International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 6; November 2017; Page No. 1125-1127

Effective and secured dynamic key generation over cloud data

[1] K Raja, [2] Dr. R Sugumar
[1] Research Scholar, Department of Computer Science, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India
[2] Deputy Director & Research Supervisor, Department of Computer Science, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India

Abstract
Cloud storage security may take as some advantages and disadvantages too. Many companies and private sectors are providing cloud storage with low cost and allocate space according to their requirements. Meanwhile security lack still remains afraid for some users. In fact, everyday users overcome lot of security issues behind cloud data sharing. So they produce advert of high secure and sharing data. But still doubt remains for many clients. For that security purpose developers implemented cryptography concepts between the client and server. They made some key concepts for the encryption. It is the process of converting normal text to cipher text. For this convention we need key and for decrypt also. So developers should take more care of highly secured key and spires couldn't able to guess the key. In this paper we created dynamic key changes algorithm for the encryption. So the pirates cannot guess the key. Proposed can protect the data while transferring, sharing and storing in data centers using Dynamic key generation. It is the process of creating unique key changes when the user read their own data. The changes of key depend upon the user action. So it is very effective and secure transmission of data over cloud. This proposed process creates highly secure cloud data even any unknown person cannot guess the key. This paper mainly deals with the key management concepts and how it creates the dynamic key generation over cloud. It provides specific authentication to the user. Key takes major place to encrypt the files and process done by virtual because we cannot able to see the process of creating the key for encryption.

Keywords: cloud storage security, dynamic key, cloud data

1. Introduction
Cloud computing provides the service of flexible and convenient ways of data sharing for both the society and individuals. Since the user store their private and most valuable data's on the cloud. Although tends to some security issues over the cloud server data. Thus it is necessary to provide more secure for sending and receiving data. So the existing system produced authentication. However secure authentication may leak. So the hackers can easily hack the client data. For that purpose, it is necessary to place encryption and decryption throughout the cloud server. Thus the cloud developers need to create a specific key to do cryptic data. Moreover all encryption techniques are lacking security somewhere through the constant key generation [1]. To this issue, we propose a dynamic key generation for both encryption and decryption. The key generation full and fully depends upon the user actions. The server allows user through the authentication process. Key management concept is given below to know the purpose of key and making reliable secure data. These processes fully occur at the server side.

1.2 The Need for Key Management in the Cloud
Key management is the main part of encryption. It is the process of accepting valid key for both encryption and decryption and also deals with updating, deletion, new and storage of key. Many cloud service providers provide some keys to the user to encrypt their data. So the handling of key is necessity and need more care [2]. This key provides the data more secure and does not lead any kind of piracy and leakage of data. Key management helps the cloud server for more secure encryption. Cloud providers should convince all the category of key management. So they can enlarge the confidential between the client and their services. Some requirements are needed for effective key management. Some important requirements are given below.

- **Secure key storage:** Key must be store in a specific protected place without knowing others for the hackers tends to know the key, and then the system will collapse and easily access all the data from the server. So the key storage must be safe and dynamically changes to the user.
- **Accessing key storage**: Accessing of key is not easy thing. It provides some authentication to verify the access of key and they provide some limitation. The key can be allowance for certain category and depends on the position can able to control over the key.
- **Recovering of key:** Key must need secure recover and backup. So that virtualized backup storage is more secure and malicious user cannot find the key. Cloud providers should ensure of key backup remains or have any loss.

2. Architecture

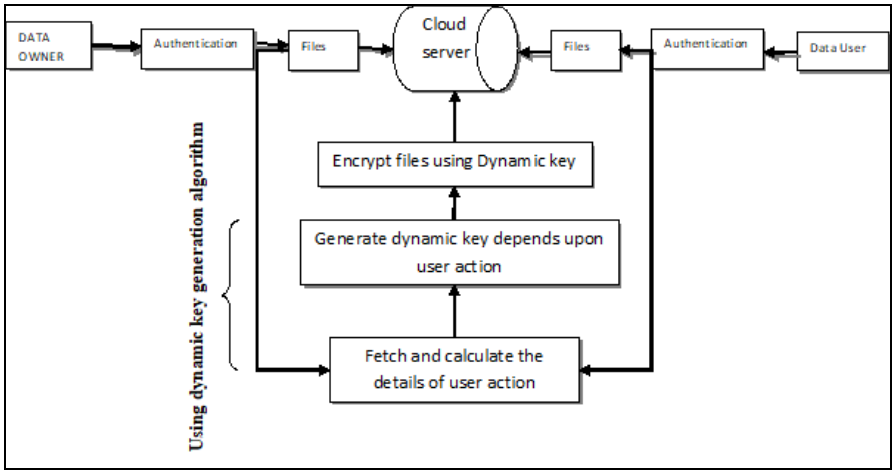

Fig 1

Above architecture describes each process of the proposed system. It depicts how the system does work and their each module. Each module has specific task. Data owner is the part of this system. They purposefully use the cloud server. Data owner cannot directly store the data to the server. Because the system it generate authentication to the owner due to false user. Through the valid verification files will moves to the cloud server. It contains several documents and sometimes works as workstation. This server mainly used for storage purpose. The proposed system mainly aims to provide highly secured data to their clients. The cloud server will deny the transmission process without proper authentication.

Specific purpose of this system is to generate dynamic keyword for both encryption and decryption to the clients [3]. It is symmetric key generation have some possibilities to assume the keyword. So this system produce dynamic key and send that key to data user. Without the key user cannot access the data from server. It provides more security than existing system.

3. Flow Chart

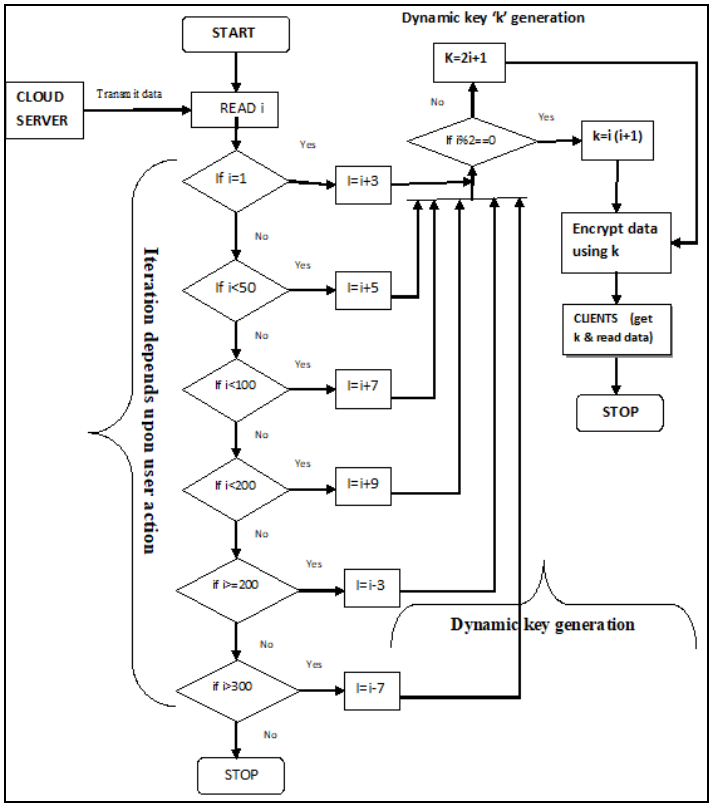

Fig 2

Above flow chart describes whole system of the proposed methods. It is the diagrammatic representation to the user's easy understanding to make sure the purpose of this system. It describes the relationship between the client and server. The main purpose of this system is to generate dynamic key for both encrypt and decrypt the data. This flow chart describes the encryption and key generation. The first process is to send data from server. Meanwhile it uses the logic of dynamic key changes. It is used in between the client read of data from the server. Key generation depends upon the user action. Firstly, client request data from server then it will send to client [4]. So the client will read the data. At the same time sensor will read and count the user read line. Based on the sensor counting it will add some specific odd numbers to it. Then the results will take as key. That key does not exist the same number. So it makes more advantages to this algorithm. From the resulted value it will act as a key to encrypt [6]. Through the key client can able to encrypt the data. Simultaneously process will continue until the user complete sending and receiving data from the cloud server. This process is more secure because of the dynamic key generation.

3.1 Dynamic Key Generation Algorithm

Step 1: Read **i** (updating process of 'i' depends upon client viewed data lines).
Step 2: verify (i mod k) =0.
Step 3: if (i mod k) =0, then calculate k =i (i+1).
Step 4: if (i mod k) ≠0, then calculate k =2i+1.
Step 5: encrypt all sending data using dynamic key k.
Step 6: client get 'k' through authentication and decrypt the data using k through appropriate application.

4. Performance Measure

The performance measure depicts the comparison between existing and proposed system. The major parameters of this measure are key strength and how many key changing. It will be useful for both encryption and decryption. Based on this parameter, below Fig 3 shows the effectiveness and high security of the proposed system.

In the existing system, changes in key are very low. It changes the key for only one time. Sometimes two or three but it's very rare. But in this proposed, it will generate the key dynamically. Each time the user should know about the key and it is based on user action. So it leads to high secure data.

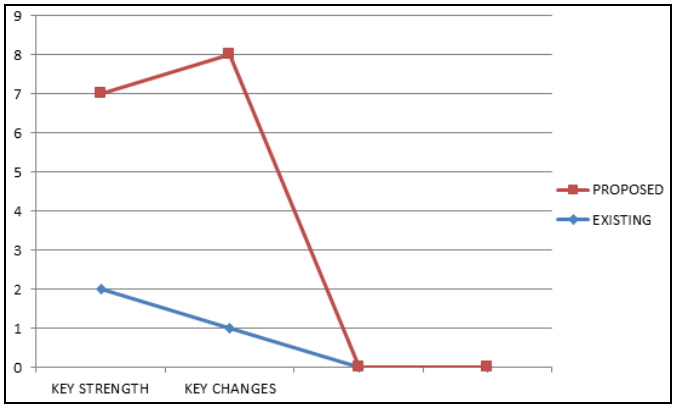

Fig 3

5. Conclusion

In this paper discussed about cloud server data transmission process and key generation for both encryption and decryption. It describes the importance of key management. Through this dynamic keyword generation data will secure and effective transmission. In existing system, propose only a constant keyword changes and symmetric algorithm. But in this proposed system, each time algorithm creates unique keyword to the user. The anti user cannot misuse the data. The keyword does not exist the same from previous. In future, dynamic key generation will be applicable for the cloud application also.

6. References

1. Xia, Zhihua, Xinhui Wang, Xingming Sun, Qian Wang. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems. 2016; 27(2):340-352.
2. Fu, Zhangjie, Xingming Sun, Qi Liu, Lu Zhou, Jiangang Shu. Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing. IEICE Transactions on Communications. 2015; 98(1):190-200.
3. Li, Ruixuan, Zhiyong Xu, Wanshang Kang, Kin Choong Yow, Cheng-Zhong Xu. Efficient multi-keyword ranked query over encrypted data in cloud computing. Future Generation Computer Systems. 2014; 30:179-190.
4. Vaquero, Luis M., Luis Rodero-Merino, Rajkumar Buyya. Dynamically scaling applications in the cloud. ACM SIGCOMM Computer Communication Review. 2011; 41(1):45-52.
5. Li, Hongwei, Yuanshun Dai, Ling Tian, Haomiao Yang. Identity-based authentication for cloud computing. Cloud computing, 2009, 157-166.
6. Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption. In Proceedings of the 2012 ACM conference on Computer and communications security, 2012, 965-976.
7. Bhardwaj, Sushil, Leena Jain, Sandeep Jain. Cloud computing: A study of infrastructure as a service IAAS. International Journal of engineering and information Technology. 2010; 2(1):60-63.
8. Che, Jianhua, Yamin Duan, Tao Zhang, Jie Fan. Study on the security models and strategies of cloud computing. Procedia Engineering, 2011; 23:586-593.