IMPLEMENTATION OF CLOUD COMPUTING DATA SECURITY FOR HEALTHCARE MONITORING SYSTEM

[1]R. Kamala, [2]K. Mythili

[1]M. Phil (Research Scholar), [2]Assistant Professor
Department of Computer Science and Applications,
Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya(Deemed to be University),
Enathur, Kancheepuram, India

ABSTRACT

In this paper, mainly focuses on Health Records security requirements for storing, searching, accessing, sharing and auditing in Cloud Healthcare Monitoring System. We introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location. The benefits of web-based cloud computing services are huge, which include the ease of accessibility, reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility and immediate time to market.

IndexTerms - **Two-factor authentication, Health Records Auditing Phase, Security Analysis.**

I. INTRODUCTION

Services like storage and computing in Cloud became well known because of the important advantages such as scalability and cost efficiency. In Cloud Computing architecture, the service owner can scale down or scale up the sources based on his/her specifications hence, he/she can pay only to the resources which he/she used like electricity bill in houses. The current charge changes every month based on usage units; similarly, the data owner can also pay the Cloud providers only for the usage of computing cycles and storage capacity as per the Service Level Agreements (SLA's). Healthcare is one of the essential services of every nation including India. Cloud servers are very advantageous while sharing the data over the internet.

II. EXISTING SYSTEM

In a Shared Cloud Environment like hospitals, the Centralized system might used by different doctor say A and B working on rotational shifts. Here the user's personal are sensitive data may be prone to risk. In these cases, user secret keys cloud is easily stolen or used by an unauthorized party. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares. In such environments a more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-banking services. In addition to a username/password, the user is also required to have a device to display a one-time password.

III. METHODOLOGY

The earlier works in ABE literature was created on single authority architecture; the KGA has rights to produce any user secret key with the help of master key. Consequently, it inherited the key escrow problem with this type of architecture.

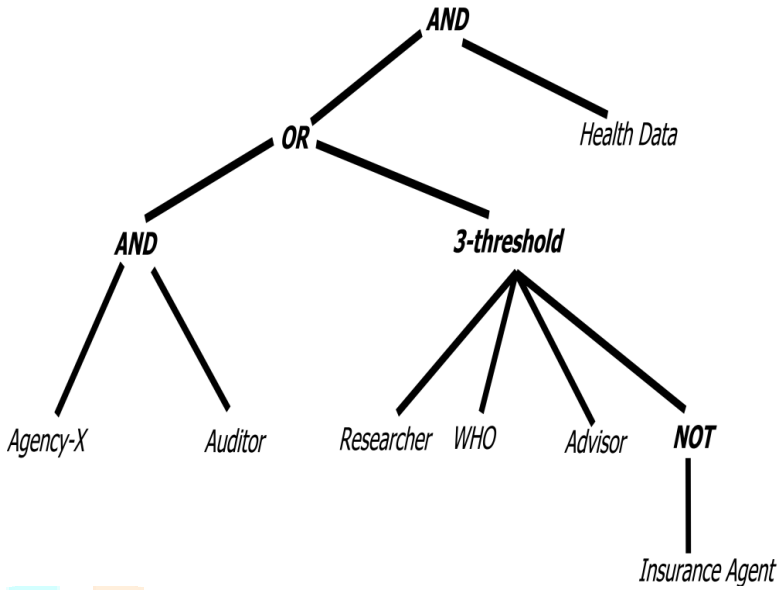

Fig 3.1: Non-monotonic access structure example

1. To create a secure framework for ensuring Health Records Integrity using Fine Grained Auditing and CP-ABE performs secure auditing task without exhibiting patient identity and protecting data privacy in the Cloud server. The recommended system consists of two-authority key generation method to determine the key escrow issue and fine-grained auditing.
2. Public Auditing: Our design provides public verifiers to check the integrity of Health Records without accessing entire data from the Cloud.
3. Identity Privacy: Our method cannot enable the public auditor to identify the patient identity while auditing the portion of patient information.
4. Key escrow: Our scheme explains the key escrow problem by utilizing two authority key generation method. In this method, Cloud server and KGA generate keys individually and send to the user. Consequently, the user can make his secret key with the help of those two keys.

3.1 Preliminaries Access Policies

The Health Records owner can define the access policies in the form of a tree structure by using decryptor attributes. Here, 'A' can render tree access structure. It comprises leaf and non-leaf nodes, leaf nodes are the decryptor attributes and non-leaf nodes are 'AND', 'OR', 'Threshold-K' and 'NOT' gates. When the data owner uses 'NOT' in the access tree can be called as non-monotonic access structure. The above tree structure displays an instance of a non-monotonic access structure defined by patient Bob. Bob requires verifying his/her medical data integrity in the Cloud. Accordingly, he confers permission to public auditors to access his information from the Cloud server for data integrity checking. Here, the tree contains 'AND', 'OR', 'NOT' and 'K-Threshold' gates as non-leaf nodes and public auditor attributes as leaf nodes. In this tree, non-negated auditor attributes are Health Data, Agency-X, Auditor, Researcher, World Health Organization (WHO), Advisor, and negated auditor attribute is Insurance Agent. Sample of authorized access policy is as follows.

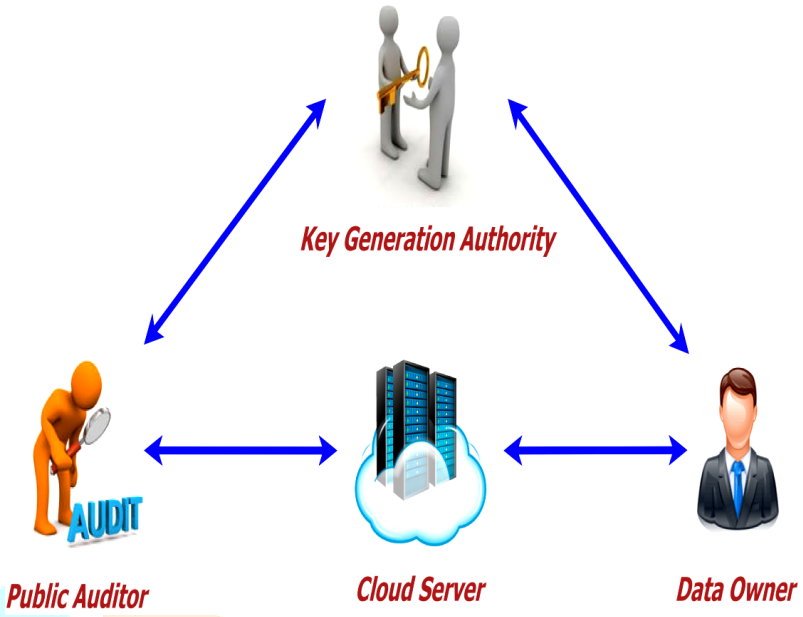

Fig 3.2 System model for secure Health Records auditing service

Is an Auditor related to Health Data from Agency X' ↔ {(Auditor 'Λ' Agency X) 'Λ' Health Data}. Instance of unauthorized access policy is: 'Insurance Agent is Researcher and an Advisor related to Health Data' ↔ {Insurance Agent 'Λ' Researcher 'Λ' Advisor 'Λ' Health Data}.

3.2 System Model

Data owner: Data owner is a patient, who is concerned with storing his Health Records in the Cloud server for overcoming the storage and computation cost.
Public Auditor: The public auditor is the public verifier who wishes to verify the correctness of outsourced Health Records in the Cloud server.
Cloud Server: It presents storage and computation services. Data owner can deposit his information in the Cloud to distribute it with others.
Key generation authority: An authority creates secret keys of all users in CPABE scheme. The KGA includes all rights regarding key creation, updating, and deletion. Hence, KGA can decrypt the data as much as possible.

3.3 Proposed Framework

3.3.1 Setup Phase

Here, public key PK and master key MK are generated for Cloud server and KGA as displayed in Fig.3.3 setup phase. The controller defines a bilinear group 'G0' of prime order 'p' and generator 'd' based on safety parameter. It picks a couple of hash functions h: {0,1}* → G0 and h1:G1→Zp* from the universal group. First, KGA creates its master key and public key MKK and PKK respectively by using random exponent α.
MKK ← α
PKK ← d α
Secondly, the Cloud server generates its master key and public key MKC and PKC respectively. It selects random exponent 'β' to produce two keys.
MKC ← d β
PKC ← e(d, d) β
The Cloud server and KGA both use these two keys for all activities like creating of data owner keys, auditor keys and so on. The security assumption is, these two authorities cannot share their master keys to any extent.

3.3.2 Key Generation Phase

KGA creates data owner/ auditor/ user keys. Both KGA and Cloud server have engaged in this phase for generating secret keys by using two authority computation scheme. This phase is depicted in fig.3.3. Both KAG and Cloud server authorities separately generate individual secret keys PKK, Ut and PKC, Ut respectively. PKUt← PKK,Ut PKC,Ut

3.3.3 Encryption Phase

This phase transforms plaintext into ciphertext to secure information from unauthorized users or any other who can harm the data. Initially, the data owner specifies access policies 'A' based on target users attributes

3.4 Health Records Auditing Phase

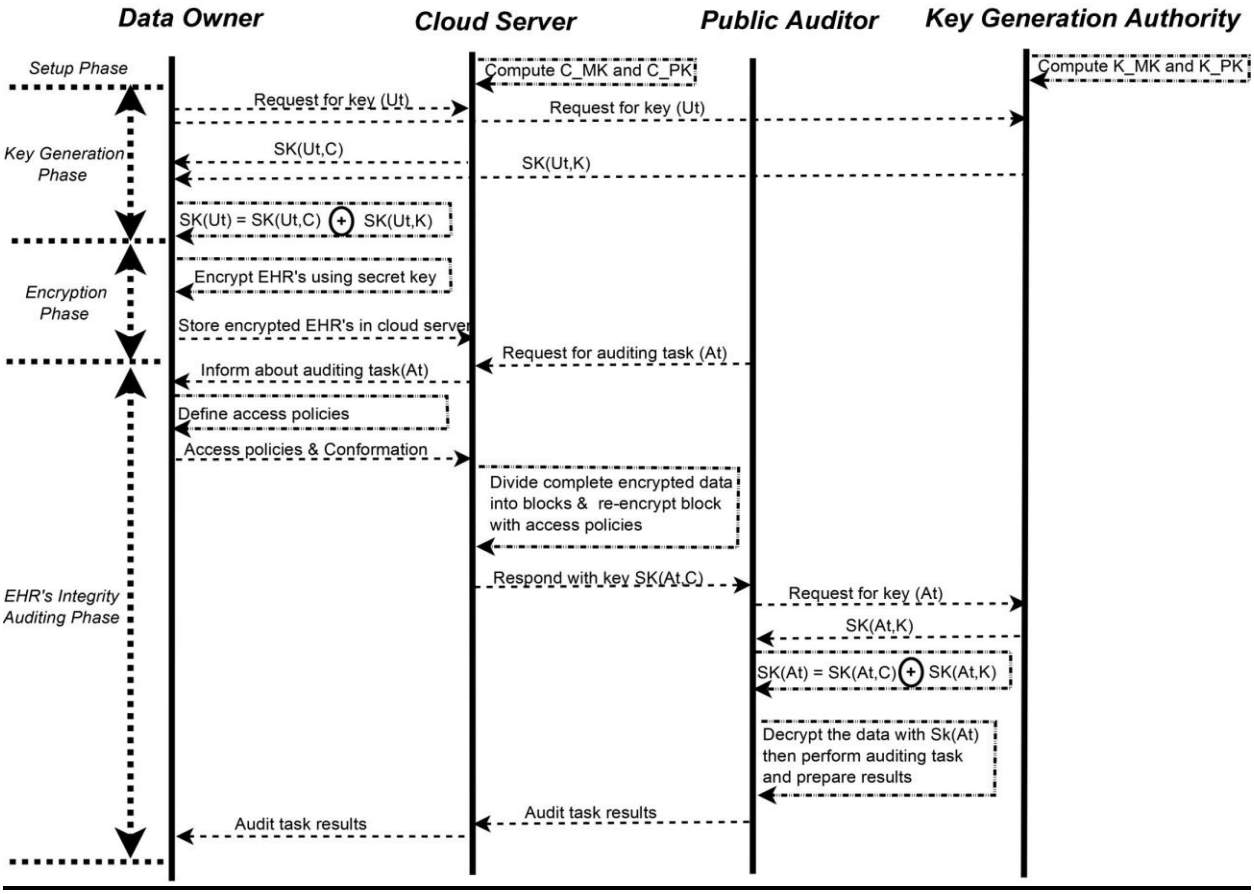

Fig 3.3: Secure framework for Health Records integrity auditing

SK - Secret Key, Ut - User ID, C - Cloud server, K - KGA, At - Auditor ID, C_MK - Cloud server master key, C_PK - Cloud Server Public key, K_MK - KGA master key, C_PKKGA - Public key

3.4.1 Auditing setup phase

In this, first auditors forward a request to Cloud server about EHRs auditing challenge with their details. The data owner specifies the access policies using auditor details and sends them to the Cloud server as displayed in Fig. 3.3.

3.4.2 Re-encryption phase

It can re-encrypt the ciphertext that is encrypted earlier by using new auditor access policies as conferred in Fig. 3.3.

3.5 Security Analysis

In our mechanism, the CP-ABE scheme is adopted and two authority key computation method for maintaining privacy in Health Records during integrity auditing. The proposed mechanism associated with some existing mechanism as displayed in table 3.1.

	PDP[85]	WWRL[86]	Our Scheme
Public Verifying	True	True	True
Data Security	False	True	True
Identity Privacy	False	False	True

Table 3.1 Comparison of our mechanism with existing privacy preserving mechanisms

3.6 Performance Analysis

The table 3.1 displays the comparison of public verifying, data security and identity privacy between the proposed scheme and some existing systems. PDP and WWRL do not support identity privacy. In the recommended framework, to conserve identity privacy two-authority key computation architecture and ABE are used. In ABE scheme, the logic is described by the non-monotonic access policy. It allows negative attributes to represent the access policy very explicitly than in other methods. Also, our framework achieves additional fine-grained auditing service; it means the entire information is partitioned into small blocks and transfer to the auditor for verification purpose. This procedure enhances the efficiency. The proposed system also solves key escrow problem by applying two authority computations.

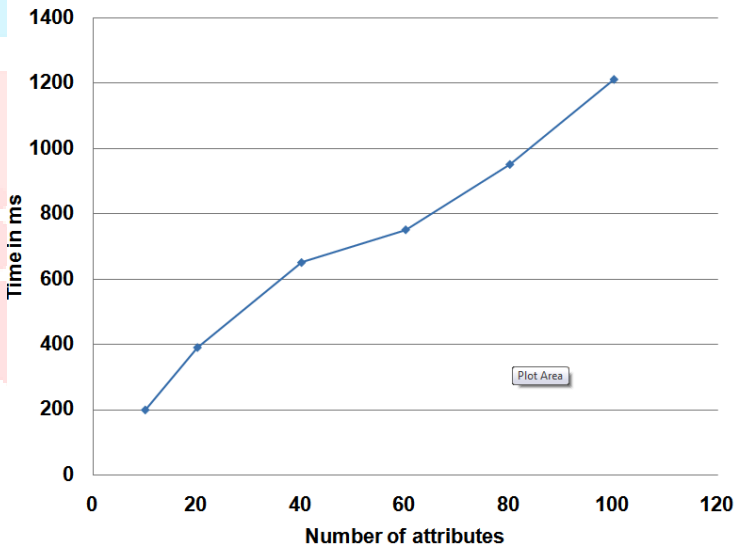

Fig 3.4 Encryption time

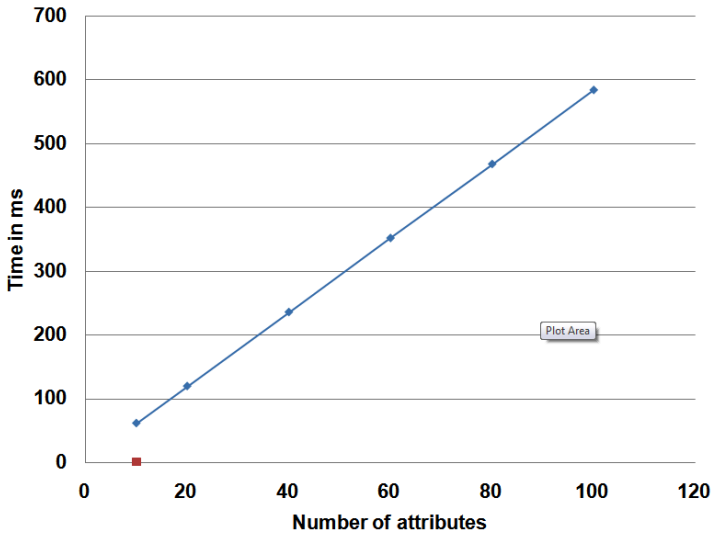

Fig 3.5 Decryption time

At present, the performance of the recommended framework is evaluated for fine-grained auditing scheme. The experiment is conducted using pairing based Cryptography(PBC) library and a 160-bit elliptic curve group based on the supersingular curve 'y2=x3+x' over a 512-bit finite field. All benchmark test cases are performed on an Ubuntu 14.04 desktop platform with Intel Core(TM) Core i7-5500U CPU 3.0 GHz and 8GB. All the experimental results are the average of 10 trials. Fig.3.4 describes the encryption time of Health Records. It involves two phases, namely first encryption phase and re-encryption phase. The encryption time is proportional to the number of attributes. The attributes vary from 10 to 100 respectively as the time changes from 199 to 1210ms. Fig.3.5 shows the decryption time of Health Records. The decryption time is proportional to the number of attributes. The attributes change from 10 to 100 respectively as the time changes from 68.1 to 583.3ms.

IV. CONCLUSION

In this CHMS, patients, doctors, chief doctor are connected to eclipse private Cloud. The doctors stores his patient's health records in private Cloud and gave the permission to those who wish to access the Health Records. The doctors can access the patient's Records through the internet and, analyze, and send the reports to the patient.

REFERENCES

[1] J. Bethencourt et al. Ciphertext-Policy Attribute-Based Encryption, Proceedings IEEE Symposium Security and Privacy, (2007) 321-334.
[2] S.S.M. Chow, Removing Escrow from Identity-Based Encryption, Proceedings Int. Conf. Practice and Theory in Public Key Cryptography (PKC '09)(2009) 256-276.
[3] The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/
[4] G. Ateniese et al. Provable Data Possession at Untrusted Stores, Proceedings 14th ACM Conf. Computer and Comm.Security (CCS '07) (2007) 598-610.
[5] H. Shacham et al. Compact Proofs of Retrievability, Proceedings 14th Int. Conf. Theory and Alication of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08)(2008) 90-107.
[6] M. Chase et al. Improving Privacy and Security in Multi-Authority Attribute Based Encryption, Proceedings ACM Conf. Computer and Comm. Security (2009) 121-130.