OCSC
Oceania Cyber Security Centre

A Secure Cloud-Based Healthcare System

Project Impact White Paper 2020

Abstract

In this paper we explore the security implications of storing healthcare records in a cloud environment. We first explore the problem and show that the traditional encryption approach is difficult to manage and error prone. Then we explain the high-level operation of our solution and demonstrate its advantages. Finally we conclude this paper with a summary of what we have discussed and explain the benefits of our solution.

RMIT UNIVERSITY
LA TROBE UNIVERSITY
MONASH University
VICTORIA UNIVERSITY

Problem Overview and Motivating Example

Healthcare Records and the Healthcare Provider

Healthcare records are of fundamental importance to the healthcare provider. Thus we want provide almost instantaneous access to all authorised parties while minimising cost.

At the same time, we want to ensure the security of the records against malicious actors. We will motivate this problem by developing a small hypothetical example.

Storage of Healthcare records in the Cloud

Cloud-based hosting providers offer great value for their cost because they are able to offer economies-of-scale, among other benefits (Amazon, 2020). So we could store all the healthcare records in the cloud according to Figure 1.

A patient may have many specialised records for different aspects of their healthcare, but we group all records related to a patient into one record for simplicity.

Record Number	Name	…
R1	John	…
R2	Sally	…
R3	Sam	…

Figure 1

Security of Healthcare Records in the Cloud

It is obvious that directly storing all the records offers a number of advantages in terms of cost and accessibility, but has inherent security concerns. The main problem is that the cloud is vulnerable to exploitation, because the cloud has direct access to the records.

We can overcome this problem by encrypting each record before upload. In this case, even if the cloud is compromised, then an adversary will be unable to recover any useful information about the records because they are encrypted. Let us illustrate this approach with an example.

Suppose that we have the following users of the healthcare system, with their associated attributes and encryption keys, as listed in Table 1. The keys are randomly generated and assigned to each user.

User	Attributes	Key
John123	Doctor, Cardiology	Key1
Jay456	Doctor, Neurology	Key2
Bob42	Nurse, Neurology	Key3
Jane84	Nurse, Cardiology	Key4

Table 1

Suppose further that we wish R1 to be accessed by a doctor, nurse or receptionist from the cardiology department. We can express policy using the following rule: P = '(Doctor OR Nurse OR Receptionist) AND (Cardiology)'.

Then we would store the encrypted record R1 on the cloud as shown in Figure 2. We denote encrypting record R with encryption key K as E (K, R).

Record Number	Name	…
R1	John	…
R2	Sally	…
R3	Sam	…

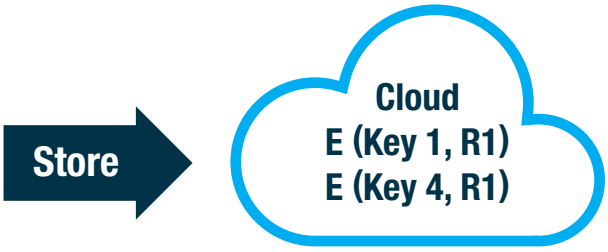

Figure 2

Thus the cloud stores encryptions (E (Key1, R1) and E (Key4, R1)) for John123 and Jane84 because only these users satisfy the given policy. As a result, only these users are able to decrypt the record correctly.

Problem Statement

The problem with this traditional method presented so far is that there is a heavy dependence on users and their encryption keys. The number of encryptions depends on the number of users requiring access to any particular record. Each time there is a new user who needs access to a record, a new ciphertext needs to be generated under the new user's key. This becomes increasingly difficult to manage as many medical systems have a large number of users.

Thus, we will demonstrate that this project develops a solution that overcomes these problems.

Problem Solution

Attribute-Based Encryption

Our solution uses an advanced encryption technique called Attribute-Based Encryption, to encode the attributes directly into the encryption process. Ultimately, this allows us to be more efficient when storing encrypted records on the cloud, as we shall see.

For the purpose of easing exposition, we will present a high-level explanation of the operation of our solution, which will be based on the same example found in the previous section. Again, suppose that we wish to encrypt R1 according to the policy: P = '(Doctor OR Nurse OR Receptionist) AND (Cardiology)'. This is illustrated in Figure 3. Observe that we do not need to look up a user's particular key before encryption.

Record Number	Name	…
R1	John	…
R2	Sally	…
R3	Sam	…

Figure 3

In order for the users to decrypt correctly an entity known as Attribute Authority, which is fully trusted by all users of the system, generates keys for each user based on their attributes. The attributes can include more than one institute, but for simplicity we will consider only one institute. These attribute keys generated by the Attribute Authority are listed in Table 2.

User	Attributes	Attribute Key
John123	Doctor, Cardiology	AttKey1
Jay456	Doctor, Neurology	AttKey2
Bob42	Nurse, Neurology	AttKey3
Jane84	Nurse, Cardiology	AttKey4

Table 2

Now John123 is able to download E (P, R1) from the cloud and decrypt using his key AttKey1 to recover R1. Similarly, Jane84 can also download E (P, R1) from the cloud and decrypt using her key AttKey4 to recover R1. On the other hand, both Jay456 and Bob42 are unable to recover R1 because the attribute keys fail to satisfy the policy P.

Since the policy is now encoded in the ciphertext, all users that satisfy the policy can now share the encrypted version of the record. This significantly reduces the complexity of managing and enforcing the security of the records via encryption.

Conclusions and Benefits

Introduced the Problem

We introduced the problem of securely storing healthcare records in a cloud environment. We highlighted the intrinsic difficulties of the traditional approach, where each record is independently encrypted to satisfy a given policy or rule.

Explained our Solution

We explained the high-level operation of our solution that demonstrated that we could overcome the inherent difficulties by employing Attribute-Based Encryption techniques.

Outlined the Benefits

Demonstrated that our solution has a number of advantages as follows.

1. Sharing of encrypted records allows for simpler updating of records
2. No need to look up a user's key before encrypting
3. Complexity of key management is reduced

Bibliography

Amazon. (2020). *Six Advantages of Cloud Computing*. Retrieved 2020 from docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing

OCSC
Oceania Cyber Security Centre

Door 34, Goods Shed,
Village Street, Docklands VIC 3008

Email: info@ocsc.com.au

ocsc.com.au