Global Journal on Application of Data Science and Internet of Things
Vol. 4, Issue 1 – 2020
ISSN: 2581-4370

Securing Data in Cloud by Time Based Encryption

C. Sunanthini[1], **M. Gowshalya**[1]
[1]*Lecturer II, DMI St. John, The Baptist University, Lilongwe.*

Abstract

Data to be shared in the cloud faces many challenges in security. Cloud computing is chosen for this purpose as it reduces cost for data management and its available resources. It is necessary to have an efficient data access control to protect data from third party cloud server. Cipher text-Policy Attribute-based Encryption is used for data security in the cloud. A time access control is very important while sharing data on the cloud. The encrypted data is uploaded by the data owners with a time limit so that other users cannot access the data beyond that corresponding limit.

Keywords: Securing, Data Access Control, Encryption.

Introduction

Cloud computing is the on demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Cloud computing is an information technology (IT) service which retrieves the data stored in the cloud by accessing the internet. It saves the user's data to an offsite storage system that is maintained by the cloud provider. Hence, the data are maintained, operated, and managed by a cloud storage service provider on storage servers that provide more advantages on easy data sharing and cost reduction. Thus, more and more enterprises and individuals outsource their data to the cloud to be benefited from these services. Although the infrastructure involved in the storage of data in the cloud is much more powerful and reliable than personal computing device, they are still facing the problem in data confidentiality and preservation. Therefore, secured access control has become a challenging issue in public cloud storage.

Securing data is always of vital importance because of the critical nature of cloud computing and the large amounts of complex data. Data security is an important aspect of quality of service and hence security must be imposed on data by using cryptographic strategies to achieve secured data storage.

There are many cryptographic methodologies to protect the data and provide access control in the untrusted cloud sever.

One of the useful cryptographic methods is Cipher text-Policy attribute Based Encryption (CP-ABE). In CP-ABE, a user's private-key is associated with a set of attributes, and a cipher text that specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. This strategy protects the data by providing flexible access control, and provides constraint on access of the data, but this will not handle time sensitive data.

To tackle the problem of handling time sensitive data, time encryption can be used to provide access privilege up to a specific time. Time based encryption is a two-factor encryption scheme combining public master key and time-dependent encryption which is kept confidential by a time-server up to a specific time.

In some cases, unauthorized users may fraudulently access the data and misuse it. The central authority maintains records of users. If there is any mismatch of the data entered or misrepresentation, the user’s data will be revoked. Hence, to ensure security, the revoked user cannot access the data anymore.

Another important aspect of cloud computing security is to provide learning-based methods. This learning method is incorporated to improvise the security of outsourced data by identifying its ideal behavior. It is important in the field of organization using the public cloud to automate the agent to determine the behavior of the outsourced data with increase in vulnerabilities. Hence, Reinforcement learning is best suited for this scenario.

Therefore, proposed methodology enhances the security of data in the public cloud with time access control and also the learning agent area automated to contrive the security and content of the outsourced data.

Related Works

Data in the cloud can be effectively acquired by anyone at any instance of time. Providing data security and data augmentation in cloud storage has definitely been a confounding work. Numerous work and researchers have been chipped away at this issue to give better data access control and data augmentation in the cloud storage.

In this article, a fine grained and time release access control by using CP-ABE (Ciphertext-Policy Attribute- based Encryption) with TRE (Time Released Encryption) has been discussed. This method was first proposed to implement fine-grained access control of document by taking a typical university setup. This work has led to the future scope of partial encryption and decryption. But unencrypted data cannot be secured. In this paper, the key generation is implemented using bilinear pairing of access structure. This increases energy consumption. To overcome this, elliptic curve cryptography was proposed which generates the key in constant size and reduces energy consumption and time taken to generate the keys. This access control is needed when the data is shared to a group of users. Along with access control, many other security aspects of data are required. Here a secured group data sharing is proposed by integrating the following methodology: 1) data confidentiality and integrity, 2) access control, 3) data sharing without using compute-intensive re-encryption, 4) insider threat security, and 5) forward and backward access control. By using this methodology, two keys are generated per user. The user gets only one key to access the files in the cloud and the other key is stored in a trusted third party server. This paper provides a foundation for future work for limiting the trust level of third party sever, thereby improving the system by avoiding insider threats. To prompt more security from various attacks, Hybrid Encryption RSA (HE-RSA) has been proposed along with AES to ensure consistency and trustworthiness. This methodology proved its efficiency in combating brute force attacks, and mathematical and timing attacks. This methodology has not been implemented in a real cloud platform. In the data sharing between data owner and data user, a scheme proxy re-encryption was proposed. In this, data owner encrypts the message using own public key before sharing it in cloud. After receiving the request from data consumer by their own public key, data owner generates a proxy re-encrypt key, by re-encrypting the encrypted message using data owner's private key and received public key, and uploads this re-encrypted message to the cloud. Data consumers download the message from the cloud and decrypt using their own private key. But this research leads to the problem of designing generic framework to implement proxy re-encryption and achieve selective security. By extending ciphertext-policy attribute-set-based encryption, hierarchical attribute-set-based encryption (HASBE) is proposed to provide access control in a hierarchical structure of users. This work implements fine-grained access control but it lacks in time access control. The data in the cloud are in the different form. In this method, one data always stays in the same cloud and other data needs to be transmitted from one cloud to another. This study is based on all three layers of cloud (SaaS, IaaS and PaaS) by dividing the data into two categories: data in rest and data in transit. Data in rest can be stored in private cloud whereas data in transit needs cryptographic strategies like block cipher, stream cipher, and hash function. This paper has only given the outline of protecting the data using various cryptographic encryptions. Asymmetric cryptography algorithm has more security in sharing the key between two users. Here data security in cloud is proposed using RSA algorithm. As RSA provides high potential data in encryption methodology, it can be suitable for data security, but, here we have not worked on access control in the cloud. Symmetric algorithm handles large volumes of encryption data at a high speed and in an efficient manner. The security of data is enhanced in the cloud by using symmetric cryptosystems. Hence, Advanced Encryption Standard (AES) algorithm is implemented which uses less memory space and provides high throughput as compared to other symmetric algorithms.

Cipher Text-Policy Attribute-Based Encryption

In **cipher text-policy attribute-based encryption** (CP-ABE) a user's private-key is associated with a set of **attributes** and a **cipher-text** that specifies an access **policy** over a defined universe of **attributes** within the system.

Time Based Encryption

After structuring the access policy, time based encryption of data is needed to provide an access privilege to the data user till the specific time. Consider a scenario in which the data owner encrypts the file, uploads it in the cloud with current timestamp, and provides a last time to access the file. So, the intended users can decrypt the message until the specific time provided by data owner. From the security aspects, Time Based Encryption ensures that 1) only the intended user can access the data, 2) Even the intended user needs to get his identity verified from the central authority to access the file, and 3) A time privilege is provided such that specific user can use the file up to the time period provided by the data owner.

Proposed Design: System Model

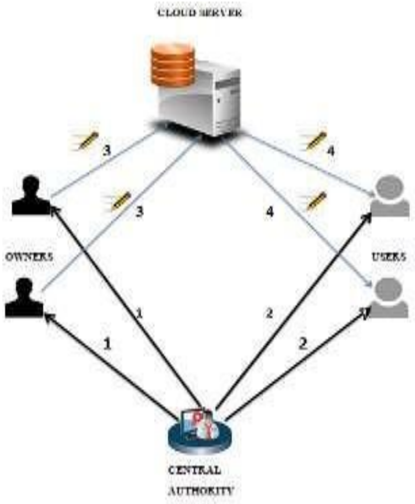

Figure 1.Architecture of Proposed System

1. Public Master Key (PMK) and Secret Key (SK)
2. PMK and SK Issue
3. Data Encrypt and Upload
4. Data Query and Decrypt

Algorithm Used

Various cryptographic algorithms are used to enhance the security while sharing data in the cloud. Hence, these algorithms are used with CP-ABE scheme which consist of four phases namely: Setup phase, Key-generation phase, Encrypt phase, and Decrypt phase.

Setup phase

In this phase, the universe of attributes U = {S1, S2, S3,………,Sn} is taken as input and the output of the phase is access tree and access policy for data owner and data user.

KeyGen phase

In this phase, the key generation algorithm takes an input of access policy attributes Å and generates the Master public key and secret key. This has been implemented in registering data in the cloud. Thus data owner/user intends to provide the data while registering in the system and the data is checked with access policy. If entered data matches with the access policy, the keys are randomly generated for different users. RSA algorithm is used to generate keys randomly.

Algorithm-1 Key Generation: Input

Two prime number p, q

Computer

Compute $n = p*q$ and (phi) $\varphi = (p-1)*(q-1)$.

Choose an integer e, $1 < e < \varphi$,

Such that $\gcd(e, \varphi) = 1$.

Compute the secret exponent d, $1 < d < \varphi$, such that $ed \equiv 1 \pmod{\varphi}$.

For each user who satisfies access policy

The public key is (n, e) and the private key (d, p, q).

End for return private key

n is known as the modulus.

e is known as the public exponent.

d is known as the secret exponent.

This private key is sent to the users via their registered mail id. Public key is used as Master public key to hash the account password using Bcrypt algorithm. As user credentials are stored in the cloud database, the password is hashed to enhance the security.

Algorithm-2 Encryption of Password

Input

Password, Public Key, Cost, Salt

Compute

for each account password do

State ← Blowfish Setup (cost, salt, Public Key)

ctext ← Password

hashed ← hashpw (state, ctext)

end for return hashed value to store in database

Encrypt phase

The data is uploaded in the form of files. These files uploaded by the data owner in cloud are needed to be converted as the ciphertext. So, the input of this phase is data in the form of files and the output of the files is encrypted text. This is to ensure the security of the file in the public cloud. So, the data owners upload the files by entering their own secret key which is generated by the Central authority in the key generation phase. A symmetric cryptosystem uses only one secret key to encrypt the file. Symmetric cryptography encrypts the data faster and in a more secured manner. There are various symmetric algorithms; in this AES algorithm is used with PBE (Password Based Encryption). Instead of generating different keys for file encryption, a constant password is taken which is generated as a 128-bit key and goes to 10 rounds of permutation, finally producing the cipher text.

Decrypt phase

This phase is used by data user who needs to get the original content of file uploaded in the cloud. Before decryption, the data user gives request to download the file and the request is sent to Central authority. After the approval of Central authority, data user enters his secret key which is generated in key generation phase and downloads the file. The file decryption is also implemented with AES with PBE algorithm.

Reinforcement Learning

Reinforcement machine learning algorithm is a learning method that interacts with its environment by producing actions and discovers errors or rewards. Trial and error search and delayed reward are the most relevant characteristics of reinforcement learning. Simple reward feedback is required for the agent to learn which action is best; this is known as the reinforcement signal. The necessity of reinforcement learning is the data owner’s need to know about intended users’ progress and the difficulties faced while using the files they uploaded, so that they can adapt their work to meet their user’s needs. For this scenario, reinforcement learning can be applied in the form of feedback. Feedback is information provided by the data users regarding aspects of understanding of the data provided by the data owner. This learning can be well suited in the case of schools or colleges. The data owner is staff and data user is the student. The student provides the feedback from the experience they are gaining from their staff. This in turn increases student’s motivation towards the subject, and subsequently decreases the number of students skipping classes or dropping out. The staff also uses a range of targeted feedback strategies to comprehend the student’s understanding of the requirements of an assessment task. In this paper, instructive feedback is used. There are various types of instructive feedback. In such a scenario, Parallel feedback is used, where the staff gives students a different form of the stimulus material that requires the same response. To gather the feedback from the various users and visualize in the form of graph, K-means clustering is used.

Algorithm-3 K-Means Clustering

Let X = {x1,x2,x3,……..,xn} be the set of feedback and V = {v1,v2,…….,vc} be the set of centers.

1. Randomly select *‘c’* cluster centers.
2. Calculate the distance between each data point and cluster centers.
3. Assign the data point to the cluster center whose distance from the cluster center has minimum cluster centers.
4. Recalculate the new cluster center using:

$$v_i = (1/c_i) \sum_{j=1}^{c_i} x_i$$

where, *‘c_i’* represents the number of data points in i^{th} cluster.

5. Recalculate the distance between each data point and new obtained cluster centers.
6. If no data point was reassigned, then stop, otherwise repeat from step 3.

Performance Analysis

An important aspect of this paper is to select an appropriate algorithm to encrypt and decrypt the file uploaded in the public cloud. To ensure data confidentiality, integrity, and faster encryption of data, symmetric algorithm was used. There are various symmetric algorithms among which the best three algorithms were selected and compared. Thus in this paper, AES-PBE algorithm is compared with BlowFish and DES algorithm.

Encryption Execution Time

The experimental result for encryption algorithms BlowFish, AES-PBE and DES are shown in Table 1, which shows the comparison of these algorithms using ten different file sizes.

Table 1.Comparison of Encryption Algorithms BlowFish, AES-PBE and DES using ten different file sizes

File Size (MB)	**Blow Fish (Sec)**	**AES-PBE (Sec)**	**DES (Sec)**
0.01	2	1	1
0.03	2.001	1.02	1.04
0.05	2.5	1.05	1.9
1.12	2.8	1.4	2
2.04	3	2	2.5
3	3.5	2.8	3
4.8	4	3	3.5
5	4.5	3.9	4
7	5	4.1	4.5
10	5.5	4.4	4.9

By analyzing Table 1, it is clear that the time taken by AES-PBE algorithm for the encryption process is quite less as compared to the time taken by BlowFish and DES algorithm.

Decryption Execution Time

The experimental result for decryption algorithms BlowFish, AES-PBE and DES are shown in Table 2, which shows the comparison of these algorithms using ten different file sizes. The results are tabulated as shown below.

Table 2.Comparison of Decryption Algorithms BlowFish, AES-PBE and DES using ten different file sizes

File Size (MB)	Blow Fish (Sec)	AES-PBE (Sec)	DES (Sec)
0.01	2	1	1
0.03	2	1	1.04
0.05	2.1	1.02	1.9
1.12	2.3	1.3	2
2.04	2.4	2	2.5
3	3	2.3	3
4.8	3.5	2.8	3.5
5	4.1	2.9	4
7	4.4	3.7	4.5
10	5.2	4.1	4.9

The analysis of Table 2 reveals that the time taken by AES-PBE algorithm for the decryption process is much less than the time taken by BlowFish and DES algorithm.

Conclusion

In this paper, algorithms have been used to save the data which is shared in public cloud. The best method to provide fine-grained access control is CP-ABE method with time based encryption. From the tables, it is proved that AES–PBE algorithm takes the least amount of time for the process of encryption as well as for decryption. As the data is passed in the cloud and encryption is done, it is highly secure.

References

1. Qin Z., Xiong H., Wu S., & Batamuliza J. (2016). A survey of proxy re-encryption for secure data sharing in cloud computing. *IEEE Transactions on Services Computing*.
2. Tadapaneni, Narendra Rao, Cloud Computing-An Emerging Technology (March 1, 2020). Volume 5, Issue 3-2020, *International Journal of Innovative Science and Research Technology (IJISRT)*, PP-37-40. Available at SSRN: https://ssrn.com/abstract=3553550.
3. Wan Z., Liu J., & Deng R. H. (2012). HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, *7*(2).
4. Albugmi A., Alassafi M. O., Walters R., & Wills G. (2016). *Data Security in Cloud Computing*. Fifth International Conference on Future Generation Communication Technologies.