# Review Paper On Achieving Secure And Fine Grained Data Access Control In Unreliable Cloud

**Saurabh Upankar[1], Sarika Bongade[2]**

*[1]PG Scholar (M .Tech) Department of CSE, [2]Asst. Professor Department of CSE*

***Abstract - Cloud computing is the innovative research area because it is the resolution for next generation. One amongst the issue in cloud computing is information security. The data owner stores encrypted information on cloud and issues decryption keys to approved users.. Re-encryption prevents the left user to decrypting the information by using the previous decryption key and to get new decryption key to valid or approved user solely. Thus only approved user will continue to access the information. By considering cloud design, such command could not be received properly as a result of unsecured network communications. once user is revoked, data owner as to re-encrypt the information in order that revoked user cannot access the information again .To perform this operation he can issue re-encryption command to cloud in order that information in cloud gets re-encrypted. Once re-encryption is finished there's a need for generation of new decryption keys to valid user, so that they will still access the information. During a cloud computing atmosphere all such commands might not be received and executed by all of the cloud servers as a result of unreliable network communications. To resolve this drawback, we are proposing time-based re-encryption scheme. During this scheme automatic re-encryption of information can takes place based on the internal clock value present at the cloud server. To perform this automatic re-encryption we'll make use of encoding technique referred to as Attribute based encryption (ABE) with DES (Data encryption Standard) and Base64 encoding. ABE gives fine –grain access management and easier user revoking system and DES and Base64 can provide encryption technique.***

***Keywords - Cloud computing, Attribute based encryption, Re-encryption.***

## 1. INTRODUCTION

Cloud computing is a technology that delivers several varieties of resources as services, chiefly over the web. It's become a viable business and technological proposition due to the numerous reduction in each infrastructure and operational prices that it offers in comparison to ancient IT services. Data owner's having large quantity of data can outsource their data to third party who has massive storage capability referred to as "cloud Service providers " (CSP) due to drawback of storage capability , cost concerned in storing information with them etc. Cloud Service provider could be a one who offers storage and process services to information. Before outsourcing information to CSP's the information owner should rely on the protection issue associated with his information thus he can encrypt the information before outsourcing data. When associate encrypted information is stored and decryption keys allotted to user they will access information from cloud however what's the case once explicit user is revoked? Once a user is revoked and he has decryption key he can access information still, therefore to overcome from this drawback there's a desire of immediate re-encryption information by data owner. As shortly as re-encryption is completed the new generated decryption keys are distributed to approve users. This resolution can result in a performance bottleneck, particularly once there are frequent user revocations. To perform this encryption we will make use of encryption scheme known as "Attribute based Encryption" scheme that provides fine-grained access management.

## 2. SYSTEM MODEL

We used a reliable re-encryption scheme in un-trusted cloud (R3 scheme for short). [6] R3 is a Time-based re-encryption technique, which allows each and every cloud server to automatically re-encrypt data based on its internal clock. Data user will only get access to that data in a particular time slot. Then time slot gets over so cloud server will automatically re-encrypt the data. Cloud server will check whether requesting user is allowed to access the data on this time slot or not. If the time slot doesn't match, cloud server will not allow data user to access that particular data. The proposed system is work on the process of Re-encryption for provide data security. We are work on cloud data is encrypted and decrypted on time based automatically. This is an automatic time based re-encryption scheme [6], in which each cloud server to automatically re-encrypted data based on their internal clock. This scheme is to associate data with an access control and an access time. Each valid user is issued key associated with attribute and attribute effective times.

The valid user using the key data is decrypted with attributes satisfying the access control and attribute effective times satisfying the access time. The command driven re-encryption scheme, the data owner and this share a secret key, with each cloud servers can re-encrypt data by uploading the access time according to their own internal clock. It does not require perfect clock synchronization among cloud servers.

An alternative solution is to use the proxy re-encryption (PRE) technique. This approach takes advantage of the extensive resources in a cloud by authorization the cloud to re encrypt information. This approach is additionally referred to as command driven re-encryption theme, wherever cloud servers execute re encryption whereas receiving commands from the data owner.

However, command-driven re-encryption schemes don't take into account the underlying system design of the cloud environment. A cloud is actually an oversized scale distributed system wherever an information owner's data is replicated over multiple servers for high convenience. As a distributed system, the cloud can experience failures common to such systems, like server crashes and network outages. As a result, re-encryption commands sent by the information owner might not propagate to all or any of the servers in an exceedingly timely fashion, therefore creating security risks.

Let us take into account a cloud environment shown in Figure, wherever the information owner's data is keep on cloud servers CS1, CS2, CS3, and CS4. Assume that the information owner issues to CS4 a re- encryption command, which ought to be propagated to CS1, CS2, and CS3. Because of a network drawback, CS2 failed to receive the command, and failed to re-encrypt the information. At this point, if revoked users query CS2, they'll get the previous cipher text, and may decrypt it using their previous keys. A stronger solution is to permit every cloud server to severally re-encrypt data while not receiving any command from the information owner.

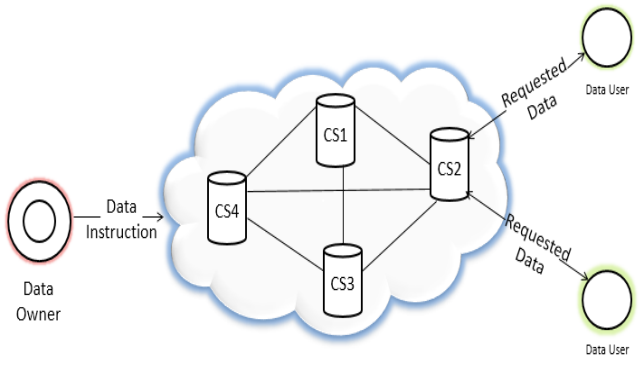


Fig-1. A Typical cloud environment.

The projected a time –based reliable re-encryption scheme that permits every cloud server to automatically re-encrypt information based on its internal clock.

## 3. PREVIOUS WORK

[1], proposed a brand new methodology for managing access control on the information being keep on the cloud server, based on the cloud server's internal clock. The technique doesn't rely on the cloud service provider to dependably propagate re-encryption commands to any or all servers to confirm access control correctness. They showed that the solutions stay secure and it's strong enough without perfect clock synchronization that depicts the cloud behavior as long as will bound the time difference between the servers and also the information owner.

The paper [2] proposed an efficient information retrieval scheme using attribute-based encryption. The proposed scheme is best fitted to cloud storage systems with substantial quantity of information. It provides rich quality as regards access control and quick searches with easy comparisons of searching entities. The proposed scheme additionally guarantees information security end-user privacy throughout the information retrieval process. A key approach to secure cloud computing is for the information owner to store encrypted data within the cloud, and issue decryption keys to approved users.

The paper. [3] Deals with the information Security. In this paper the DES algorithm is optimized up to 4 round using Xilinx software and implemented on Spartan 3 Modalism. The paper deals with numerous parameters like variable key length, key generation mechanism, etc. employed in order to provide optimized results.

The paper. [4] Proposed a new type of Identity-Based encryption (IBE) scheme that are known as Fuzzy Identity-Based encryption. In Fuzzy IBE an identity is viewed as a set of descriptive attributes. A Fuzzy IBE scheme may be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is exactly what permits for the use of biometric identities that inherently can have some noise whenever they are sampled. To boot, the Fuzzy-IBE are often used for a sort of application which will be termed as "attribute-based encryption".

The paper [5] proposed economical data accessing technique that permits the information owner to delegate most of the computation tasks concerned in fine- grained data access control to untrusted cloud servers without revealing the underlying data contents.

## 4. PROPOSED METHODOLOGY

The proposed system is work on the method of Re-encryption for provide information security. We are work on cloud information is encrypted and decrypted on time based automatically. This is an automatic time based re-encryption scheme, during which every cloud server to automatically re-encrypted information based on their internal clock. This scheme is to associate information with

an access control and a time interval. Every valid user is issued key related to attribute and attribute effective times. The valid user using the key information is decrypted with attributes satisfying the access control and attribute effective times satisfying the time interval.

A cloud computing environment consisting of a data owner, a cloud service provider (CSP) and multiple data users. [1]The data owner outsources his data in the form of a set of files F1……Fn to the CSP. Each file is encrypted by the data owner before uploading to the CSP. Data users that want to access a particular file must first obtain the necessary keys from the data owner in order to decrypt the file. The data owner can also update the contents of a file after uploading it to the CSP. This is termed a write command. Each file, F, is encrypted with two parameters, time slice and attributes. The time is divided into time slices, and every time slice is of equal length. A particular time slice is denoted as, TS, with a subscript, where TSi = (ti; ti+1).

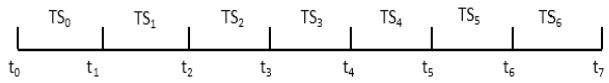


Fig.2. Sample time slice.

A data user, after being authenticated by the data owner, is granted a set of keys, each of which is associated with an attribute and an effective time that denotes the length of time the user is authorized to possess the attributes. . For example, if Alice is authorized to possess attributes a1…am from TS1 to TSn, she will be issued keys as is shown in Fig.3[1].

| Key | Description |
|---|---|
| $SK^1_{a1}$ | Keys for attributes $a_1$ for $TS_1$ |
| ..... | |
| $SK^1_{am}$ | Keys for attributes $a_m$ for $TS_1$ |
| ..... | |
| $Sk^n_{a1}$ | Keys for attributes $a_1$ for $TS_n$ |
| ..... | |
| $SK^n_{am}$ | Keys for attributes $a_m$ for $TS_n$ |

Fig.3. Alice key

*A. Attribute based encryption (ABE):*

Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes [7]. In which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is crucial security feature of Attribute-Based Encryption .An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

ABE is a new cryptographic technique [6]. It allows data to be encrypted using an access structure comprised attributes are different. Then specific decryption keys for specific files, data users are issued attribute keys. Data users must have the necessary attributes that satisfy the access structure in order to decrypt a file. For example, file encrypted using access structure {(a1 and a2) or a3)} means that either a user with attribute a1 and a2, or user with attribute a3, can decrypt the file. An alternative solution is applied to the proxy re-encryption technique [6]. This is also called as command driven re-encryption scheme as the re-encryption is performed by the servers in the cloud computing environment while receiving commands from the owner of the data.

The main goal of design is to achieve data security in cloud computing. So, we categorize our goal into the following:

*Fine Gained Access Control:* The data owner can specify expressive access structure for each and every data.

*Data Consistency:* This requires that all authorized data users who request for file F, should obtain the same content in the same time slice.

*Data Confidentiality:* The Cloud Service Provider (CSP) and malicious user cannot recover data without the data owner's permission.

*Cost Efficiency:* The re-encryption cost on the CSP (cloud service provider) is relatively low.

## 5. CONCLUSION

The technique does not rely on the cloud service provider to reliably propagate re encryption commands to all servers to ensure access control correctness. Thus, the data owner can be offline in the process of user revocations. Data user can access to the particular amount of data which is decided by the data owner. This scheme allows each user's access right to be effective in a very pre-determined amount of time, and enable the CSP to re-encrypt cipher texts automatically, based on its own time. Thus, the information owner may be offline within the process of user revocations. Knowledge user will access to the actual quantity of information that is decided by the information

owner. Our solution remains secure in several attacks due to instant re-encryption. So that, each time attacker can face new combination of cipher-text.

## 6. FUTURE SCOPES

The future enhancement to this project is that when data user request for a file if he is valid user then for easy access, the OTP is sent to the valid data user mobile number as text message.

## REFERENCES

[1] Loknath S, Shivamurthy S, Bhaskar S and Shantgouda S, "Strong and secure re-encryption technique to protect data access by revoked users in cloud," International Conference on Advances in Computer and Electrical Engineering (ICACEE'2012) Nov. 17-18, 2012 Manila (Philippines).

[2] M.Srujana* S.Satya Narayana Y.Divya M.Girvani, "Reliable proxy re-encryption in unreliable clouds," International Journal of Advanced Research in Computer Science and Software Engineering, March 2013.

[3] Nimmi Gupta, "Implementation of Optimized DES Encryption," ISSN 2249-6343 International Journal of Computer Technology and Electronics Engineering (IJCTEE) 2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT, 2005.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and Fine grained data access control in cloud computing," in Proc. of IEEE INFOCOM, 2010.

[6] Ajinkya Adhau, Payal Bobade, Priyanka Zilpe, Yashodhara Fulmali "Data security using Reliable re-encryption in unreliable cloud" International Journal of Computer Science and Network (IJCSN), April 2015.

[7] Minu George, Dr. C.Suresh Gnanadhas, Saranya.K "A survey on attribute based encryption in cloud computing "International Journal of Advanced Research in Computer and Communication Engineering, November 2013.

[8] P. Ramanathan, K. Shin, and R. Butler, "Fault-tolerant clock synchronization in distributed systems," Computer, 2002.

[9] N. Antonopoulos and L. Gillam, "Cloud Computing: Principles, Systems and Applications," Springer Publishing Company, 2010.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. of USENIX FAST, 2003.

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, 2006.

[12] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," Communications of the ACM, 2010.

[13] F. Cristian, "Probabilistic clock synchronization," Distributed Computing, 1989.

[14] K. Romer, "Time synchronization in ad hoc networks," in Proc. of ACM MobiHoc, 2001.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. of IEEE Symposium on S&P, 2007.

[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology EUROCRYPT, 1998.

[17] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. Of ACM CCS (Poster), 2010.

[18] Ritesh B. Tandel and Krishnakant Kishor, "Review Paper on Data Security For Unreliable Clouds Using Reliable Encryption" International Journal for Innovative Research in Science & Technology, December 2014.

[19] Shyam Sarania and Amit Gupta "Secure Re-encryption in Unreliable Cloud using Synchronous clock," International Journal of Advanced Research in Computer Engineering & Technology, August 2013.

[20] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

## AUTHOR'S PROFILE

**Saurabh Upankar** has received his Bachelor of Engineering degree in Information Technology from RGCER Engineering College, Nagpur in the year 2014. At present he is pursuing M.Tech. with the specialization of Cloud Computing in RGCER Engineering College.

**Sarika Bongade a**t present she is working as an Associate Professor at RGCER Engineering College, Nagpur. Her areas of interests are Cloud Computing and Distributed System.