ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A Survey on Efficient Encryption Scheme Over Data Sharing in Cloud Computing

Pooja Rajoria[1], Ravindra Patel[2]

P.G.Student, School of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya,

Airport Bypass Road, Gandhi Nagar, Bhopal, Madhya Pradesh, India[1]

Head of Department, Department of Master of Computer Applications, Rajiv Gandhi Proudyogiki Vishwavidyalaya,

Airport Bypass Road, Gandhi Nagar, Bhopal, Madhya Pradesh, India[2]

ABSTRACT: In current scenario mobile become one of the integral part of each and every one's daily life. Mobile cloud computing provides many on- demand services for the cloud user. In mobile cloud computing data can be stored at cloud server which reduces storage overhead of the user. But security of that data is the biggest concern in mobile cloud computing. In this paper a brief survey over the various techniques is presented. In [6] a encryption technique called CCBKE is presented which provides an efficient way for encryption that data. But it create problems when going to search that data. Thus [1] presents an efficient search technique which provides an efficient way to search that data. This paper proposed a classification based technique with keyword search mechanism to enhance the performance of the previous techniques.

KEYWORDS: CP-ABE(cyphertext attribute based encryption), RCCA(Root cause analysis and corrective actions), Encryption and Cloud computing.

I. INTRODUCTION

Mobile cloud computing provides a fast and efficient way to access many application. It reduces the hardware overhead and provides many on-demand services and resources for these services to the user. Mobile cloud computing combines the features of mobile computing, cloud computing and networking, to provide computational resources and on- demand cloud service framework for the user. In mobile cloud computing data stored at cloud server which reduces the storage overhead of the user and also provide application and resource to access that data as per their convenience.

Mobile cloud computing [1]-[4] gets rid of the hardware limitation of mobile devices by exploring the scalable and virtualized cloud storage and computing resources, and accordingly is able to provide much more powerful and scalable mobile services to users. In mobile cloud computing, mobile users typically outsource their data to external cloud servers, e.g. iCloud, to enjoy a stable, low-cost and scalable way for data storage and access. However, as outsourced data typically contain sensitive privacy information, such as personal photos, emails, etc., which would lead to severe confidentiality and privacy violations [5], if without efficient protections. It is therefore necessary to encrypt the sensitive data before outsourcing them to the cloud. The data encryption, however, would result in salient difficulties when other users need to access interested data with search, due to the difficulties of search over encrypted data. This fundamental issue in mobile cloud computing accordingly motivates an extensive body of research in the recent years on the investigation of searchable encryption technique to achieve efficient searching over outsourced encrypted data [6]-[7].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Networking A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links (data connections).

Cloud is defined by the two essential concepts:

1) Abstraction: Abstraction is one of the most important concepts of cloud computing. It store detail description of operation and execution perform by the user. User's application, location where data is store and outsource data is not defined.

2) Virtualization: There are two resource are used for virtualization firstly sharing of data and secondly pooling of data. It is based on the centralized infrastructure, where central system or server share data according to requirement. Cost of sharing data is depending upon used data by the user [8].

II.LITERATURE REVIEW

Our aim is device an efficient encryption scheme over data sharing in cloud computing so here we discuss most of the related work in this field.

Hongwei Li, Dongxiao Liu, Yuanshun Dai,Tom H. Luan and Xuemin(Sherman) Shen [3]

This paper propose a multi-keyword ranked search scheme to enable accurate, efficient and secure search over encrypted mobile cloud data. Security analysis have demonstrated that this scheme can effectively achieve confidentiality of documents and index, trapdoor privacy, trapdoor unlinkability, and concealing access pattern of the search user. Extensive performance evaluation has shown that this scheme can achieve better efficiency in terms of the functionality and computation overhead. Still authentication and access control issues need to be investigated.

Mathew Green, Susan Hohenberger and Brent Waters [11]

This paper is about outsourcing the decryption of ABE Ciphertexts, a new paradigm for ABE that largely eliminates the overhead of complexity of access formula for users. If ABE ciphertexts are stored in the cloud, this paper shows how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE ciphertexts satisfied by the user attribute into a (constant size) EI Gamal-style ciphertext, without the cloud being able to read any part of the users message. Moreover this approach has a minimal impact on performance.

YerraguntaHarshada, K.Janardhan [12] presents a ranking based share authority privacy preserving authentication protocol, in this protocol a ranking at the admin level assign to file on the basis of how frequently that file accessed. In this access control mechanism incognito access request matching is provided without disclosing user's information. User can access their data by the feature based access control process. Universal composability model is used to provide security for the data when different protocols are used during the process. A ranking is assign at the admin level to mention that how many time that file accessed. User can see that in their dashboard. That enhances the security of the system and provides knowledge about the vulnerability of the file.

Jianyongchen, Yang Wang [10] presents an on-demand security architecture for cloud computing. In this architecture three layers are there one is input layer, second is policy layer, and third layer is security mechanism layer. In input layer three checks is performed first is security level, in this only authorized user can be allowed to access the service unauthorized user doesn't have permission to access data. Second is type of service, in this, what type of service user want to access is checked because different type of service needs different security. Access network risk, in this the risk when service passes through the server is checked. Security policy in this layer data is checked and security parameters are implemented on the basis of security level,. Third layer is security mechanism layer, in this each domain provides different security mechanism, like encryption/decryption in storage domain, IP security in the network domain, honey pot in service do.

S Sankareswari, S Hemanth presents an access control mechanism for shared data over cloud. This technique a decentralize access control mechanism is used, in that there are several no of key distribution centers KDCs to share

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

key among the user. In existing technique a centralized key distribution mechanism is used, which sometimes leads to the problem of single point failure. To prevent replay attacks which used to performed to get access for the user's data. In this if a user once restricted by the protocol then he cannot back stale their information. Identity of the user is also not disclosed to the cloud server during the whole process. In this a SHA based encryption is used to hide the information of the user. In this information of the user not disclosed to the cloud server but cloud server knows the access mechanism for each data that stored in the cloud server.

B. Wang, S. Yu, W. Lou, and Y. T. Hou [13] In this paper a multi-user searchable encryption scheme with efficient access control for cloud storage is proposed. Specifically, it present the first solution to search the data that a user can decrypt by using the partial order relations. Here a new method to verify each user attributes without disclosing his relation of his identity and attributes is also design.By dividing the secret key the user can deligate the most CP-ABE decryption to a proxy server without disclosing the content, this is a secure and highly efficient scheme. Here focus is on access control instead of keyword search so further direction is to extend single keyword search to more expressive keyword search in the multi-user setting such as the conjuctive or Boolean keyword search.

Neelam S. Khan, Dr. C. Rama Krishna and Anu Khurana [14] In this paper an attempt was made to improve the data discovery and user searching experience by supporting secure ranked fuzzy multi-keyword search. In RFMS the time to generate the index at the DO reduced to a great extent. Also the overhead of generating the trapdoor for each query sent by Du is eliminated on DO. The DU directly queries the cloud server C. In future this searching scheme can be made more efficient by reducing the searching time as much as possible. An efficient ranking algorithm can also be made that will rank files first on the basis of multi-keyword match and then for the files with same rank it will calculate relevance score on the basis of frequency of each keyword in the file.

Chang Liu, Chi Yang, Xuyun Zhang and Jinjun Chen [15] In this paper a novel authenticated key exchange scheme namely Cloud Computing Background key Exchange (CCBKE), which aimed at efficient security-aware scheduling of scientific applications in hybrid computing environments such as cloud computing. This scheme has been designed based on commonly used Internet Key Exchange (IKE) scheme and randomness reuse strategy. In future, further investigation on new strategies to improve the efficiency of symmetric key encryption can be carry out.

III. BLIND STORAGE SYSTEM

A blind storage system is build on the cloud server to support adding, updating and deleting documents and concealing the access pattern of the search user from the cloud server. In the blind storage system, all documents are divided into fixed size blocks. These box are indexed by a sequence of random integers generated by a document-related seed. In the view of a cloud server, it can only see the blocks of encrypted documents uploaded and downloaded. Thus the Blind storage system leaks little information to the cloud server. Specifically, the cloud server does not know which blocks are of the same document, even the total number of the documents and the size of each document. Moreover all the documents and index can be stored in the blind storage system to achieve a searchable encryption scheme.

IV. CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

In ciphertext policy attribute-based encryption (CP-ABE), ciphertexts are created with an access structure (usually an access tree) which defines the access policy. A user can decrypt the data only if the the attribute embedded in his attribute keys satisfy the access policy in the ciphertext. In CP-ABE, the encrypter holds the ultimate authority of the access policy.
To precisely define and demonstrate the advantages of this approach, we provide new security definations for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of our algorithms

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

4.1Cryptography

For providing security in cloud computing cryptography is used. It is Greek word which means "secret writing.". There is minor difference between cipher and code. A cipher is a bit-for-bit transformation, without observe to the linguistic structure of the message. In contrast, a code interchanges one word with another word. Encrypted message is known as plaintext and transformed by the function that is known as key. After completing encryption process itis known as the ciphertext. This ciphertext is transmitted by radio. If any intruder copies down full ciphertext, but without knowing the decryption key cannot decrypt the ciphertext. Plaintext, ciphertext and keys are denoted by P,C and K respectively. It formulated as C = EK (P) to mean that the encryption of the plaintext P using key K gives the ciphertext C. likewise, P = DK(C) show the decryption of C to get the plaintext again.

4.4.1Two Fundamental Cryptographic Principle

1) Redundancy

Messages should contain some redundancy.

2) Freshness

Some method is required to foil replay attacks. Each messages including timestamp for 10 seconds. Then receiver switch new message and compare newly messages to old once. Message more than 10 sec automatically rejected [7]. In cryptography variety of ways to disguise message in order to avoid the interception from an unauthorized interception is known as cryptography. Encrypt correspond to the message transformation performed at the transmitter in order to mask the message. Decrypt corresponds to the inverse transformation performed at the receiver in order to recover the mask message into original message back.

4.5 Symmetric key encryption algorithm

Symmetric key encryption is also known as secrecy key encryption algorithm. The safety of conventional encryption depends on the confidentiality of the key, not the secrecy of the algorithm. We do not require to the algorithm confidentiality; we need only the secret key.

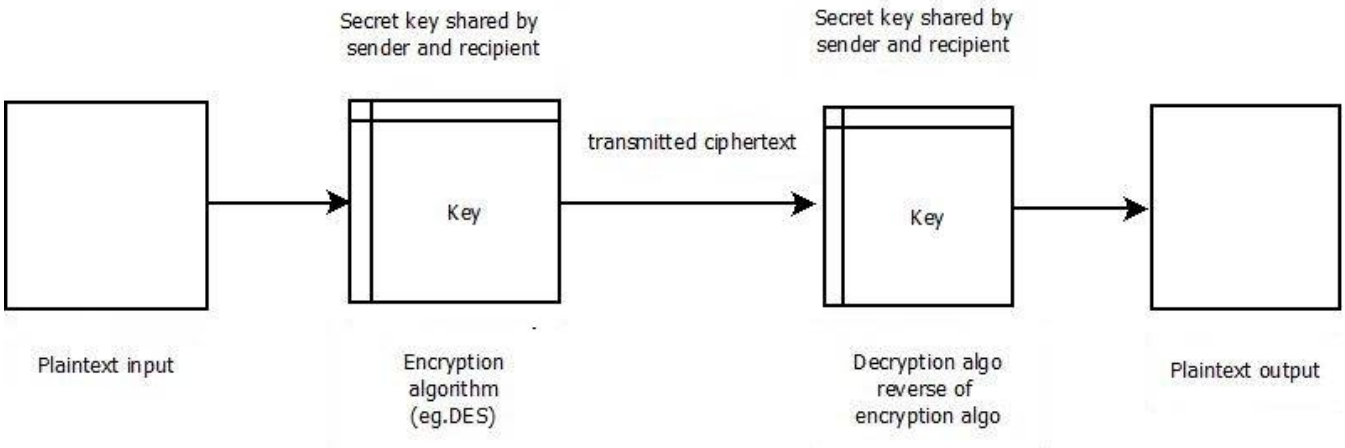

Figure 4.1: Symmetric key encryption

Figure 4.1 briefly describes the symmetric key entryption technique in which the input plaintext is encrypted and cypertext is send and then decrypted using suitable algorithm reverse of encryption and output is again plaintext.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Substitution Ciphers
In a substitution cipher each letter or group of letter is replaced by other letter or group of letter to differentiate it. One of the oldest cipher is known as Caesar cipher, attribute to Julius Caesar. In this method substitute different letter so unauthorized user can't access message like a become D, b become E, c become F, and z become C. For example, attack converted into DWWDFN.

For better understanding take a example let assume a is replace by 3, b is replace by 5, c is replace by 7 so on, replacement of message is called encryption and using this rule or key convert this encrypted message is called decryption and whole process is called cryptography.
Let assume
Plaintext: a c e g i k m o q s u w y b d f h j l n p r t v x z
Ciphertext: P Q R S T U V W X Y Z A B C D E F G H I J K LM N O

Transposition Ciphers
Convert original message in to the plaintext at the time of sending of data .Than convert this message into original message using key at receiving side but sequence of message is same.
In contrast, change the sequence of the letter but denote disguises them represent a common transposition cipher. The columnar transposition

M E A B U C K
7 4 5 1 2 8 3 6
W E L C OM E T
O S A f i r e 2
A P R A K A S A
A P R A K A S A
M A P
Plaintext: WELCOME TO Safire-2K8, CHIRALA, PRAKASAM, AP.
Ciphertext: CfHAOilKEeASE8PALACRPT2LAWOKAMMrRA
Key word:MEGABUCK

Advantage

1) Highly efficient than asymmetric key algorithm.
2) For encryption it takes less time because small encryption key size.
3) It used for large message.

But encryption is not sufficient for security of cloud computing so we can used

4.6 Proxy Re-encryption
A cryptographic prehistoric called proxy re-encryption, where a proxy can transform without seeing the plaintext and a ciphertext encrypted under one key into an encryption of the same plaintext under other key. The data sharing among the multiple users proxy re-encryption method is applied by the cloud server. Proxy re-encryption methods are cryptosystems which permit third parties to modify a ciphertext which has been encrypted for one entity, so that it may be decrypted by another entity.

PROXY RE-ENCRYPTION SCHEME
Proxy re-encryption schemes are like to usual symmetric or asymmetric schemes, with contain additional two functions.
1) Delegation

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Delegations permit a message recipient to produce a re-encryption key based on his secret key based and the key of the delegated client. This re-encryption key is used as input data to the re-encryption function, which is complete as ciphertext to the delegated key for clients. Asymmetric proxy re-encryption schemes are two types bi-directional and unidirectional.

• In a bi-directional scheme, the re-encryption scheme is invertible, like using re-encryption key translates messages from Jack to Charlie, as well as from Charlie to Jack. This can have multiple security issues, depending on the message. One of the most important characteristic of bi-directional schemes is that both the delegate and delegated party (e.g., Charlie and Jack) must merge their secret keys to produce the re-encryption key.

• A Unidirectional scheme is successfully one-way messages. It can be re-encrypted from Jack to Charlie, but not vice and versa. Unidirectional schemes can be constructed such that the delegated party require not disclose its secret key. For example, Jack could pass on to Charlie by merging his secret key with Charlie's public key.

2) Transitivity

Transitive proxy re-encryption schemes permit for a ciphertext to be re-encrypted a multiple times. For example, a ciphertext of the jack is re-encrypted from Jack to Charlie, and then again it was re-encrypted from Charlie to Ravi and this process is continued. Non-transitive schemes permit for only one of re-encryptions.

Advantage

1) Only single-hop because of this all known unidirectional schemes that resist collusions.
2) Using re-encryption our system is more efficient.
3) Using re-encryption builds on the primary unidirectional scheme.

4.7 Authentication

Authentication is Greek word which means real. Authentication mean if any user want to access any data than check is this has access permition to the particular data. On other hand identification is different from authentication means in identification check the user document, personal identity of user. Using identification authentication is performing means any type of document of identity is used for authentication.

There are 3 type of authentication

1) Firstly check that prove given by the user is valid and correct or not.

2) Second type of authentication is comparing the attributes of entity itself to what is known about matter of the origin.

3) Third type of authentication shows the proof on document or other external confirmation.

4.8 RCCA CONSTRUCTION

Root Cause Analysis(RCA) is an in depth process or technique for identifying the most basic factor underlying a variation in performance(problem).

- Focus is on system and process.
- Focus is not on individual.

Root cause analysis and corrective action (RCCA) is a systematic closed loop process for identifying issues and associated causes that are contributing factors to the key problem. The RCCA process facilitates concrete corrective actions in preventing reoccurrence , while promoting a team problem solving approach.

Corrective Actions

- Immediate actions.
- Permanent root cause corrective action.
- Preventing (systematic) root cause corrective action.

Process of RCCA

- Identifying a problem.
- Containing and analyzing the problem.
- Defining the Root cause.
- Defining and implementing the actions required to eliminate the root cause.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

- Validating that the corrective action prevent recurrence of problem.

V. CONCLUSION

This paper presents a brief overview for the various techniques which used to encrypt and search data in mobile cloud computing. In [6] an encryption technique is presented which uses CCBKE to overcome the Drawbacks of the existing IKE based encryption technique which is slow in performance for decryption. But there is a technique is needed to provide efficient search functionality to search that encrypted data. For that purpose many search technique are presented like in [5] a multi user searchable scheme is presented which uses CP-ABE based decryption technique to reduce the overhead of the decryption. In [1] a searchable encryption technique for multi keyword rank search is presented. But in all these technique all the data encryption storage is treated as same and there is no categorizing mechanism is provided to categorize that data. A classification technique with the searchable encryption technique for multi keyword rank search is proposed to enhance the performance of these techniques.

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An SMDP-based Service model for interdomain resource allocation in mobile cloud networks," IEEE Trans. Veh. Technol., vol. 61, no. 5,pp 2222-2232, jun. 2012.
[2] M.Armbrust, "A view of cloud computing, communications of the ACM", vol 53, no. 4, (2010).
[3] Hongwei Li, Dongxiao Liu, Yuanshun Dai,Tom H. Luan and Xuemin(Sherman) Shen "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage",March 2015
[4] H.T. Dinch, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput.. vol. 13, no.18,pp 1587-1611, December 2013.
[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity- based authentication for cloud computing" in cloud computing Berlin Germany: Springer-verlag,pp 157-166, 2009.
[6] W. Sun et al., "Privacy preserving multi-keyword text search over encrypted data in the cloud supporting similarity based ranking."in proc. 8th ACM SIGSAC Symp.Inf., Comput.Commun. Secur.,pp 71-82,2013.
[7] Y. Yang. H. Li, W. Liu, H. Yang, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in proc GLOBECOM. Anaheim.CA. USA, 2014.
[8] Li Chen, Xingming Sun, *Zhihua Xia and Qi Liu "An Efficient and Privacy- preserving Semantic Multi-Keyword Ranked Search Over Encrypted Cloud Data", International Journal of security and its application, 2014.
[9] S. Sankareswari, S. Hemanth "Attribute Based encryption with privacy preserving using asymmetric key in cloud computing" IJCSIT, 2014.
[10] Jianyongchen, Y. Wang, X. Wang, "On-demand Security Architecture for cloud computing" IEEE, 2012.
[11] Mathew Green (Johns Hopkins University), Susan Hohenberger (Johns Hopkins University), Brent Waters (University of Texas at Austin), "Outsourcing the decryption of ABE Ciphertexts".
[12] Y. Harshada, K. Janardhan, "Ranking Based Shared Authority Privacy Preserving Authentication protocol in cloud computing" IJIRCCE, May 2015.
[13] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in Proc. IEEE INFOCOM, April/May 2014.
[14] Neelam S. Khan, Dr. C. Rama Krishna and Anu Khurana, " Secure Ranked Fuzzy Multi-Keyword Search over Outsourced Encrypted Cloud Data",2015 5th International Conference on computer and communication technology.
[15] Chang Liu, Chi Yang, Xuyun Zhang and Jinjun Chen, "CCBKE-Session key negotiation for fast and secure scheduling of scientific applications in cloud computing".
[16] M. Naveed, M. Prabhakaran, and C. A. Gunter. "Dynamic searchable encryption via blind storage," in Proc, IEEE Symp. Sector: Privacy May 2014.