ENHANCING SECURITY FEATURES IN CLOUD COMPUTING FOR HEALTHCARE USING CIPHER AND INTER CLOUD

Aruna Devi. S[1], Manju.A[2]

[1, 2]Assistant Professor, Department of Computer Science and Engineering, Saveetha Engineering College, Tamilnadu, India

Abstract

Health Care is the most important unindustrialized field. Cloud is an emerging trend in software industry. In medical field, there are large dataset comprising highly sensitive data about patient's medical records. Based on these records, diagnosis for the patient will be given. Moving data to the cloud makes to explore a large information for diagnosis as expert documentation will also be stored as part of health record. Physicians from anywhere at any time can get access over these reports for better treatment. The Medicare industry vacillates to store these data to the cloud as the patients might feel insecure about their health records. This work introduces the idea of combining Cipher Cloud, Inter Cloud and ABE schemes, proposes an innovative method to enhance security features in the cloud by double encryption using algorithms and tools. By this, only authorized entities are proficient of accessing these records. Rather than storing data in single cloud, Inter Cloud (Multi-cloud) also adds advantage for our proposed work.

Keywords: *Virtualization, Cipher cloud, Trust, Encryption, Inter cloud*

---***---

1. INTRODUCTION

Cloud computing is an emerging trend in software field as it focuses on shared resources. Application areas of cloud computing are not only limited to IT field but also extended for e-Government, Healthcare, e-Business, Libraries etc., Cloud computing purely relies on virtualization, which increases the infrastructure deployment in reduced cost and IT operations are scampered up. On-demand access attracts more number of users towards cloud. Cloud imposes pay-per-use model. Users tend to pay only for actually consumed resources. The resources stored in cloud can be accessed anywhere anytime. Fig.1 visualizes cloud deployment models and its services such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud can be called as EaaS (Everything as a Service). Fig. 2 gives the different types of cloud viz. Public cloud, Private cloud, Community cloud, Hybrid cloud. Yet, in the beginning people falter to use cloud because of the security and privacy concerns while storing the highly confidential and sensitive data into the cloud. Moving to cloud in Health Care is the major challenge rather than other fields because of the above stated reason. So, we are proposing architecture to overcome the pitfalls in the cloud by moving to cipher cloud.

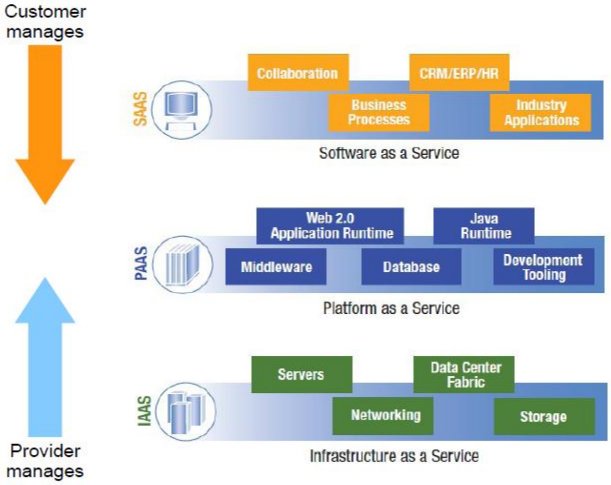


Fig. 1 Cloud Deployment Model

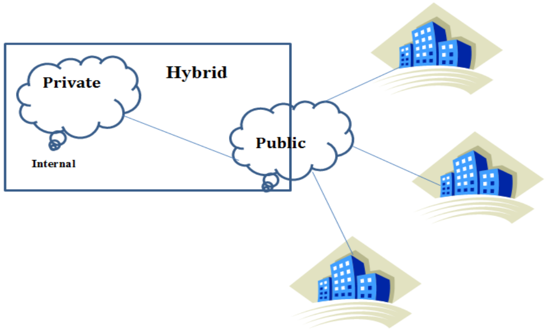


Fig. 2 Types of Cloud

In this paper we combine the topics of cloud computing and trust in the cloud which can be called as cipher cloud. We discuss how security can be imposed in a cloud so that highly sensitive data in all fields can be stored in a cloud without any hesitation. This offers cloud service providers the possibility to penetrate market areas where higher security requirements need to be met. For achieving this, we extended the inter cloud and cipher cloud models.

The paper is structured as follows. First, we briefly introduce basics of cloud computing with its deployment models and services rendered by it. Section 2 deals with the related work from the literature. A motivation behind cloud computing in Healthcare is also provided. In Section 3, we discuss about the proposed work in which cipher cloud architecture is combined with inter cloud models to enhance data security and reliability. Section 4 presents the methodology to achieve the above. Section 5 draws some concluding remarks and some ideas for future work.

2. RELATED WORK

In [3], the authors describe various applications of cloud computing over Healthcare, its implications. Patients and health organizations take advantages of the new technology by improving patients quality of service through a distributed high-integrated platform (Wang, 2010), coordinating of medical process as well as reducing IT infrastructure investment or maintenance costs which leads to a better healthcare environment. Concentrating on the Global Market for Cloud Computing in Healthcare, IT industries invest heavily to build infrastructure for cloud to support it and help organizations take benefit from it. The rate of increase in adopting cloud is directly proportional to the rate of achieving greater efficiencies. This results in providing extraordinary sharing capabilities between the healthcare organizations and patients alike.

The Challenges of Cloud Computing in Health Care is mostly due to two important concerns associated with security and interoperability (Sanjay P. Ahuja 2012).

By taking advantage of solutions available, the above mentioned issues can be overcome. This leads to movement towards cloud and taking advantage of the solutions it provide. Since Healthcare data is highly confidential, its privacy and security concerns need to be tackled. Security concerns can be addressed by following Health Insurance Portability and Accountability Act (HIPAA) when moving health record to the cloud. The healthcare data comprises of sensitive information yet migration of the medical records to the cloud (third party) may be trusted. To prevent uncovering of information to unauthorized persons, security activities such as imposing access controls, providing authentication, checking authorization can be done. These issues are an obstacle that have slowed the cloud implementation and should be addressed in order to enable the trustworthiness of cloud systems.

Interoperability is also another concern to be dealt with when moving data to outside provider. This arises because of diverse data modeling constructs adopted in different Medicare organizations which leads to different database designs, implementation, management, platforms, programming languages and incompatible systems. The Healthcare systems interoperability may occur either at the provider, or software, or computer, or data levels and /or system integration.

Ming Li(2013), describes a novel patient centric framework and mechanisms for data access control to PHRs stored in semi-trusted servers. Attribute-Based Encryption (ABE) technique was used to encrypt each patient’s PHR file. It exploits multi-authority ABE for the privacy of patient’s by dynamic modification of access policies. Revoking of access policy is not possible at all the moments and the attributes which were known to the user leads to privacy concern.

In Attribute-based encryption [2], the owner of data has to predefine the attributes based on which the encryption needs to be done. The number of users in the system doesn’t matters. Each attribute has public key, secret key, and a random polynomial, so different users cannot combine their attributes to recover the data, and different users cannot carry out collusion attacks. Only the user who possesses the authorized attributes can satisfy the access policy to decrypt data. The access policy contains a boolean formula such as AND, OR et al. which can let the access structure be flexible to control users' access.

Almost all key generation schemes used by authority are prevailing. Since these schemes contain the authority that just suits the private cloud environments, the authority should be removed in the future.

3. PROPOSED WORK

Data encryption should be adopted to enforce privacy policies in the cloud since the cloud server is no longer assumed to be fully trusted. In ABE scheme, as the number of users’ increases, their attributes for generating cryptographic keys also increases and this leads to complexity in key management.

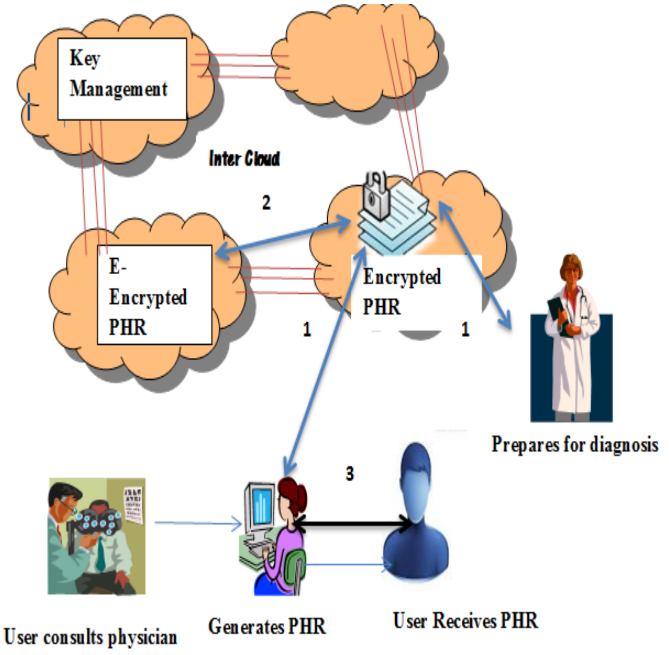
In the proposed work, for ensuring security, encryption tools are used along with attributes of user. Usage of tools overcomes the complexity in key management in ABE schemes. So we are proposing architecture by combining the concepts of cipher cloud and ABE in which the PHR encrypted by encryption tool is again encrypted by using attribute based encryption (ABE).

3.1 Methodology

Our methodology implements security in two stages. In stage 1, the PHR is encrypted by tools such as TrueCrypt 7.0 / Boxcryptor 1.0 and stored into cloud. In stage 2, the encrypted PHR is encrypted by the cloud service provider using attributes of user.

The architecture of our proposed work is given in Fig.3. The user consults doctor and the doctor generates Personal Health Record which comprises the patient's history of health issues, symptoms, diagnosis undergone. This PHR is encrypted by encryption tools such as TrueCrypt / Boxcryptor and stored into cloud. Again this encrypted PHR is encrypted using the attributes of user. In order to manage the keys generated, inter cloud is taken into account to minimize the complexity.

When the patient is under treatment, his/her PHR is retrieved from cloud by decrypting it with key and tools. This can be used for further references and helps in diagnosis.



1→ Encryption / Decryption by Encryption tool
2→Encryption using attributes of user
3→Key Sharing

Fig.3 Architecture of Proposed System

TrueCrypt 7.0 is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). Without user intercession, the data is automatically encrypted or decrypted right before it is loaded or saved. Only by using the correct keyfile / password or encryption key, the stored encrypted data can be decrypted (read).Not only the data in file gets encrypted but also the meta data, file name, folder name and everything related to the file will be encrypted. In addition to resilient and translucent encryption, TrueCrypt also creates more secure (and obscured) file protection by creating hidden volumes within encrypted volumes. Since online backup is increasingly popular, Boxcryptor 1.0 tool allows the user to create an encrypted folder of the user's PHR and synchronizing that folder with cloud provider. This improves privacy as even a third-party gets the PHR, the encrypted folder can be decrypted only by the user and their relatives.

The cloud service provider needs to manage this software as a service. Once the encrypted PHR stored into cloud, the CSP encrypts their record by using user's attributes which results in more secured data storage in the cloud. Whenever the PHR is needed by the physician for diagnosis, he/she will decrypt the record using the attributes of concerned patient and then it is decrypted automatically by TrueCrypt/ Boxcryptor software by using correct password. This system is more secure as encryption and decryption are done twice by software and attributes.

Complexity in key management can be reduced by having managing resources in another cloud so that key management and secured storage will be carried over in separate clouds. This needs inter cloud implementation.

4. CONCLUSIONS

In this paper, we have proposed a novel framework to realize patient-centric privacy for personal health records in cloud computing. Patients themselves encrypt the data using encryption tools and their attributes are used for double encryption by CSP. The framework addresses the challenges brought by multiple PHR owners and users, by reducing the complexity of key management when the number of owners and users in the system is large. We utilize encryption tools and multi-authority attribute-based encryption to encrypt the PHR data.

The work can be extended by enhancing the features of inter cloud while storing the data.

REFERENCES

[1]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" , IEEE Transactions on Parallel and Distributed Systems, (Vol. 24 No. 1) pp. 131-143, Jan. 2013.
[2]. Cheng Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.
[3]. Sanjay P. Ahuja, Sindhu Mani & Jesus Zambrano, "A Survey of the State of Cloud Computing in Healthcare",

Network and Communication Technologies; Vol. 1, No. 2; 2012.

[4]. Rolim, C.O, Koch, F.L. ; Westphall, C.B. ; Werner, J. ; Fracalossi, A. ; Salvador, G.S, ”A Cloud Computing Solution for Patient’s Data Collection in Health Care Institutions”, Second International Conference on eHealth, Telemedicine, and Social Medicine, pp. 95 - 99 , 2010.

[5]. Ming Li, Shucheng Yu, Kui Ren, Wenjing Lou, “Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings”, Social Informatics and Telecommunications Engineering, Volume 50, pp 89-106, 2010.

[6]. Wang, X. (2010). Application of Cloud Computing in the Health Information System. Computer Application and System Modeling(ICCASM).Retrievedfromhttp://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5619051

[7]. M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing," Communications of the ACM,vol. 53, pp. 50,58, 2010.

[8]. J. Bethencourt, A. Sahai, and B. Waters, ”Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security andPrivacy, pp. 321V334, 2007.

[9]. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349

[10]. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010

[11]. S. Subashini, and V. Kavitha. (2010) “A survey on security issues in service delivery models of cloud computing.” Journal of Network and Computer Applications, Volume 34, Issue 1, pp. No. 1-11, Jan 2011.

[12]. S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[13]. M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.

[14]. http://www.zurich.ibm.com

BIOGRAPHIES

Aruna Devi. S, working as Assistant Professor in Saveetha Engineering College, Areas of interest includes Data Mining, Compiler Design, Cloud Computing and Big Data Analytics

Manju A, working as Assistant Professor in Saveetha Engineering College, Areas of interest includes Networks, Network Security, Cloud Computing.