International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 7: July 2015, pp 25-27. www.aetsjournal.com ISSN (Online) : 2394-6237

Dynamic and Efficient Data Sharing in Cloud Storage Using Key Aggregate Cryptosystem

N.Dhivya Bharathi , J.Kavitha

Abstract— The growing need for the remote caring of patients at home combined with the ever-increasing popularity of mobile devices due to their ubiquitous nature has resulted in many apps being developed to enable mobile telecare. The Cloud, in combination with mobile technologies has enabled doctors to conveniently monitor and assess a patient's health while the patient is at the comfort of their own home. This demands sharing of health information between healthcare teams such as doctors and nurses in order to provide better and safer care of patients. However, the sharing of health information introduces privacy and security issues which may conflict with HIPAA standards. In this paper, we attempt to address the issues of privacy and security in the domain of mobile telecare and Cloud computing. We first demonstrate a telecare application that will allow doctors to remotely monitor patients via the Cloud. We then use this system as a basis to showcase our model that will allow patients to share their health information with other doctors, nurses or medical professional in a secure and confidential manner. The key features of our model include the ability to handle large data sizes and efficient user revocation.

Keywords: Cloud computing, HIPAA, health information, large data sizes.

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a comprehensive solution that delivers IT as a service.

The flexibility of cloud computing is a function of the allocation of resources on demand. Before cloud computing, websites and server-based applications were executed on a specific system. Cloud computing is broken down into three segments application, storage and connectivity. The mobile health applications, to enable secure sharing of telecare data in the Cloud. The Cloud, as an enabler for mobile telecare, can help provide effective treatment and care of patients due to its benefits such as on-demand access anywhere anytime, low costs and high elasticity. However, the Cloud is susceptible to privacy and security attacks, many of which occur from within the Cloud providers themselves as they have direct access to stored data. There is considerable work on protecting data from privacy and security attacks. NIST has developed guidelines to help consumers protect their data in the Cloud. Encrypting data before storing to the Cloud is an effective way to prevent unauthorised users from accessing sensitive data.

However, plain encryption techniques are not enough especially when considering the scenario of sharing data among a large group of users. A trivial solution of data sharing is handling out encryption keys to all members of the group. In that way, only the members of the group will have data access. However, when considering the problem of user revocation, the data owner must re-encrypt the data again with a new key and distribute the new key to all remaining users. This is computationally inefficient and places a burden on the data owner when considering very large data sizes as well as large group sizes where users continually join and leave. Our main contribution in this paper is to demonstrate our security protocol that will allow private and secure sharing of data in the Cloud within the context of mobile health applications.

Moreover, we attempt to address the problems of achieving efficient user revocation, especially when considering large data sizes. First, we define a secure data sharing model and protocol.

II. RELATED WORK

In this section, we review related work on data sharing in the Cloud and focus on the literature used to handle the user revocation problem. We also briefly review previous related works on the integration of mobile technology and the Cloud for health monitoring.

2.1. Data sharing in the Cloud

Data sharing in the Cloud is fast becoming vital for organisations and social users alike. In a survey by Information Week, nearly all organisations shared their data in one way or another with 74% sharing data with customers and 64% sharing data with suppliers. The benefits include higher productivity and better time management for example by using collaborative tools such as Google Docs ith social users, the benefits of data sharing are clear, for example

N.Dhivya Bharathi , PG Student, Dept of Computer Science & Engineering, Shanmuganathan Engineering College, Pudukkottai. (Email: dbrathi15@gmail.com)

J.Kavitha, Asst.Professor, Dept of Computer Science & Engineering, Shanmuganathan Engineering College, Pudukkottai(email: kavisaras@gmail.com)

with Facebook where the ability to share photos and videos as well as share day-to-day information creates a sense of enjoyment in one's life and can also enrich some people as they are amazed at how many people are interested in the events in their lives. Healthcare providers are now rapidly turning to the Cloud and the benefits of sharing are also clear. Healthcare providers are willing to store and share electronic medical records via the Cloud and hence remove the geographical dependence between healthcare provider and patient. Sarathy R. and Muralidhar K.Review the impact of the Internet on data sharing across many different organisations such as government agencies and businesses. Butler describes the issues of data sharing on the internet where sharing information can allow users to infer details about users. Feldman and Patel et al. discuss the important benefit of data sharing in terms of public health, in particular for education and professional development. Tran et al. utilise the idea of a proxy re-encryption scheme where the data owner's private key is divided into two parts where one is stored in the data owner's machine and the other on the proxy. The same occurs for all members of the group. The data owner encrypts data using his key piece while the proxy encrypts the entire data using the remaining key piece. An authorised member of the group can then retrieve data as the proxy will transform the ciphertext held by the data owner to another ciphertext which can be decrypted by the authorised member's key. The data will first be decrypted using the member's key piece in the proxy and then fully decrypted when the member decrypts it using the remaining key piece held by the authorised member. User revocation will simply involve removing the revoked user's key piece in the proxy and hence is efficient. However the problem with this technique is that it does not handle the case where a revoked user and the proxy collude, which can then reveal all other user's private keys in the group. Also another major problem with this is that since it uses ElGamal public key cryptography, it will not allow the encryption or decryption of very large data, which is consequently a feature of medical data. We will extend upon this in our secure data sharing framework to handle the collusion and data size problem. Nguyen Thanh Hung et al. better handled the case of a revoked user colluding with a proxy by introducing a number of proxies. The more proxies there were, the less likely the revoked user would be able to collude with all proxies to reveal all the keys. When a user is revoked access rights, the key manager simply instructs all proxies to remove the key pair corresponding to the revoked user. We take advantage of this in our data sharing model in order to enhance security

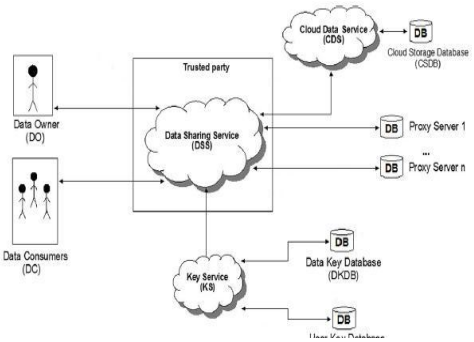
2.2 Attribute-Based Encryption

Attribute-Based Encryption (ABE), originally proposed by Sahai and Waters et al. is a technique used to enable fine-grained access control of data. Access Control Lists(ACLs) were initially used but were phased out as it provided only coarse-grained access to data and hence was not scalable, a primary feature of the Cloud. There are two types of ABE Key-Policy ABE (KPABE) where the access control policy is stored with user's private key while a number of attributes are stored with the ciphertext. A user can decrypt data if, and only if, the attributes satisfy the access control policy. Ciphertext-Policy ABE(CP-ABE) is essentially the opposite of KP- ABE, where a number of attributes are stored with theuser's private key and the access control policy is stored with the ciphertext. Tu and Niu make use of CP-ABE in the context of enterprise applications and developed a revocation mechanism that simultaneously allows high adaptability, fine-grained access control and revocation. When a user is revoked access rights, the data is reencrypted in the Cloud rendering the revoked user's key useless. Even though, the re-encryption process is delegated to the Cloud, this is not efficient when considering very large data sizes.

Li and Niu et al. also leverage ABE in the context of the sharing of personalhealth records (PHR) in the Cloud and is based on role-based fine- grained access control policies. Yang et al. proposed a combination of proxy re-encryption and attribute- based encryption to enable secure data sharing in the Cloud. It involved storing two keys; the ABE key and proxy re-encryption key as well as the encrypted data to the Cloud and uses an authorisation list. Data access involves using both keys to decrypt the data. The ABE key determines the user's access rights and the proxy key generates the cipher that can be transformed to enable decryption by the user's private key. User revocation simply involves removing the user from the authorisation list and hence is computationally efficient. However, the scheme does not handle the scenario where a revoked user rejoins the group with different access privileges. Nguyen et al. used the concept of bilinear maps to create a secure data sharing model in relation to tables. It involves splittinga key and giving a portion of the key to authorised users while the others are sent to the proxy. The user can then decrypt data with the help of all the proxies. Our method is different in that it is not limited to only table data and can handle large data sizes. In our work, we attempt to address some of the shortcomings described to provide a better method of data sharing in the Cloud. We extend upon the work of Tran et al. by attempting to solve the collusion problem and take advantage of the work by Nguyen Thanh Hung et al. in terms of increasing the number of proxies, to provide a more secure and confidential method of data sharing in the Cloud.

III. SYSTEM DESIGN & SYSTEM ARCHITECTURE

The Device table contains information about a healthmonitoring device connected to this system, such as the name and type of the device and its unique MAC address. It contains information such as the doctor that is authorised to view the data associated with the service, the device used, the patient it is monitoring, and the start and end times of the service. Since the focus of this paper will be on enabling



secure data sharing in the Cloud, the data model for the database stored in the CSP will be described illustrates our data model for the health-monitoring system. Note that the data model is generic medical data service for the proof of concept and is not focused on one particular medical service such as heart intensive care service.The User table contains all the users of our system, including patients and doctors. The email and password are used for authentication and the role determines whether the user is a doctor or a patient.

TECHNIQUES

ElGamal encryption, invented by T. ElGamal is a public-key cryptography system. We take advantage of ElGamal Encryption in our work since it does not rely on a user's public key infrastructure (PKI) and the algorithm is both simple and efficient. There are three main steps of the ElGamal encryption algorithm:

• Initialisation: Given a prime p, a primitive root c of p, compute

b = cx mod p. Also randomly select a secret key x. The public

key is thus {p, b, c} and private key is x.

• Encryption: Generate random value r and encrypt data m as

follows:

E(m) = m ・br mod p

= m ・crx mod p. (1) Also note: g = cr mod p.

• Decryption: This decrypts m with secret key x as follows:

Dx(E(m)) = g-x ・E(m) mod p

= (cr)-x ・m ・crx mod p

= c-rx ・m ・crx mod p

= m mod p. (2)

Proxy Re-Encryption is based on the concept of a semitrustedproxy that uses a re-encryption key to translate a cipher-text under the data owner's public key into another ciphertext that can be decrypted by another user's private key. The data is never decrypted before it is re-encrypted hence the proxy will never be able to reveal the plaintext at any time. Many recent works have realised proxy re-encryption as a technique to enable data sharingin the Cloud. In our work, although we do not use proxy reencryption explicitly, our system mimics a proxy re-encryption algorithm scheme from the point of view of the data owner and consumer.

IV. CONCLUSION AND FUTURE WORK

Data sharing application in the Cloud is an exciting area and is fast becoming feasible in the near future. As more and more applications enter the health domain, there is now increasing demand to use the Cloud for health-related purposes such as for the sharing of health information. This places strong demands for data privacy and security in the Cloud. In this paper, we have developed a secure data sharing model and protocol that will allow private and secure sharing of data in the Cloud. Our secure data sharing protocol addresses the user revocation problem and the handling of large data sizes. The feasibility of the protocol has been demonstrated through our developed prototype that allows remote health-monitoring via the Cloud. We then carried out an analysis on the security aspects of our protocol. We also carried out performance tests on our developed prototype to test for feasibility. The overhead introduced by our security protocol in our prototype was a little longer in uploading due to the cryptography algorithms and key management operations, however we found this to be efficient as upload times were mainly insignificant to the user. Download times were comparatively low and hence makes our solution particularly attractive to use and share data.

Currently, in our secure data sharing model and protocol, we assume the DSS to be a fully trusted party. As part of our future work, we aim to remove this assumption and treat the DSS as an untrusted party. We also plan to continue to improve our developed app. I will improve my Ciphertext Classes and extract random class to encrypt the large size of data to share keys to data accessing user.

REFERENCES

[1] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M.Yiu, "SPICE – Simple Privacy-Preserving Identity- Management for Cloud Environment,"Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

[2] R. Canetti and S. Hohenberger, "Chosen- Ciphertext Secure Proxy Re-Encryption," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 185-194, 2007.

[3] C.-K. Chu and W.-G.Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," Proc. Information Security Conf. (ISC '07), vol. 4779, pp. 189-202, 2007.

[4] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009,

[5] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213- 229, 2001.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[7] G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322, 1989.

[8] T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption," Proc. 10th Int'l Conf. Cryptology and Network Security (CANS '11), pp. 138-159, 2011.

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.