

DATA SHARING STRATEGY IN CLOUD COMPUTING USING ATTRIBUTE BASED ENCRYPTION

¹Deepanshu Mohan, ²Sayyed Wahid Rabbani, ³R. Mangalagowri

³Assistant Professor

^{1,2,3}Department of Computer Science and Engineering SRM University, Chennai

¹deepanshu_mohan@srmuniv.edu.in, ²wahid_rabbani@srmuniv.edu.in

³mangalagowri.r@ktr.srmuniv.ac.in

Abstract: In today's world, storing and sharing information on internet is becoming common on trusted third party servers known as Cloud Servers. Users retrieving and sharing their secret data possess a certain risk of getting their information leaked by some third-party authority. In order to maintain the data integrity and confidentiality, many cryptographic algorithms are implemented to solve the issue. In Health Care System, patients and doctors share their major details to the hospital management by storing it online on the Cloud (internet). Important health details such as Blood Group, disease, etc. can be accessed by illegal users. Key Escrow is one of the major risks in data sharing over the cloud servers as the third-party key authority can also misuse their data. In our paper, we introduce an enhanced two-party key distributing system so that either of admin and cloud authority could access the data of the client. Both costs and encryption quality for a ciphertext are minimized. With the implementation of Attribute-based encryption in cloud computing, we are able to achieve secure and improved data sharing in Health Care System.

Keywords: Key Escrow problem, Data Sharing, Cloud Computing, Health Care System, Cipher Text-Attribute based Encryption, Data Confidentiality.

1. Introduction

Cloud Computing is an information model that allows universal access of computing services such as servers, databases, networking, referred as "Cloud". It is a type of computing that relies upon sharing of computing data over a large network instead of having a local server to handle the services. In order to access cloud application, the user must have the web supported device. Cloud computing applications are platform independent and can be accessible anytime and anyplace.

In Health care system, there is a need for an application which minimizes time and efforts as well as

expensive operations to generate full medical record of patient and combine the cluster of health details to deliver it to the healthcare professionals (eg: Doctor, Surgeons). Online health records have been widely used by big organizations such as hospitals, help the patients to generate, access, control and update health-related data. Patient health care are improved by using cloud computing as it provides secure, fast and better services which reduces the cost and time.

Though cloud computing provides us with many advantage, it own a major risk of data security. The major risk in cloud computing is presuming security to the online data shared online from unsanctioned access. The security issues are faced by both data owners and cloud service providers. In order to solve this security issue, many Encryption techniques have been performed. All the algorithms, which are proposed, provide better security to the information. Hence, providing a secure information is one of the hardest problems in cloud computing. Our work in this field is based on the use of Attribute-based Encryption.

Attribute-based encryption is a encryption in which the ciphertext and user's unique key are based upon the attributes (e.g.: Contact number, blood group) of the user. The decryption of a encrypted data is possible only if the attributes of the user matches the attributes of the encrypted information.

Attribute-Based Encryption is an important technique that provides cryptographic-based fine-grained information access control for harmful storage. Attribute-based encryption can be classified into two types – Ciphertext-Policy Attribute-based Encryption and Key Policy Attribute-based Encryption. CP-ABE has proved as an important encrypting process for secure data sharing. Using this encryption method, we need not data server to check data from unauthorized user access.

All the patient's data need to be decrypted by the admin or the key provided by a completely trusted Cloud authority (CA).

Key escrow problem can occur due to this. By getting unique key of Admin, Doctor can decipher all the user's encrypted text and can misuse it.

The scheme of this system will occur in the following steps –

1. System Setup
2. Key Generation
3. Information Encryption
4. Information Re-encryption
5. Update Key
6. Information Decryption

The data storing as well as the key generation system are accountable for the issuing of the Admin key. After the Doctor contacts the two parties, the key generation system helps in doctor and user verify and issuing of attribute keys to the user if he/she is entitled to the attributes. Accordingly, security and efficiency of the patient's information is one of the hardest problem faced in cloud computing [1], [11],

2. Proposed Method

In order to solve the Key Escrow problem, we propose the Ciphertext-Policy Attribute-based Encryption in Cloud Computing.

We propose a Key generation protocol to resolve the Key Escrow problem in Cloud Computing.

This algorithm can restrict the Admin and cloud authority from getting to know each other's unique key so that none of them can decrypt the data of users individually. Hence, data confidentiality can be maintained.

3. Algorithms Used

RSA Algorithm – This algorithm is used for secure transmission of information and can be done in four steps – Creation of the Key, Encryption, Key delivery, Decryption. It includes a Public and Private key. The Public Key is used for encrypting the data and know to everyone.

KeyGen Algorithm – This algorithm is used for encrypting/decrypting the data. There are two types of encryption algorithms - Symmetric key and Public key.

Symmetric Key - This algorithm uses a single shared key which is used to keep the data secret.

Public Key Algorithm - This algorithm uses a Public and Private Key. The Public key is available to every user and admin by means of the digital certificate. The sender uses the public key to encrypt the data. User those have a private key can decode the information.

In this, we put forward double encryption technique on the basis of two-party key generation, Here, the admin can only see the patient data in encrypted form and a

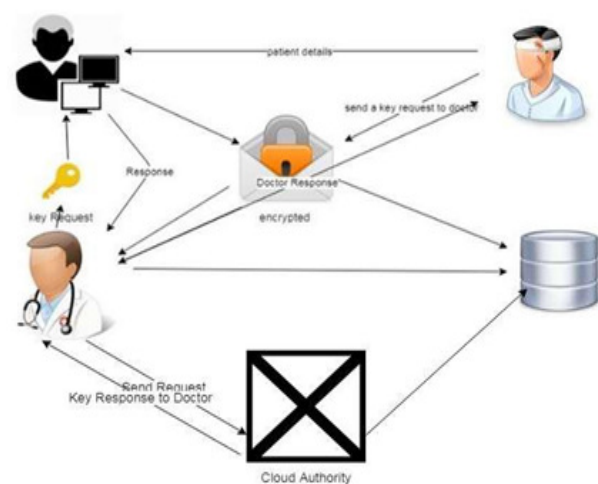
unique attribute is taken as a key to decrypt the data when the doctor wants to access the patient's data.

When the doctor wants to decrypt the data of the patient, he requests the key from admin. When he gets the original admin key, he sends this Key to CA (cloud authority) for another key with which he can be able to send a response to the patient particularly. (2,8,9)

Through this, admin and cloud authority are restricted to see the data of patient and key escrow problem is resolved.

4. System Architecture

The system architecture of our proposed model consists of four different modules – Admin, Doctor, Patient and Cloud Authority. Below we have given a detailed representation of our proposed model.



Admin - They will store and upload the personal health records of the patient. They respond to the doctors with the key and also request to the Cloud authority for the secret key.

Patients - Patients are the users who will register and can see their data and response from the doctors. They will send a key request to the doctors for accessing their encrypted details.

Doctor - Doctors will respond to the patient by requesting the secret key from the Admin and Cloud Authority. They will have the health records of the patients in encrypted form.

Cloud Authority - They are a semi-trusted party which has the secret key in the database and responds to the Admin with the key. When the Cloud Authority responds with the key to the Admin, the decryption operation takes place.

The proposed system contains several phases:

- 1) Initial System State- This phase contain admin page where admin login and enter the patient details,
- 2) Data encryption- Here, the data which admin enters is encrypted using Cipher encryption technique and only a single unique attribute is in decrypted form, which is not visible to admin as well as doctor,
- 3) Key Generation- now, the unique attribute of patient detail is used as a key which admin provides to the doctor.
- 4) Data Decryption- when the doctor needs to see the data of patient, the log in and sends request to admin for key to decrypt the data, also if he needs to respond to patient, he sends the admin key to CA and when he gets the CA response he send response to the patient.(4,5,6). CA verifies if the admin key is correct, and then only he sends the KEY to the doctor. patients also need to log in and send a request to admin to get his details and doctor name.

5. Conclusion

In our paper, we implement Cipher text Attribute-based Encryption (CP-ABE) to make health care data secure in cloud. Our proposed system issues a key that eliminates the Key Escrow problem. The user keys are generated by calculation such that the key generation cannot obtain the private key. The improved key issuing protocol enhances the data privacy and authenticity in cloud computing against Admin and Cloud authority as well as illegal users (3). Cost of ciphertext for storing and computing can be depreciated. The proposed system is scalable and systematic to securely manage the patient's data in healthcare system in cloud computing.

References

- [1] M.Karthikraj, S.Arunkumar and M.Muralikrishnan, "Secure Data Sharing In Cloud Computing By Implementing Amended Attribute Based Data Sharing Scheme", International Journal of Engineering And Computer Science ISSN: 2319-7243.
- [2] "A Survey on Data Sharing Using Encryption Technique in Cloud Computing", was published by . Swarup Kshatriya and Dr.Sandip M Chaawar .
- [3] Shoolan Wang, Kaityi Liang MemberWeixin Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security.
- [4] "Survey on attribute-based data sharing scheme revisited in cloud computing",done by Mr. Swapnil R. Patil, Prof. N. D. Kale, Multidisciplinary Journal of Research in Engineering and Technology.
- [5] Ms.Dipali Patil, Dr.P.K.Deshmukh, "Data Security in Cloud with Efficient Keyword Search", International Journal of Scientific & Engineering Research, Volume 7, Issue 1, January-2016 ISSN 2230-5519.
- [6] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-Policy Attribute-Based Encryption", Proceedings of the 2007 IEEE Symposium on Security and Privacy.
- [7] V. Goyal, O. Pandey, "Attribute-based encryption for fine-grained access control of encrypted data," in 13th ACM conference on Computer and communications security.
- [8] Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems".
- [9] Kaitai Liang and Wiilly Susilo, "Searchable Attribute-Based Mechanism with Secure Cloud Storage", IEEE Transactions on Information Forensics and Security
- [10] Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of the smart grid. IEEE Transactions on Cloud Computing, 3(2):233–244,2015.
- [11] C. K. Chu, W. T. Zhu, J. Han, J. Xu, Security concerns in popular cloud storage services. IEEE Pervasive Computing,
- [12] T. Jiang, X. Chen, "Towards secure and reliable cloud storage against data re-out sourcing". Future Generation Computer Systems, 52:86–94, 2015.
- [13] T. Padmapriya, V.Saminadan, "Performance Improvement in long term Evolution-advanced network using multiple input multiple output technique", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, Sp-6, pp: 990-1010, 2017.
- [14] S.V.Manikanthan & K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27 Feb. 2015,Publisher: IEEE,DOI:10.1109/ECS.2015.7124833.

