

SECURE RE-ENCRYPTION IN UNRELIABLE CLOUD USING SYNCHRONOUS CLOCK

Arudra Gopala Rao¹, Sk. Nagul²

¹M.Tech (CSE) Scholar, ²Assistant Professor

Nalanda Institute of Technology (NIT), Siddharth Nagar, Guntur A.P, (India)

ABSTRACT

Main aspect of cloud computing is data security and provide the sensitive awareness about the information which was store in cloud. Because some of the situations cloud will face an attack from the malicious user, it's an attack of inside the cloud server and through this storage process may fail in cloud. To overcome this became a challenging task to the organizations. So for that reason we are implemented this paperto maintain the high level security in cloud. In general data owner will store there information without modification, but before uploading in cloud we are encrypting thefile with an attribute based encryption algorithm based on user provided data attributes and its time functionality. That time cloud will generate a key for the decryption it will send to the data owner by using mail authentication. So here we are encrypting the data or the file two times with different levels of security providing. Because cloud is maintain multi servers, that all the information will not revile to the other users in the network because its intention is to provide the security in cloud. So based on specified time intervals it will re- encrypt the data and it will create a security keyword for that updated file in cloud server. Whenever the data has modified in cloud it will send a security keyto authenticated use by the mail authentication scheme. By that key only data owner can decrypt the file and he can access that file at anytime.

Keywords: Security, Re-Encryption, Cloud Server Point, Data Owner and Chipper Text.

I. INTRODUCTION

Cloud computing is for the security purpose and to deliver different kinds of services to the cloud users. And to maintain huge information in distributed systems and to provide services for the different kinds self-governed steps in the computers. To store large amount of data in distribution system we most proffer distributed systems, but sometimes it creates some of the problems, so to overcome these problems we are taking cloud computing support for the transaction of data. We have different types of network connections and it will provide online services to the organizations. Cloud means online available server at anytime, it simplifies the complexity of data transference in between the servers. Cloud computing is an easy available service at anytime and anywhere. If user has the internet connection he can access cloud at anywhere. To share large amount of data in online user needs cloud supportto send information to the other system. That means its providing the backup to online transferring data from system to system. Like all the information which was uploaded and there is a process of storing encryption keys in cloud and it stores in database when the permission of user has revoked in cloud still it provide the encryption key to the users in earlier system. So then after getting of key information he can access the data and he can download the files which were needed to him from cloud servers. There was a new proposal here to stop the guessing of keys in cloud when data owner has uploaded it will encrypt and

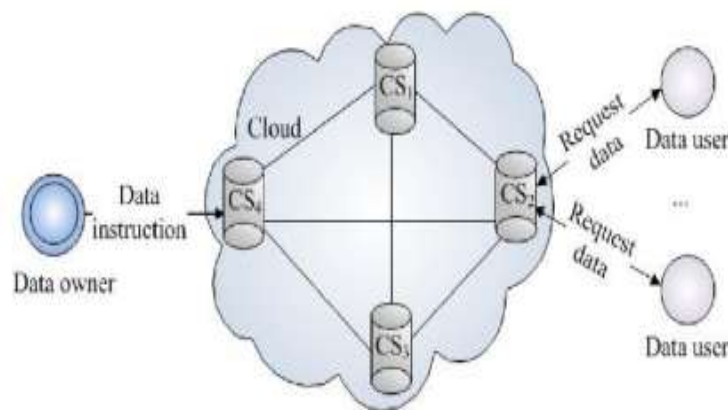


Fig 1. A typical cloud environment

Data storage in cloud is entirely different to other servers storage, if we store in our local servers we just store and keep with the security lock that's it. But if we want to store in cloud we that we have to encrypt that all the information with the help of Attribute Based Encryption (ABE) algorithm. To encrypt the uploaded information we are proposed ABE method, because whatever the data we are keeping in cloud may contains different types attributes and different types information. It will provide a key for each and every individual data files based on its attributes information. In general for each file there is different secured key. It doesn't specifically allocated key for files based on its information or type. To encrypt the file we need its structure that means attribute information with the users or its related data then it can be decrypt.

Here the alternative thing is to apply the proxy encryption process for the uploaded data in cloud systems. This will make an advantage in cloud to re encrypt the data dynamically whatever the data was received from the client and based on user command mode it will check. That means which was propagated and stored on the available clouds like if we have multi clouds means CS1 and CS2 like. In an existing process the data will be encrypt and it will contain only one secret key with that anyone can decrypt the key and they can view the data. For the better situation in cloud servers we are implemented another way cloud itself can encrypt the data automatically, that means without the intimation of data owner and his command request cloud will encrypt the data and it will generate another key for the re encrypted data. In un-trusted cloud for the security reasons we are implemented. Based on time intervals in the cloud system it was implemented. This method will allows all the cloud servers to perform the re encryption process which was uploaded by the users in un-trusted cloud servers. Theme of re-encryption in an outsourcing cloud is to maintain the data with an access control and in an acceptable time point. There is a secured key for each user it was issued based on their attributes and related to its time access. When user wants to decrypt the data he has to provide the key based on its attribute, then after it will check the time accessing based on that it will decrypt. Cloud is large amount of data collector, which can store in multiple servers and to maintain a large scale of distribute system services. In distributed system we will store the information of clients and as well as their related uploaded information in multi servers for high quality performance. With the distributed system there were some of failures to maintain a large amount of data, to overcome that re-encryption concept was implemented in the cloud.

II. RELATED WORK

In general data owners will store there in cloud servers for the security purpose like the cloud we have CS1 and CS2 etc. For an example if we have four cloud servers and which was the data uploaded by the users has a stored in multi servers, in the time of command passing data owner has passed his command to the cloud server it was getting by the fourth server, then after the data revocation from cloud the command was received by the cloud server two then it will send the old cheaper text to the user and he will decrypt that data with the provide key from the cloud. At that time this will be a problem to user if he gets the old cheaper text. So to avoid that problem in cloud servers we are implemented re- encryption process without receiving any command from the data owner when the file is uploaded on server it will automatically re encrypt the data which was there in the cloud server. This process will do on a bulk activity at a time to transfer data into cloud servers.

For this state we are implemented this reliable re-encryption process in an outsourcing cloud. It transfers to the cloud server based on time and based on activity. This will allow on each server to encrypt the data automatically without any request from the data owner. And it will be update on cloud and that information will store in secure manner and after that an automatic mailing process which can support by the cloud setting. Here for implementation of this task we have three ways they are the first one is data owner, second is cloud storage system and third one is customer portal by using of this three ways we are proposed this paper and with the help of cloud storage server we are encrypting the data files and its related information which was uploaded in cloud servers. With this three user modules and with these three steps we are implemented for an efficient response from the cloud server.

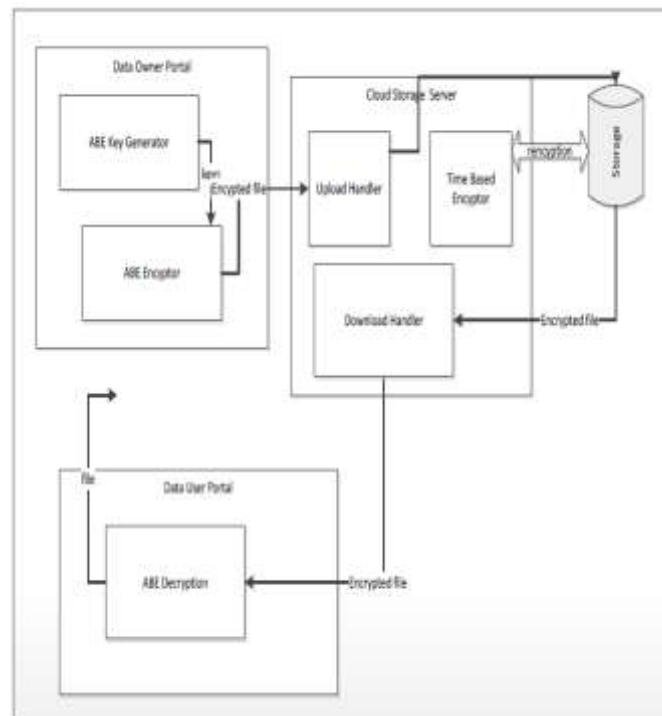


Fig2: Implementation of Cloud Process

We are having two typed of inner adversaries in cloud computing. Any one of un-authorised person can try to get the information from cloud server. To protect the cloud information we are provided a secure protocol which can provide the security for the transmission data in cloud servers. When we check this the both cloud server

and as well as the malicious users are involved in the process, so through this we can process for the further process of data in to a small proxy servers and will not allow any malicious users and cloud server provider to access and to transfer the information which was stored.

Here we have multiple numbers of users and cloud servers; data owner will upload different types files like F_1, F_2, \dots, F_m in cloud server point. Before uploading the file in cloud server it will be encrypt and then after it will be upload in cloud server. To decrypt that file user has to need the decryption key from the cloud server. Based on the user command which has send cloud server point from the data owner and each one of the encrypted file F will have two parameters they are the attribute and time interval. Here we performed slice operation on the files which was uploaded for each file there was an equal length of time period and its related intervals. So let's declare TS is time slice of the attribute. $TS_i = [t_i: t_{i+1}]$ attributes are in count number form and it was like an increasing number of 1,2 and 3. After satisfaction all the 3 conditions it will pass the command to the cloud server for the data encryption.

After completion of authentication verification in Time slice method it will arrange and assign key to the data owner based on attributes and based on time interval. Because some of the situations cloud will face an attack from the malicious user, it's an attack of inside the cloud server and through this storage process may fail in cloud. To overcome this became a challenging task to the organizations. So for that reason we are implemented this paper to maintain the high level security in cloud. In general data owner will store there information without modification, but before uploading in cloud we are encrypting the file with an attribute based encryption algorithm based on user provided data attributes and its time functionality. That time cloud will generate a key for the decryption it will send to the data owner by using mail authentication. So here we are encrypting the data or the file two times with different levels of security providing. Because cloud is maintain multi servers, that all the information will not revile to the other users in the network because its intention is to provide the security in cloud. So based on specified time intervals it will re- encrypt the data and it will create a security keyword for that updated file in cloud server. Whenever the data has modified in cloud it will send a security key to authenticated use by the mail authentication scheme. By that key only data owner can decrypt the file and he can access that file at anytime. Take an example of data owner has passed through the verification of time slicing TS then after the verification for that data owner there will be key will be allocated like TS_1 to decrypt the file. Based on data owners and uploaded files related to its attributes it will be allocate to each users.

III. RESULT

In this research we are proposed a strong encryption method to provide the security in cloud server point. Here without the involvement of third party authenticator we are implemented. Everything passing information or the command response from the server everything is an instance time period we are implemented.

Here cloud server has to register and the data owner has to register in this application after the registration completion he has will login with his authentication details. After the login user can upload files in cloud but here before uploading the file in cloud server we are encrypting the data and after that it will be uploading to the cloud server. After completion of encryption it will generate one security key to the users file and that key will be having with the data owner. After the encryption he has to upload that file in cloud server, cloud server will provide another security key and automatically without user request cloud server will decrypt the file then it will generate the security key for the file and it will send to the data owner by an email authentication process.

After the completion of data uploading whenever user want to download that file he has to give the secured key which was shared by cloud server to him. If user given valid details he can able to access his file otherwise the request processing will be fail in the server. After that cloud users who ever want to get files they has to send the key request to the data owner if data owner is willing to share that key to the cloud user he can share or else he can ignore the data. and to know the information. If cloud user get the key he can download the file like this we are implemented. In the middle if any attacker has tried to attack and get the file he can get only chipper text information only because it was re-encrypted. If anyone want to get that file he has to get the authentication key which was share to data owner and as well as the attribute time interval specification information in the time of file download. There was a security state from the hackers then user can be happy to that information without having any problem in cloud servers.



IV. CONCLUSION

Here we are focused on time interval to achieve the well increase access control. And to revoke the information from the cloud server point. We are implemented for the re-encryption process for the cloud server point. In existing process when user uploading any data in cloud server he will upload normal data without any modification. Here we are proposed a way of attribute based encryption based on the content and time intervals of the file before uploading in cloud we are encrypting the data. After the completion of encryption we are uploading that same file in cloud server when that file has transferred into cloud server without any intimation of data owner it will encrypt the file then it will store that file in cloud server point. Whenever user need he can send request to cloud server he will get the authentication key to his mail then he can download the file.

REFERENCES

- [1] S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, 2010.
- [2] 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.
- [3] Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT, 2005.
- [4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, 2006.
- [5] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. of IEEE Symposium on S&P, 2007.
- [6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.
- [7] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. of ACM CCS, 2008.
- [8] 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.

AUTHOR PROFILE

	<p>Arudra. Gopala Rao is currently pursuing M.Tech in the Department of Computer Science & Engineering, from Nalanda Institute of Technology (NIT), siddharth Nagar, Kantepudi (V), Sattenapalli (M), Guntur (D), Andhra Pradesh, Affiliated to JNTU-KAKINADA.</p>
	<p>Sk. NAGUL working as Assistant Professor at Nalanda Institute of Technology (NIT), siddharth Nagar, Kantepudi (V), Sattenapalli (M), Guntur (D), Andhra Pradesh, Affiliated to JNTU-KAKINADA.</p>