Smart and Secure Healthcare Administration over Cloud Environment

Govinda.K[1], Rajkumar.R[2], Gowthaman.A[3]

[123]*School of Computing Science Engineering, VIT University, Vellore, India*

Abstract - *Cloud computing is an emerging technology that is expected to support internet scale critical applications which could be essential to the healthcare sector. Its scalability, resilience, adaptability, connectivity, cost reduction, and high performance features have high potential to lift the efficiency and quality of healthcare. With the widespread application of healthcare Information and Communication Technology, constructing a stable and sustainable data sharing circumstance has attracted rapidly growing attention in both academic research area and healthcare industry. Cloud computing is one of long dreamed visions of Healthcare Cloud (HC), which matches the need of healthcare information sharing directly to various health providers over the Internet, regardless of their location and the amount of data. This paper, proposes tool related to secure health information sharing and integration.*

1. INTRODUCTION

With the development in healthcare and economic fields, greater number of medical records is generated. There is urgent need and demand to improve the levels and standards of modern health-care records management by using innovative technology. The objective of this study is to introduce the concept of Cloud Computing and discuss the challenges of applying Healthcare Cloud (HC) to improve the Health Information Science research. With the new concept of Cloud Computing emerging in recent years, more and more interests have been sparked from a variety organizations and individual users, as they increasingly intend to take advantage of web applications to share a huge amount of public and private data and information in a more affordable way and reliable IT architectureThis document is template. We ask that authors follow so.

More specifically, the medical and health information system based on the cloud computing is desired, in order to realize the sharing of medical data and health information, coordination of clinical service, along with the effective and cost-containment clinical information system infrastructure via the implementation of a distributed and high-integrated platform.

Since health informatics seek new ways of driving health information science research forward, for example, international research collaboration, growing demands are now placed on computer networks to provide hardware and software resources and pave a new avenue to share sensitive and private medical data from different geographic locations. This new model of service (Cloud Computing) offers tremendous opportunities for the collaborative health information science research purpose; unfortunately, it has also introduced a set of new and unfamiliar challenges, such as lack of interoperability, standardization, privacy, network security and culture resistance. In this paper, we will identify the challenges of applying healthcare cloud in the health information research and discuss potential approaches to conquer those barriers, such as audit, disaster recovery, legal, regulatory and compliance.

Finally, the paper will focus on the security of Cloud Computing applied in the health information science research. Research on the various security issues surrounding healthcare information systems has been heated over the last few years.

2. LITERATURE REVIEW

The advent of cloud computing in recent years has increased a lot of interests from different stakeholders, business organizations, institutions and government agencies. The growing interest is fueled by the promised new economic model of cloud computing which brings a change from heavy IT infrastructure invest for limiting resources that are internally managed and owned to pay per use for IT service owned by a service provider. Cloud computing paves a new avenue to deliver enterprise IT. As all major disruptive changes in technology and Internet revolution, it represents an innovative democratized of Web computing. Cloud computing not only upgrade the business models and the way IT infrastructure is being consumed, but also the underlying architecture of how we develop, deploy, run and deliver applications.

Mell and Grance (2010) give a definition of cloud computing that is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resource that can be rapidly provisioned and released with minimal management effort or service-provider interaction. We have already seen similar more limited applications for years, such as Google Docs or Gmail. Nevertheless, cloud computing is different from traditional systems [2]. Armbrust et al. introduce that cloud computing offers a wide range of computing sources on demand anywhere and anytime; eliminates an up-front commitment by cloud users; allows users to pay for use of computing resources on a short-term basis as needed and has higher utilization by multiplexing of workloads from various organizations. Cloud computing includes three models: (1) Software as a Service (SaaS): the applications (e.g. EHRs) are hosted by a cloud service provider and made available to customers over a network, typically the Internet. (2) Platform as a Service (PaaS): the development tools (such as OS system) are hosted in the cloud and accessed through a browser (e.g. Microsoft Azure). (3) Infrastructure as a Service (IaaS): the cloud user outsources the equipment used to support operations, including storage, hardware, servers and networking components. The cloud service provider owns the equipment and is responsible for housing, running and maintaining it [3]. In the clinical environment, healthcare providers are able to remotely access the corporate Intranet via a local Internet service provider, since they have the option to have an ISDN line installed to their home or hospital linking with cloud.

The majority of physicians in healthcare do not always have the information they require when they need to rapidly make patient-care decisions, and patients often have to carry a paper record of their health history information with them from visit to visit. To address the problems, IBM and Active Health Management collaborate to create a cloud computing technology-based Collaborative Care solution that gives physicians and patients access to the information they need to improve the overall quality of care, without the need to invest in new infrastructure [5]. IBM facilitated American Occupational Network and HyGen Pharmaceuticals to improve patient care by digitizing health records and streamlining their business operations using cloud-based software from IBM Med Trak systems, Inc. and The System House, Inc. Their technology handles various tasks as a cloud service through the internet instead of developing, purchasing and maintaining technology onsite [5]. Acumen solution's cloud computing CRM and project management system were selected by the U.S. Department of Health & Human Services' office of the National.

Coordinator for Health IT is to manage the selection and implementation of EHR systems across the country. The software will enable regional extension centers to manage interactions with medical providers related to the selection and implementation of an EHR system. Sharp Community Medical Group in San Diego will be using the collaborative. Care solution to change the way physicians and nurse's access information throughout the hospital group's multiple electronic medical record systems to apply advanced analytical and clinical decision support to help give doctors better insight and work more closely with patient care teams [6]. One of similar example of applying cloud service in the healthcare area is the architecture of the hospital file management system (HFMS). A HFMS cluster contains a master server and multiple blocks of servers by multiple client access.

3. PROPOSED METHOD

In the proposed method describes security challenges in healthcare information sharing, and different security concerns related to threats and vulnerabilities are analyzed and a method of alleviating these barriers. There are steps taken to reduce the risk that an EHR system will be hacked:

Keep the EHR on a segregated network, if possible. Shelter the EHR from the rest of the network infrastructure. Otherwise it's very easy for a provider's practice management system or mobile or medical device to pass on a virus or other infiltration to the EHR system.

Check for vulnerabilities. Run risk assessments and conduct audits. Correct weaknesses discovered.

Consider buying and running a data loss prevention software program, which runs on the perimeter server.

Apply security patches to internet applications that are connected to the EHR systems, such as internet explorer, java and adobe acrobat.

Make sure that the firewalls are installed properly, and that the antivirus programs are operational. Hackers are looking for easy access into computer networks. Don't make the EHR system that easy a target.

Comply with objective, specific measures, such as those recommended by the National Institute of Standards and Technology or HITRUST, so you can defend the adequacy of the safeguards you took to protect patient information.

Make sure that the EHR and health IT vendor contracts support off-the-shelf antivirus software.

Designate who within the organization is responsible for maintaining the integrity of the system.

Clearly delineate with the EHR/Health IT vendor who will be responsible for security patches. Don't assume that the vendor will do it; many vendors don't.

Make sure that any medical software you're working with runs without "super user" rights. This makes it harder for a hacker to gain access to the records.

3.1 Security Measures

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories-

Deterrent controls: These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

Preventive controls: Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Physical security: Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security: Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive

Privacy: Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

3.2 Attribute Based Encryption

In the CP-ABE, the encryptor controls access strategy, as the strategy gets more complex, the design of system public key becomes more complex, and the security of the system is proved to be more difficult. The main research work of CP-ABE is focused on the design of the access structure. In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the left to decrypt.

Algorithm

1. **Setup**

The setup algorithm chooses bilinear group triple (G1; G2; GT) of prime order p and a bilinear map e:

G1 _ G2! GT. The algorithm also picks generators g of G1 and h of G2. Then it chooses 3 random
Exponents e,i in Z^p. It then sets u = g_ and v = e (g; h).
After that it chooses a suitable encoding _ sending each of the m attributes at 2 P onto a (di_erent)
Element _ (at) = x 2 Z_p. It then chooses a set of m - 1 dummy attributes D = fd1; dm^1g. By the
Notation Di for i < m - 1, we will denote the set of the dummy attributes from d1 to di.

PK (public parameters): {f P; u; v; h; fh in igi=0; 2m-1; D; t}

MK (master secret key): f; g; h g

2. Key Generation

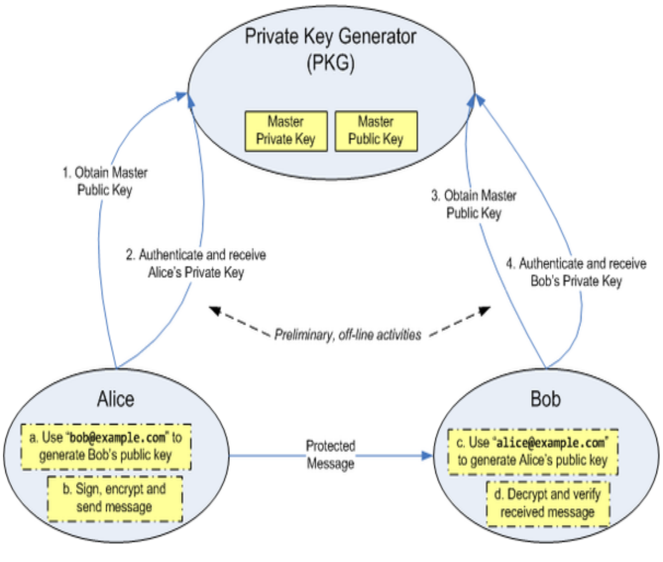
KeyGen (PK, A, MK)
Given a set of attributes a _ P, the central authority picks an r 2 Z_ p at random and computes the secret
Key for the user as follows:
SKA =nfg

3. Encryption

Enc (PK, T, M)

For every non-leaf node x of the access tree T, we choose a polynomial qx. We, proceed in a top down
Manner in selecting the polynomials, starting from the root R. For a node x we set the degree of the node
Dx = kx ^ 1, one less than the threshold value that needs to be satis_ed at the gate at that node.
Now, beginning at the root, we choose a random s 2R Z_ p and set qr (0) = s. Then choose dr other points of the polynomial qr to de_ne it completely. For all other non-leaf nodes x, we set
Qx (0) = qparent(x)^Index(x)
_
And choose dx other points to completely de_ne qx.
For the last level of non-leaf nodes, x 2 T, we compute the following two values:
Cx1 = u^ qx (0)
Cx2 = h ^ qx (0):_Qat2Sx (+_ (at)) Qd2Dm+kx^1^sx (+d)

The cipher text is given by:
CT = f ~ C = M _ e (g; h)_s ; C0 = h_s ; fCx1;Cx2g8x2 T



Attribute based CP-KBE encryption algorithm flow chart
Chart – 1: Flow chart for CP-KBE

3.2 Fully homomorphic Encryption

Fully homomorphic encryption allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption.

ALGORITHM

In the following examples, the notation $\mathcal{E}(x)$ is used to denote the encryption of the message *x*.
In the full homomorphic cryptosystem, in a cyclic group G of order q with generator g, if the public key is (G,q,g,h), where $h=g^x$, and x is the secret key, then the encryption of a message m is $\mathcal{E}(m)=(g^r,m\cdot h^r)$, for some random $r\in\{0,\ldots,q-1\}$. The homomorphic property is then

$$\mathcal{E}(m_1)\cdot\mathcal{E}(m_2)=(g^{r_1},m_1\cdot h^{r_1})(g^{r_2},m_2\cdot h^{r_2})$$

$$=(g^{r_1+r_2},(m_1\cdot m_2)h^{r_1+r_2})=\mathcal{E}(m_1\cdot m_2).$$

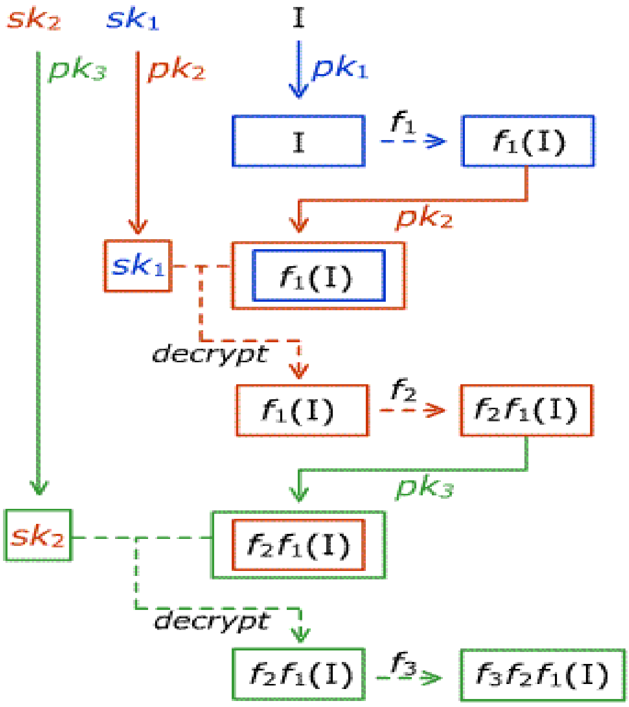


Chart – 2 : Diagrammatic representation of FULL Homomorphic Encryption

DATA SET for FULL HOMOMORPHIC ENCRYPTION

X AXIS (modules)	0	10	20	30	40	50	60	70	80	90	100
Y AXIS (time)	10^(-4)	10^(-4)	10^(-3)	10^(-3)	10^(-3)	10^(-3)	10^(-3)	10^(-3)	10^(-3)	10^(-2)	10^(-2)

DATA SET for ABE

X AXIS (modules)	0	10	20	30	40	50	60	70	80	90	100
Y AXIS (time)	1	1	10	10	10	10	100	100	1000	1000	10000

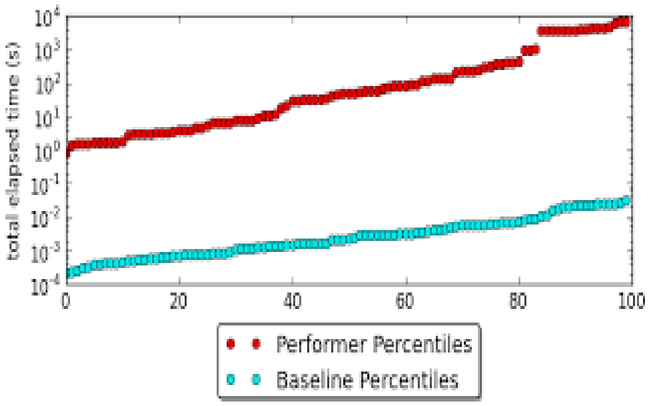


Chart – 3: Comparison of ABE and Homomorphic.

The chart3 is based on **time.** Here the dark line refers to **ABE** method and light line belongs to **FULL Homomorphic** method. So Homomorphic method is good.

4. CONCLUSIONS

Little literature in the health information science research addresses the critical challenges and solutions of applying Cloud Computing. While the use of Cloud Computing continues to increase, legal concerns are also increasing. Although Cloud Computing providers may run afoul of the obstacles, the long run providers will successfully navigate these challenges. By using Cloud Computing security framework, the collaborative parties can answer questions related to governance and best practice and determine whether the organization is capable of IT governance in the Cloud Computing applications. Also it is observed that ABE method of encryption is better than Full Homomorphic method. The reason being in ABE we can define our own encryption algorithm and hence it is more secure.

REFERENCES

[1] ANSI, ISO/TS 18308 Health Informatics-Requirements for an Electronic Health Record Architecture, ISO 2003.

[2] Mell, P., Grance, T. “The NIST definition of cloud computing.” Communication of the ACM, 53 (6),50,2010.

[3] Armbrust, M., et al. “A view of cloud computing.” Communication of the ACM, 53 (4), page 50-58, 2010.

[4] Guo L, Chen F, Chen L, Tang X. The building of cloud computing environment for e-health. In: Proceedings of the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT). New York, NY: IEEE; 2010 Presented at: The IEEE International Conference on E-Health Networking; July 1-3, 2010; Lyon, France.

[5] IBM and ActiveHealth Management. ActiveHealth and IBM Pioneer Cloud Computing Approach to Help Doctors Deliver High Quality, Cost Effective Patient Care. http://www-03.ibm.com/press/us/en/pressrelease/32267.wss. Accessed on September 1st, 2011.

[6] Acmen Solution. Acumen nabs ONC cloud computing contract.URL:http://www.cmio.net/index.php ?option=com_articles&view=article&i d=20648: acumen-nabs-onc-cloud-computing-contract&division=cmio. Accessed on June 27, 2012,

[7] Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, et al. EECS Department, UC Berkeley. 2009. above the Clouds: A Berkeley View of Cloud Computing. Technical Report. URL: http:// www.eecs.berkeley.edu /Pubs/TechRpts/2009/EECS-2009-28.pdf accessed on June 28, 2012,

[8] Pearson S. Taking account of privacy when designing cloud computing services. In: Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09). New York, NY: IEEE; 2009 Presented at: the IEEE First international workshop on software engineering challenges for Cloud Computing (ICSE); May 16-24, 2009; Vancouver, BC, Canada.

[9] CSA. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance. 2009.

[10] A. Harrington, C. Jensen. Crytographic Access Control in a Distributed File System. Proceeding of the eight ACM symposium on Access control models and tecnologies, 2003, 158-165.

[11] BSI BS ISO/IEC 27001: 2005/BS 7799-2:2005: Information Technology-Security Techniques-Information Security Management Systems-Requirements. British Standards Institution. (2005 a).

[12] M. H. Kuo, Opportunities and Challenges of Cloud Computing to Improve Health Care Services, J Med Internet Res 2011;13(3):e67.

[13] http://www.hhs.gov/ocr/privacy/hipaa/administrative /breachnotificatio nrule/breachtool.html accessed on August 14, 2012.

BIOGRAPHIE

Dr.K.Govinda received the degree in computer science and engineering from NAGARJUNA University in 1998. he is Associate Professor in School of Computing Science and Engineering, VIT University. His interests are database, data warehousing and cloud computing