem with storing data is maintaining data centres outside of country, it causes feel of low security.

3. Data Sharing and Data Availability: patient data is shared among hospitals, pharmacy, health insurance companies, physician portals, mobile health app, ambulances etc., with the use of cloud. With help of cloud the patient data is easily accessed by doctors. Doctors give the prescription based on the patient's old records. When medical data is moved to cloud it is shared from anywhere/anyplace in the world. In cloud rapid application development is possible so it is possible to keep storage centre within hospital or any other place. By getting permission of patient the information is accessed from anywhere.

4. Reliability and Efficiency: cloud provider is responsible to provide more reliable and efficient data to customers over cloud. Efficiency leads to speed up of services and get fast results. On demand services, automation are important feature of cloud computing.

5. Cost Reduction: In cloud with the sharing of resources notable cost reduction possible. In cloud the external company will maintain and manage everything, and we just pay to what we use. The company uses fewer employees, less investment it leads to reduction of cost. Patients want more security to their data compared to cost, because their data is shared among hospitals.

IV. Security Principles in Cloud

Following is a sample of cloud security principles that an enterprise security architect needs to consider and customize:

1. Services running in a cloud should follow the principles of least privileges.
2. Isolation between various security zones should be guaranteed using layers of firewalls – Cloud firewall, hypervisor firewall, guest firewall and application container. Firewall policies in the cloud should comply with trust zone isolation standards based on data sensitivity.
3. Applications should use end-to-end transport level encryption (SSL, TLS, IPSEC) to secure data in transit between applications deployed in the cloud as well as to the enterprise.
4. Applications should externalize authentication and authorization to trusted security services. Single Sign-on should be supported using SAML 2.0.
5. Data masking and encryption should be employed based on data sensitivity aligned with enterprise data classification standard.
6. Applications in a trusted zone should be deployed on authorized enterprise standard VM images.
7. Industry standard VPN protocols such as SSH, SSL and IPSEC should be employed when deploying virtual private cloud (VPC).
8. Security monitoring in the cloud should be integrated with existing enterprise security monitoring tools using an API.

Table I Potential Solutions to The Cloud Computing Challenges

Challenges	Resources	Solution Summary
Management and technical issues	Armbrust et al [1]	Solutions to handle technical, policy, and business issues
	Buyya and Ranjan [2]	References to handle cloud-federated management issues
	Kuo et al [3]	XML-based mediator to handle data lock-in problems
Security and legal issues	Cloud Security Alliance [4]	Solutions to handle cloud governance and operation issues
	NIST[a] guidelines [5]	Recommendations to deal with security and privacy issues
	Ward and Sipior [6]	Five strategies for handling data jurisdiction issues

Cloud computing in hospital patient information management system is explained with help of following scenarios.

1. *Scenario 1:* Data sharing - In this patient data sharing will happen between different health organizations when moving from one place to another place. In present systems when we visit a hospital our data is stored on their local databases. However we visit a remote location hospital our data is in accessible from old hospital. In this situation we move from starting onwards, it is both costly and time consuming process. Such type of wasting of time may put patient life in danger. Data availability throughout the world is beneficial for fast treatment to the patient. The issues like privacy, security and trust must be resolved by getting patient permission before moving data into cloud. After completing treatment patient records is updated by hospital personnel or patient himself/herself and then uploaded to the previous hospital private data.
2. *Scenario 2:* Data storage - The concept of data storage is explained with help of figure 3. Patient is able to store all type of his/her data like old medical records, prescription, x-rays in cloud with proper authentication process. Patients can also store their every day diet related information in cloud and give permission to his/her personnel doctor and gym instructor. So the patients are up to date by following their instructions.

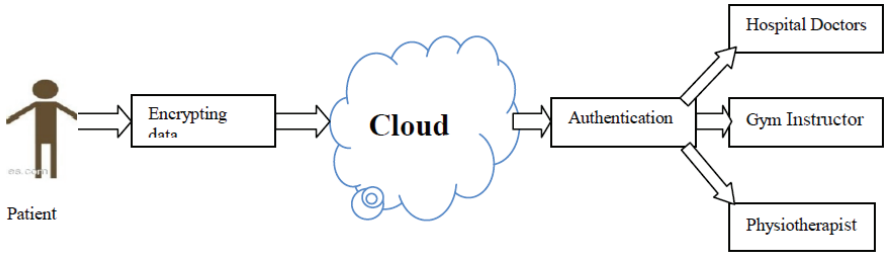

Fig. 2 Data storage architecture

3. *Scenario 3:* Multi cloud - Figure 4 describes about availability of information in cloud environment. For uninterrupted services multi cloud is the best option. If cloud is down or cloud provider goes belly up then also the hospital management system can access their data from second cloud. In this cost of data storing is not a big issue, but security is major while using multi cloud.

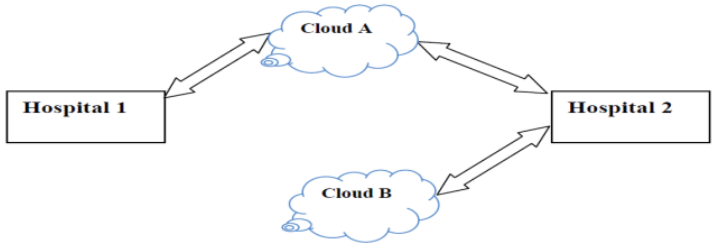

Fig. 3 Availability of information in cloud

A. Service Models

1. *Software as a Service* - Software as a Service (SaaS) delivers business processes and applications, such as CRM, collaboration, and e-mail, as standardized capabilities for a usage-based cost at an agreed, business-relevant service level. SaaS provides significant efficiencies in cost and delivery in exchange for minimal customization and represents a shift of operational risks from the consumer to the provider. All infrastructure and IT operational functions are abstracted away from the consumer.

2. *Platform as a Service* - Platform as a Service (PaaS) delivers application execution services, such as application runtime, storage, and integration, for applications written for a pre-specified development framework. PaaS provides an efficient and agile approach to operate scale-out applications in a predictable and cost-effective manner. Service levels and operational risks are shared because the consumer must take responsibility for the stability, architectural compliance, and overall operations of the application while the provider delivers the platform capability (including the infrastructure and operational functions) at a predictable service level and cost.

3. *Infrastructure as a Service* - Infrastructure as a Service (IaaS) abstracts hardware (server, storage, and network infrastructure) into a pool of computing, storage, and connectivity capabilities that are delivered as services for a usage-based (metered) cost. Its goal is to provide a flexible, standard, and virtualized operating environment that can become a foundation for PaaS and SaaS. IaaS is usually seen to provide a standardized virtual server. The consumer takes responsibility for configuration and operations of the guest Operating System (OS), software, and Database (DB). Compute capabilities (such as performance, bandwidth, and storage access) are also standardized. Service levels cover the performance and availability of the virtualized infrastructure. The consumer takes on the operational risk that exists above the infrastructure.

TABLE II COMPARISON OF CLOUD SERVICE MODELS

Type	Consumer	Services provided by cloud	Service level coverage	Customization
Saas	End user	Applications finishing	Performance of application. Uptime of application	Minimal to no customization
Paas	Owner of application	Environment to run application code Cloud storage Other cloud services such as integration	Availability of environment Performance of environment No application coverage	High degree of application customization within constraints of the service offered
Iaas	Application owner or IT provide middleware, OS and application support	Virtual server Cloud storage	Availability of virtual server Time to provision No platform or application coverage	Minimal constraints on applications installed on standardized virtual OS builds

Two dimensions are used to classify the various deployment models for cloud computing:

- Where the service is running: On customer premises or in a service provider's data centres.
- Level of access: Shared or dedicated.

B. Deployment Models

Deployment models (shared or dedicated, and whether internally hosted or externally hosted) are defined by the ownership and control of architectural design and the degree of available customization. The different deployment models can be evaluated against the three standards - cost, control, and scalability.

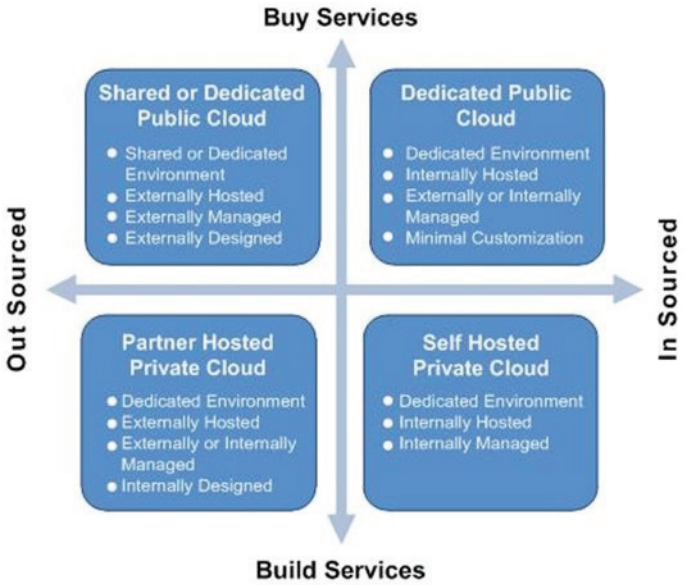

Fig. 4 Deployment models

1. Public Cloud - The Public Cloud is a pool of computing services delivered over the Internet. It is offered by a vendor, who typically uses a "pay as you go" or "metered service" model. Public Cloud Computing has the following potential advantages: you only pay for resources you consume; you gain agility through quick deployment; there is rapid capacity scaling; and all services are delivered with consistent availability, resiliency, security, and manageability. Public Cloud options include:

A. Shared Public Cloud: The Shared Public Cloud provides the benefit of rapid implementation, massive scalability, and low cost of entry. It is delivered in a shared physical infrastructure where the architecture, customization, and degree of security are designed and managed by the provider according to market-driven specifications.

B. Dedicated Public Cloud: The Dedicated Public Cloud provides functionality similar to a Shared Public Cloud except that it is delivered on a dedicated physical infrastructure. Security, performance, and sometimes customization are better in the Dedicated Public Cloud than in the Shared Public Cloud. Its architecture and service levels are defined by the provider and the cost may be higher than that of the Shared Public Cloud, depending on the volume.

2. Private Cloud - The private cloud is a pool of computing resources delivered as a standardized set of services that are specified, architected, and controlled by a particular enterprise. The path to a private cloud is often driven by the need to maintain control of the service delivery environment because of application maturity, performance requirements, industry or government regulatory controls, or business differentiation reasons. For example, banks and governments have data security issues that may preclude the use of currently available public cloud services. Private cloud options include:

A. Self-hosted Private Cloud: A Self-hosted Private Cloud provides the benefit of architectural and operational control, utilizes the existing investment in people and equipment, and provides a dedicated on-premise environment that is internally designed, hosted, and managed.

B. Hosted Private Cloud: A Hosted Private Cloud is a dedicated environment that is internally designed, externally hosted, and externally managed. It blends the benefits of controlling the service and architectural design with the benefits of data centres outsourcing.

C. Private Cloud Appliance: A Private Cloud Appliance is a dedicated environment that procured from a vendor is designed by that vendor with provider/market driven features and architectural control, is internally hosted, and externally or internally managed. It blends the benefits of using predefined functional architecture, lower deployment risk with the benefits of internal security and control.

Table III Comparison of Cloud Deployment Models

Deployment type	Hosting location	Shared or dedicated	Architectural control	Scalability	Investment
Shared public cloud	External	Shared	Provider or market	Minimal constraints	Pay as you go
Dedicated public cloud	External	Partially or fully dedicated	Provider or market	Constrained by contract	Pay as you go
Self-hosted private cloud	Internal	Fully dedicated	Self	Constrained by capital investment	Build the cloud, share services
Hosted private cloud	External	Fully dedicated	Self	Constrained by capital investment or contract	Varies by contract, may or may not have capital impact
Private cloud appliance	Internal	Fully dedicated	Provider	Constrained by offering	Varies by contract may or may not have capital impact

Our reference architecture will be based upon the NIST definition as we define the core principals, concepts and patterns used throughout the reference architecture and subsequent implementation guidance in this content series. The reference architecture will consist of reference frame that outlines the overall cloud computing stack based on the NIST definition and defines the core principals, concepts and patterns of good reference architecture. This is then followed by service delivery guidance to guide the business on solution based delivery of an on-premise private cloud infrastructure. The reference architecture presented contain practices that are independent of any specific platform provider and generally should be present on any Infrastructure as a Service platform or service engagement available from or through a provider of cloud based computing capability. Where applicable we will link with solution implementation guidance that is based on the use of Microsoft Server products to illustrate the capability discussed in the reference architecture.

V. Reference Model For Private Cloud

In the content above we describe several characteristics, service models and deployment models that are aligned to the NIST definition of cloud computing. Now we couple this with Infrastructure layer components that are briefly described in the Blueprint for Private Cloud Infrastructure as a Service and expand the Infrastructure Layer in the Private Cloud Reference Model. This expanded reference model illustrated in the figure below shall be the basis of the Private Cloud Infrastructure as a Service architecture design contained in this series.

Throughout the Infrastructure as a Service series the focus will be upon the Infrastructure Layer of the Reference Model however as illustrated the Infrastructure Layer has a light coupling with the Management Layer and the Platform Layer. Further the Infrastructure and Management Layers are influenced by the Operations Layer. Certain key areas of the Management Layer such as Fabric Management are covered in detail in this Infrastructure as a Service series while remaining areas of the Management, Operations Layer and Service Delivery Layers are covered in later or future content in the Private Cloud Reference Architecture. We can now define that Private Cloud Infrastructure as IaaS is an advanced state of IT maturity that has a high degree of automation, integrated-service management, and efficient use of resources. Virtualization can be a key enabler of IaaS but in most models, including the NIST cloud definition, virtualization as common, not and essential, attribute. An infrastructure that is 100 percent virtualized may have no process automation; it might not provide management and monitoring of applications that are running inside virtual machines (VMs) or IT services that are provided by a collection of VMs. In addition to virtualization, several other infrastructure-architecture layers are required to achieve the essential cloud attributes. A rich automation capability is

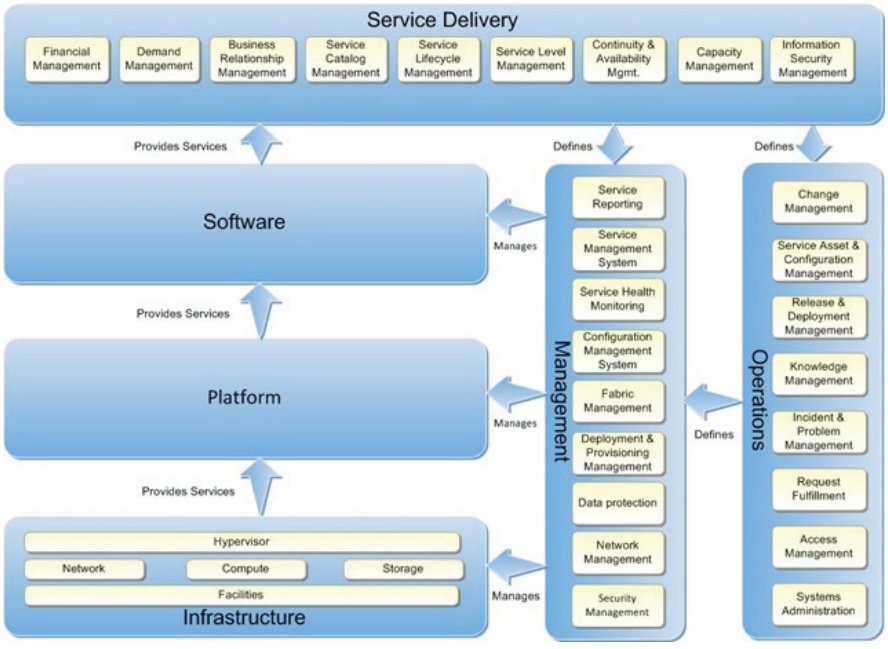

Fig. 5 Reference model for private cloud./ http://www.infoq.com

required. Automation must be enabled across all hardware components including server, storage, and networking devices as well as all software layers, such as operating systems, services, and applications. The Windows Management Framework which comprises Windows Management Instrumentation (WMI), Web Services-Management (WS-Management), and Windows Power Shell is an example of a rich automation capability that was initially scoped to Microsoft products, but that is now being leveraged by a wide variety of hardware and software partners.

A management layer that leverages automation and functions across physical, virtual, and application resources is another required layer for higher IT maturity. The management system must be able to deploy capacity, monitor health state, and automatically respond to issues or faults at any layer of the architecture. Orchestration that manages all of the automation and management components must be implemented as the interface between the IT organization and the infrastructure. Orchestration provides the bridge between IT business logic, such as "deploy a new web-server VM when capacity reaches 85 percent," and the dozens of steps in an automated workflow that are required to actually implement such a change. The IaaS solution's primary purpose is to host other higher layers such as the PaaS and SaaS. The final layer is the Service Delivery layer providing interfaces for both service providers and service consumers. The integration of virtualization, automation, management, and orchestration layers provides the foundation for achieving the highest levels of IT maturity.

A. Private cloud Iaas Design Considerations

Several key concerns must be established that are cross cutting in the overall design of a Private Cloud Infrastructure as a Service design.

1. Data - Centres and Location - The physical data centres is the enterprise facility where the organizations cloud capability is deployed. When providing cloud services we generally think of services that just exist and not where they exist. However the physical data centres we must consider location. For some organizations their data centres may exist in one or more corporate locations. For large organization there may be dedicated facilities just for location of their data centres. Increasingly these considerations include locations that offer climates that enable the use of nature air to provide environmental climate control within the data centres and reducing energy consumption. Location may also provide access to low cost costs for energy consumed by the data centres. Location of a data centres plays an active role in the design of Private Cloud Fault Domains and options available to the IT consumer when selecting capabilities to purchase and deploy through Private Cloud Self Service.

2. Scale Units - The Private Cloud Reference Architecture defines the private cloud pattern of a Scale Unit. However there is no specific predefined set or selection of values that comprise a scale unit. The determination is part of the private cloud design and planning process. A Scale Unit is a pool of compute, storage, and network resources that can be deployed as a single unit or in bundles that allow both extensibility and reuse or reallocation without physical reconfiguration. Examples of these resources are:

- Compute – Blade servers, deployed by one or more racks at a time.
- Storage – Enterprise SAN, with disk capacity to match compute capability.
- Network – New access and distribution designs to meet compute and storage requirements.

3. Resource Pools - A resource pool is comprised of server, network, and storage scale units that share a common hardware and configuration baseline but does not share a single point of failure with any other resource pool other than the facility itself. Note that a resource pool could be subdivided further into Fault Domains.

4. Fault Domains - The Physical Fault Domains pattern is defined in the Private Cloud Reference Architecture. In an Infrastructure as a Service design a fault domain is a set of physical infrastructure with a common configuration within a resource pool that does not share a single point of failure with any other fault domain.

5. Upgrade Domains - An upgrade domain is infrastructure within a resource pool that can be maintained, take offline, or upgraded without downtime to the workloads running in the resource pool.

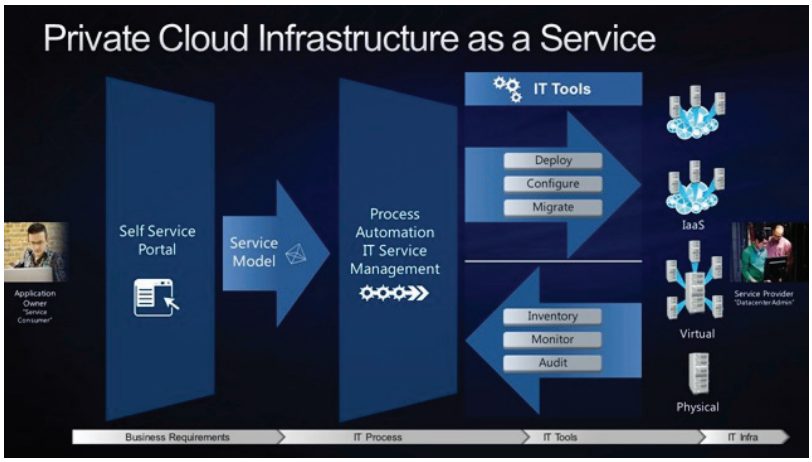

Fig. 6 Private cloud Iaas

B. Cloud Security Threats and Mitigation

Does cloud computing exacerbate security threats to your application? Which emerging threats are relevant? Which traditional threats are amplified or muted? Answers to these questions are dependent on the combination of cloud service deployment and operational models in play. The following table illustrates the dependencies which should be taken into consideration when architecting security controls into applications for cloud deployments:

In addition to the aforementioned threats to information confidentiality and integrity, threats to service availability need to be factored into the design. Please remember that the basic tenets of security architecture are the design controls that protect confidentiality, integrity and availability (CIA) of information and services.

Table IV Cloud Security Threads and Mitigation

	Public/Hybrid Cloud –Threats	Private Cloud - Threats	Mitigation
IaaS	Data leakage (inadequate ACL) Privilege escalation via management console mis-configuration Exploiting VM weakness DoS attack via API Weak protection of privileged keys VM Isolation failure	Data theft (insiders) Privilege escalation via management console mis-configuration	Hardening of VM image Security controls including encryption, multi-factor authentication, fine granular authorization, logging Security automation - Automatic provisioning of firewall policies, privileged accounts, DNS, application identity (see patterns below)
PaaS	[In addition to the above] Privilege escalation via API Authorization weakness in platform services such as Message Queue, NoSQL, Blob services Vulnerabilities in the run time engine resulting in tenant isolation failure	[In addition to the above] Privilege escalation via API	

VI. Conclusion

Cloud computing is an emerging technology, but there are many issues involved during adoption of cloud in e-health. The main aim of this paper is to explore the issues like opportunities, barriers, and challenges for adoption of cloud in e-health. In public talk Cloud computing considered as unsecure, so it progress in health sector is not as expected. To aware about cloud computing vendors should conduct workshops, demonstrate about system security, proper training to health care personnel and other stockholders. The considerable issues during cloud adoption take place are data storage and reliability, trust of patient and data centre location, Cost savings, ease of use, etc.., important point to

remember is due to lack of knowledge about cloud computing and computer knowledge in health care sectors. People are uncomfortable about data security, data integrity, and more dependent on technology, vendors. Our reference model of private cloud Iaas will definitely helpful to overcome security issues in data storage. We clearly mention about the differences among cloud deployment models, cloud service models, and the security threats among public and private clouds.

VII. References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz and A. Konwinski, et al. "EECS Department, UC Berkeley", Above the Clouds: A Berkeley View of Cloud Computing. Technical Report. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[2] R. Buyya and R. Ranjan, "Special section: Federated resource management in grid and cloud computing systems", *Future Generation Comput Syst,* Vol.26, No.8, pp.1189-1191, 2010.

[3] MH. Kuo, AW. Kushniruk and EM. Borycki, "Design and implementation of a health data interoperability mediator", *Stud Health Technol Inform,* Vol.155, pp.101-107, 2010.

[4] W. Jansen and T. Grance, "National Institute of Standards and Technology", US Department of Commerce. Guidelines on Security and Privacy in Public Cloud Computing, 2011.

[5] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, 2009.

[6] BT. Ward and JC. Sipior, "The Internet jurisdiction risk of cloud computing", *Inf Syst Manag,* Vol.27 No.4, pp.334-339, 2010.

[7] X. Zou, Y. Dai, B. Doebbeling, and M. Qi, "ependability and Security in Medical Information System", *HCII,* pp.549–558, 2007.

[8] J. M. Fonseca, A. D. Mora, and C. Ana Marques, "A Multi-Agent Information System For Bioprofile Collection", *CIMED,* Portugal, 2005.

[9] A. Appari, and M. Eric Johnson, "Information security and privacy in healthcare: current state of research", *Int. J. Internet and Enterprise Management,* Vol.6, No.4, pp.279-314, 2010.

[10] L. K. Gottlieb, et al., Regulatory and policy barriers to effective clinical data exchange: Lessons learned from medslnfo-ED. *Health Affairs,* Vol.24, No.5, pp.1197-1204, 2005.

[11] J. M. Fessler and F. Grimy, "Ethical Problems in Health Information Systems", *Method Inform Med,* Vol.40, pp.359-361, 2001.

[12] K. Häyrinen, K. Saranto and P. Nykänen, "Definition, structure, content, use and impacts of electronic health records: A review of the research literature", *International Journal of Medical Informatics,* Vol.77 No.5, pp.291–304, 2008.

[13] G. Lejiang, et al. "The building of cloud computing environment for e-Health", *IEEE,* 2010.

[14] K. Thirupathi Rao, P.Sai Kiran and L.S.S.Reddy. "Energy Efficiency in Datacenters through Virtualization: A Case Study", *Global Journal of Computer Science and Technology.* Vol. 10 Issue 3 (Ver 1.0), April 2010.

[15] K. Thirupathi Rao, P. Sai Kiran and L.S.S. Reddy. "High Level Architecture to Provide Cloud Services Using Green Data Center", *Advances in Wireless and Mobile Communications I*SSN 0973-6972 Vol.3, No.2, pp. 109–119, 2010.

[16] K. Thirupathi Rao, L.S.S. Reddy, P. Sai Kiran and V. Krishna Reddy. "Genetic algorithm for energy efficient placement of virtual machines in cloud environment", *International Conference on Future Information Technology* (ICFIT 2010).

[17] K. Thirupathi Rao, "Prospective of Cloud Computing", *IJCC Volume* I/Issue 1/2012