ISSN 2395-1621

A Secured Approach for Multi Keyword Ranked Search Over Encrypted Cloud Data

[#1]Vijay Bharkade, [#2]Sainath Bharkade, [#3]Abhilash Pawar, [#4]Rohit Agrawal

[1]vijaybharkade123@gmail.com
[2]saibharkade123@gmail.com
[3]pawar.abhilash598@gmail.com
[4]rohitagrawal008@gmail.com

[#1234]Padmabhooshan Vasantdada Patil Institute of Technology, Bavdhan Pune

ABSTRACT

In now a days due to increasing demand and popularity of cloud computing more and more data owners are getting attracted towards it and outsourcing their data to the cloud servers due to great convenience and reduce cost in data management. Before outsourcing the sensitive data the data needs protection and security like encryption to the data. In which the utilization is like keyword-based retrieval.In this paper we are going to present secure multi keyword ranked search over encrypted cloud data, which support dynamic operations like deletion and insertion of documents. In this we are trying to provide security sensitive data using AES encryption algorithm.Due to this technique users can retrieve the data using our provided description key hence an authorize user can access the data easily from cloud server with security.

ARTICLE INFO

Article History

Received :8th March 2016

Received in revised form :

10th March 2016

Accepted : 12th March 2016

Published online :

14th March 2016

Keyword:- cloud computing, encryption, decryption, multi-keyword search, ranked search.

I. INTRODUCTION

Cloud computing is a popular technology which is used in IT infrastructure. Using this technology we reduce the cost of hardware and give great flexibility for shared network using shared pool. By attracting towards this technology enterprises are outsourcing their data to the cloud. Cloud customer can remotely store their data into cloud on demand using shared pool then can access data.Due to various advantages of cloud services, users are outsourcing sensitive information such as e-mail, personal health record, company finance data, government documents, etc. The cloud service provider (CSP) provides security to data so that user may access sensitive information with authorization. Cloud service provider provides security using encryption and decryption keys. When users wants to outsource there data at that time cloud service provider store the data in encryption form. If user wants to access their outsourced data at that time cloud service provider provides decryption key to authorized user. using decryption key authorized users can access data.In this paper we provide security over the encrypted cloud data, which support multi keyword ranked search and dynamic operation on collection of documents. We also provide security on data storing and accessing time using one time password (OTP).

II. ALGORITHM

AES ALGORITHM:

KeyExpansions:

round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

InitialRound:

AddRoundKey: each byte of the state is combined with a block of the round key using bitwise xor.

Rounds :

it consists of following operation

Sub Bytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

Mix Columns: a mixing operation, which operates on the columns of the state, combining the four bytes in each column.
AddRoundKey

Final Round (no MixColumns)
Sub Bytes
Shift Rows
AddRoundKey.
10 cycles of repetition for 128-bit keys is performed here.

III.EXISTING SYSTEM

In the previous paper they used the RSA algorithm for the encryption, which was not providing good flexibility and security, and again there is less security provided for sign up and sign in new users. So due to this anyone can access there outsourced data using their username and password so its not good security provided by cloud service provider (CSP).

IV.PROPOSED SYSTEM

In this paper we overcome the drawbacks of previous system and we define a new system using Advance Encryption Standard algorithm (AES) for security. The AES algorithm is more secured than RSA algorithm and not easily accessible to unauthorized users. One more update on existing system is we use the one time password (OTP) for users registration and for log in. So the data can be access only by the trusted users not unauthorized users. If users are authorized then only cloud service provider (CSP) provides decryption key.

V. SYSTEM ARCHITECTURE

The system architecture in this paper involves three different entities: data owner, data user and cloud server, as illustrated in Fig. 1.

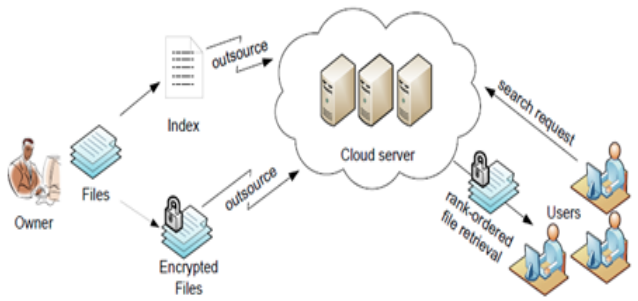

Fig.1 system architecture

1.Data Owners
The data owner is responsible for the update operation of his documents stored in the cloud server. While updating, the data owner generates the update information locally and sends it to the server.

2.Data users
Data users are authorized ones to access the documents of data owner. With query keywords, the authorized user can generate a trapdoor according to search control mechanisms to fetch encrypted documents from cloud server. Then, the data user can encrypt the documents with the shared decrypt key.

3. The cloud server
The cloud server in the proposed scheme is considered as "honest-but-curious", which is employed by lots of works on secure cloud data search. Specifically, the cloud server honestly and correctly executes instructions in the designated protocol. Meanwhile, it is curious to infer and analyse received data, which helps it acquire additional information, depending on what information the cloud server knows.

VI. CONCLUSION

In this paper, we tried to overcome the security problem, which was facing by the cloud users hence we define one time password for registration and log in. At the time of registration users have to give interest keywords. By using the interest keywords system can search the records in the cloud server. System can use the MRSE algorithm for searching records using interest keywords. In this paper we are providing the Advance Encryption Standard algorithm for data encryption for the purpose of data security.

ACKNOWLEDGEMENT

This work was supported in part by the Computer Department of Padmbhooshan Vasantdada Patil Institute Of Technology. We would like to thank our project guide Mrs. Sarika Bodke and authors Ning Cao for providing us with their experimental code for performance comparisons, and we also thank the editor and reviewers for their valuable suggestions.

REFRENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr, 2011.

[2] L.M. Vaquero, L. Rodeo-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM
SIGCOMM Compute. Common. Rev., vol. 39, no. 1, pp. 50-55, 2009.

[3] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFO- COM, pp. 693-701, 2012.

[4] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467- 1479, Aug. 2012.

[5] [6] I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.

[7] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

