IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Securing Shared Data with Efficient User Revocation using OTP in Cloud

[1] Pranoti Kulkarni; [2] Dipa Dharmadhikari

[1] Computer Science and Engineering, Dr. BAMU, MIT
Aurangabad, Maharashtra, India

[2] Computer Science and Engineering, Dr. BAMU, MIT
Aurangabad, Maharashtra, India

Abstract - Need for storing large amount of data in the cloud is increasing day by day. So, this makes securing data in the cloud more important. Several methods used to sign each block present in the cloud and user had to sign each block for getting access to the data from the cloud. For some security and privacy issues, when a user leaves the cloud or misbehaves in cloud, the respective user must be revoked from the cloud. So, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid in the cloud. Therefore, although the content of the data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be signed again by an existing user in the group. Again signing each block is very tedious task to be done. So, to overcome the above disadvantages a new concept of one time password is to be used here so as to protect the files that are been stored in the cloud. Any user, either new or already registered user, he/she will have to login to the system first. Another new algorithm namely AROcrypt encryption method is to be implemented in this system. Also one more encryption technique as Rijndael technique is also implemented so as to provide better security for the data stored in cloud.

Keywords - *Cloud Computing, AROcrypt, Rijndael Technique, One Time Password*

1. Introduction

Technologies as cloud computing makes reference to both functions delivered with the benefits over the online network and the hardware and systems software in the data centres that provide those benefits. The services have been referred to as service that has been provided by the software. Three aspects that is been considered in cloud is as follows, first of all the confusion created by enormous computing assets accessible on requirement, thereby terminating the need for Cloud Computing users to plan far ahead for provisioning. Secondly, the closing of assignment by users, thereby giving association to start and develop hardware resources only when there is more required need for that respectively. And last but not the least, the ability to make use of computing resources on a short term analysis and remove them as needed, thereby rewarding conservation by providing machines and storage move when developers are no longer useful [1].

The main objective here is not only to validate the effectiveness of our approaches, but also show scrutiny system has a lower computation overhead, as well as a shorter extra storage for audit mete data. For efficiency, the communication and computation of the server and client during checking the protocol should be extremely smaller than sending or reading the data. Even though the server is only asked to use a few locations of its storage during a check, it must maintain full knowledge of all client data to be able to pass. The rapid use of net, cloud, social media *etc* has reduced the effectiveness of traditional security for data. An auditing methodology for data stored in the cloud for its privacy must be used. Today there are no broadly accepted practices that safeguard practice providers to ensure sufficient security. So, security is the main thing that must be achieved in Cloud respectively.

2. Literature Survey

Several methods and algorithms were used so as to improve security in cloud as follows. Several schemes were proposed to realize efficient and secure data integrity in cloud such as vector commitment, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data & encryption techniques was also implemented.

2.1 Proxy Re-encryption Schemes

Here, a data owner encrypts shared data in cloud with an encryption key, which is further encrypted and transformed by cloud, and then distributed to legitimate recipients in accordance with access control. Uniquely, the cloud-based transformation leverages re-encryption keys derived from private key of data owner and public key, and eradicates the key security problem in integrity based cryptography and the need of certificate. While preserving data and key privacy from semi-trusted cloud, this authorizes maximal cloud assets to reduce the computing and communication cost for data owner [2].

2.2 Dynamic Audit Services

Here, check service is constructed based on the techniques, as fragment structure, index hashing and random structure supporting provable updates to expand data. Also a method based on regular verification is introduced here for performance improvement [3]. It requires less storage for audit metadata.

2.3 Privacy Preserving Mechanism

This is a privacy preserving methodology to check the integrity of shared data. Here, group signatures are constructed so that the third party auditor is able to verify the integrity of shared data for users without retrieving the entire data [4].

Efficiency is not affected by number of users in the group. Group signatures to compute verification information on shared data

2.4 Dynamic Proofs of Retrievability

Here, it allows a client to store her data on a remote server and periodically execute an efficient audit protocol to analyze that all of the information is being maintained correctly and can be retrieved from the server so as to maintain the latest version of user data [5]. At any point in time, the client can execute an adequate audit protocol to ensure that the server advances the latest version of the client data. The main difficulty is to prevent the server from identifying and deleting too many codeword symbols belonging to any single data block.

2.5 Methods for Reliable and Efficient Distributed Storage

The equivalence between the edge-coloured graph model and degree-one-and-two encoding symbols based array codes is introduced.

Using this equivalence result, in general array codes using graph based results is designed. Similarly, based on this equivalence result, a new result for edge-coloured graph models using results from array codes is introduced [6].

2.6 Divertible Protocols

Here, the notion of divertability as a protocol property as opposed to the existing notion as a language property is introduced. Atomic proxy cryptography, in which an atomic executor function, in association with a public executor key, converts cipher texts (messages or signatures) for one key into cipher texts for another is also introduced [7]. First solution is provided proofs of retrievability for dynamic storage, where the client can perform arbitrary reads/writes on any location within her data by running an adequate protocol with the server.

3. System Development

We have studied about the previous methods implemented so as to obtain security in the cloud network. But we have also seen some disadvantages that are present in the above given methodologies. One of them was re-signing each and every file is very tedious and time consuming which is overcome here in this proposed system. Firstly, we will see how the flow of this system is going to be. To provide security, a new concept of OTP is going to be introduced in this system. Any user, either new or already registered user, he/she will have to login to the system first. And after entering its respective user id and password, user enters on a new page where for secure login OTP will be sent to his email id. After entering the correct OTP, he/she will be able to login to the system and use the files in the cloud. Another new algorithm namely AROcrypt encryption method is to be implemented in this system.

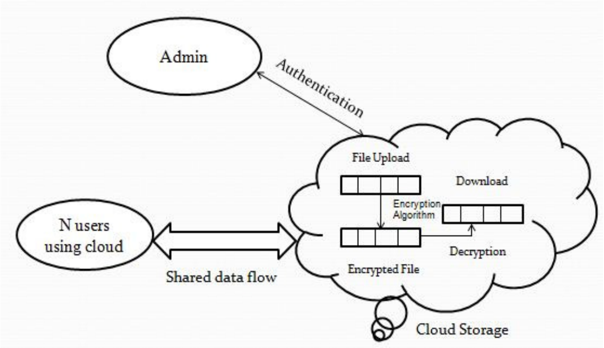

Fig 1: Proposed System Architecture

For OTP, random number generation algorithm is used which is explained further. New user will register him first then logs in to the system by entering login details. After that another login page is provided where login is done via OTP which is sent to the user’s email id respectively. Now here after inputting correct OTP provided to the user’s email, user enters to the system where he can upload files, view files and download files respectively. After user uploads file, that uploaded file is stored in the cloud in encrypted format where here AROcrypt encryption technique is used. User can view his files and other user's file. He can download other files only when admin give him access to do so. Foe that user have to send request to the file he has to download to the administrator.

3.1 AROcrypt Encryption Technique:

In this technique, following is the algorithm that is carried out:

1. Input text (t)
2. Convert text into ASCII code
3. N= Count(t) which is converted into ASCII
4. Store it in a square matrix and divide that matrix into three sub parts as upper matrix, lower matrix and diagonal matrix respectively.
5. Now consider three keys as k1, k2 and k3 and assign some values to it.
6. Add k1 to upper matrix, k2 to diagonal matrix and k3 to lower matrix respectively.
7. Now, again make these three matrixes into one single matrix and convert this ASCII values into character where we get out encrypted text.

This technique is used to hide sensitive data from the data that we store in cloud. This is simple but effective encryption technique so as to gain and maintain confidentiality of the data we store.

3.2 Rijndael Encryption Technique:

This is another technique that is used for encrypting and decrypting data. This technique is used to gain resistance again known attacks. Four main steps are carried out here in this technique as follows:

1. Byte sub transformation where each byte of block is replaced by its substitute in an S-box.
2. Shift row transformation, where each row of state is shifted cyclically in a certain number of steps.
3. Mix columns transformations, where state columns are treated as polynomials over GF(2^8).
4. And finally, round key addition where XOR round key is done with state.

4. Performance Analysis

4.1 File Size

File size is the parameter for performance evaluation. Different sizes of files are taken under consideration which is calculated after uploading file.

Table 1: Uploading time for different file types and sizes

File type	Actual Size	Size after encrypting & uploading	Upload Time (In sec)
Text File	100 Bytes	150 Bytes	1
	100 KB	150 KB	4
	10 MB	30 MB	20
Document File	100 Bytes	150 Bytes	3
	100 KB	150 KB	10
	10 MB	30 MB	22

For file download:

Table 2: Downloading time for different file types and sizes

File type	Actual Size	Size after decrypting & downloading	Download Time (In sec)
Text File	100 Bytes	100 Bytes	2
	100 KB	100 KB	5
	10 MB	10 MB	12
Document File	100 Bytes	104 Bytes	2
	100 KB	110 KB	6
	10 MB	15 MB	12

4.2 Encryption Techniques and its Comparison:

Table 3: Encryption techniques comparison

Size (Text Files)	Encryption Types (Time in ms)	
	Rijndael	AROcrypt
1 MB	399	282
2 MB	607	468
3 MB	895	656
5MB	1208	1102
10 MB	2429	2253

4.3 Decryption Techniques and its Comparison:

Table 4: Decryption techniques comparison

Size (Text Files)	Decryption Types (Time in ms)	
	Rijndael	AROcrypt
1 MB	310	235
2 MB	590	438
3 MB	830	627
5MB	1165	1069
10 MB	3510	3341

As we can see in table above, AROcrypt technique is the most efficient technique to be used, as it takes less encryption and decryption time respectively.

5. Conclusion and Future Enhancement

Several methods which were studied and implemented had various improved mechanisms that were implemented but also had a few drawbacks such as resigning each block was a tedious job. It worked on semi trusted servers & reducing average workload was extremely difficult. So, here a new security mechanism of using one time password for providing security is to be implemented in this paper respectively. Cloud computing provides efficient storage setting to store and retrieve the cloud user's data. Ensuring data security is a vital role to cloud users as well as cloud providers. . Recommended security benefits processes the data and then data is acknowledged to the cloud storage. Data encryption is done by choosing AROcrypt security service algorithm and Rijndael technique. It also describes Security as a Service in cloud environment. It also ensure security and confidentiality of data stored in the cloud. These techniques works on text and document files, so the future scope would be that encryption can be applied on other file formats too.

References

[1] X. Wu, L. Xu and X. Zhang, "CL-PRE: A Certificate less Proxy Re encryption Scheme for Secure Data Sharing with Public Cloud," Proc. Seventh ACM Symp Information, Computer and Communication Security, pp. 87-88, 2012.

[2] A. Fox, R. Griffith, A.D. Joseph, M. Armbrust, R.H. Katz, A. Rabkin, I. Stoica, A. Konwinski, J. Lee and M. Zaharia, "A view of Cloud computing," Communication ACM, vol 53, pp.50-58, 2010.

[3] A. Kupco, D. Wichs, D. Cash "Dynamic proofs of retrievability via Oblivious RAM," Proc Theory and Applications of Cryptographic Techniques, pp. 279-295, 2013.

[4] M. Strauss, G. Bleumer, M. Blaze, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Intl Conf. Theory and application of cryptographic techniques, pp. 127-144, 1998.

[5] H. Wang, G.J. Ahn, Y. Zhu, H. Hu, S.S. Yau, "Dynamic Audit services for integrity verification of outsorced storages in cloud," Proc. ACM Symp Applied computing, pp. 1550-1557, 2011.

[6] H. Li, B. Wang, B. Li, "Knox, A Privacy preserving auditing for shared data with large groups in cloud," Proc. Applied cryptography and network security, pp. 507-525, 2012.

[7] S. Yu, W. Lou, N. Cao, Y.T. Hou, Z. Yang, "LT Codes based secure and reliable cloud storage service," Proc. IEEE Infocom, pp. 693-701, 2012.

[8] L.V. Mancini, G. Ateniese, R.D. Pietro, G. Tsudik, "Scalable and efficient provable data possesion," Proc Security and privacy in Communication. Networks, pp. 65, 2008.