Secure Health Care Based Encryption Schemes On Cloud Computing Storage

[1]Ruchika Bhandarkar, [2]Manasi Yadav, [3]Iffat Pagarkar, [4]Prof. Amol Karande

Information Technology Department
Pillai HOC College of engineering
Raigad, Maharashtra, India

Abstract: **Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. This leads to address the privacy issues i.e., hide the sensitive health information of a patient, as the information can be accessible to unauthorized parties because of the nature of the storage. This paper describes novel patient-centric secure data sharing framework for cloud-based PHR systems. The paper is to create Health Care Information (HCIs) that are efficient and secure. HCIs can be stored in a third party cloud. The patients, who have created their profiles in the system, make their own HCIs, mentioning their disease, symptoms and other sufficient details. The doctors who are also a part of the system attend to the queries of the patients that have been updated in the cloud. The doctors' prescription is updated by the admin of the system, whereas the cloud admin has no access to the data. The level of encryption is considered before generating the encryption key. The record is then accessed using the key that the admin has generated. The health care services can look up to the user details. The details of the secured information remains encrypted, whereas the other details remain as updated.**

***Keywords*: Health Care System, PHR, HCI, CP- ABE, Cloud Computing, PHA**

INTRODUCTION

Health Care Information (HCIs) is a health information exchange that is related and managed by the patients, themselves. HCIs is often out sourced to be stored at a third party like cloud providers. This involves privacy issues since the sensitive health information can become accessible to the cloud providers and at times, to unauthorized parties. This makes encryption mandate. The data should be encrypted by a trusted method that performs encryption before the data is outsourced and stored in the cloud. Encrypting data would raise issues such as risks like sensitive data being exposed, a large number of keys to be generated, differences in security level provided by the system and expected by the user and inability to access during emergency. In this paper, we proposed a novel method to encrypt the data at different security levels, as the patient desires. Efficiency is achieved by dividing the users into two different domains. The domain containing doctors whom the patients send their queries to, can access the patient details. Whereas, the health care departments like insurance providers can access only the details that are insecure. Key revocation is used invalidate the existing key and generate a new one. This can be of great help in emergency scenarios when there is a demand for a new key.

II. RELATED WORK

Cloud computing became highly accepted and advantageous over the years since it serves the consumers with the computer infrastructure. This has made the computing paradigm has become the key in various industries. However, this boon of technology comes along with a list of issues to be addressed, the most important of which is security. Sensitive information can draw many intruders to extract information from the cloud. Cryptographic methods are used to maintain the security of data. This in turn produces a heavy computation overhead. We can achieve high security by using the combination of Attribute based Encryption (ABE), Proxy Re-encryption and Lazy Re-Encryption [8]. Health Care Systems require high cost of storing and maintaining health records. Hence managing the data about health information is highly essential. The system should be able to provide information to reliable consumers, when necessary. Hence, a system should be built, that is able to collect, maintain and manage all the records related to health information [1]. Mobile devices have been used to access patient information over the years. However, there is no standard for security. Hence, mobile devices were used after specific authentication [2]. The use of cloud computing technology in managing health records has given opportunities to the users and other personnel like heath care providers and insurance providers to manage health care information. However, the security of the information is questioned. The issues associated with the cloud-stored information have been analyzed and solutions have been identified. Architecture that provides a consumer controlled approach has been proposed to improve security

I. Existing System

Existing system focuses on health information exchange but suffers from many security issues.

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers.

The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust.

II. Proposed system

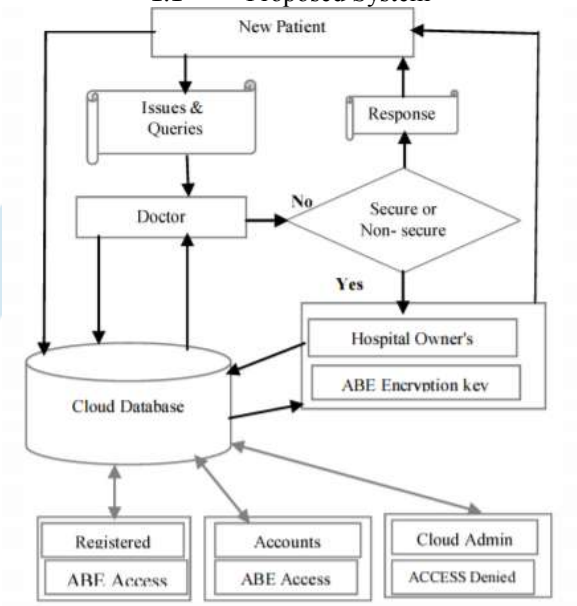
∗ This paper proposes a framework for secure health care system on cloud storage. The proposed system Ciphertext-Policy Attribute Based Encryption with Delegated Equality

∗ Test. Ciphertext-Policy Weighted Attribute Based Encryption for Fine-Grained Access

∗ Control. Conditional CPABE Encryption Scheme in Vehicular Cloud. An Efficient Key-

∗ Policy Fixed Cipher-text Size to construct a KP-ABE scheme that will have Ciphertext size as well as a constant private key size. ABE for Securing PHR on Cloud and Secure of PHR shared in cloud using CP ABE

1.1 Proposed System



IV. Conclusion

Our system has a patient centric model for secure sharing of personal health records in cloud computing.
In this framework we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works.
This model also proves its security. Through implementation and simulation, we show that our solution scalable and efficient.
It has been an immense pleasure on working on this project which comes under Cloud Computing, which is the need of the hour in this technology driven world.

VI. Acknowledgement

We remain immensely obliged to Mr. Amol Karande for providing us with the moral and technical support and guiding us. We would also like to thank our guide for providing us with her expert opinion and valuable suggestions at every stage of project. We would like to take this opportunity to thank Dr. J.E Nalawade, Head of Information Technology Department for her motivation and valuable support. This acknowledgement is incomplete without thanking teaching and non-teaching staff of department of their kind support. We would also like to thank Dr.Mathew T.J, Principal of Pillai HOC College of engineering, Rasayani for providing the infrastructure and resources required for project.

References

[1] Yang Ming, Liu Fan and Han Jing-Li 2011 An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control , IEEE International Conference on Computer Comunication and Control 978-0-7695-4519-6/11 516- 520.
[2] Kan Yang and Xiaohua Jia 2012 Attribute-based Access Control for Multi-Authority System in Colud Storage, 32nd IEEE International Conference 536-545.
[3] Xun Yi, Yuan Miao, Elisa Bertino and Jan Willemson 2013 Multiparty Privacy Protection for Electronic Health Records IEEE. 978-1-4799-1353-4/13 2730-2735.
[4] Vijaya Lekshmi and Revathi 2014 Implementing Secure Data Access Control For Multi Authority cloud storage system using ciphertext policy-Attribute based Encryption, o.978-1- 4799-3834-6/14/ IEEE, ICICE
[5] Yun Wang, Dalei Zhang and Hong Zong 2014 Multi-authority Weighted Attribute Encryption Scheme in cloud Computing, IEEE International Conference on Natural Computation. 978-1- 4799-5151-2/14 1033-1038