ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.2

A Result Paper on Outsourced Revocation of Encryption Based on Identity in Cloud Computing

Pruthviraj S. Patel[1], Kailas Patidar[2], Manoj Yadav[3], Rishi Kushwah[4]
PG Student[1], Professor & Head[2], Assistant Professor[3, 4]
Department of CSE
SSSIST, Sehore, M.P, India

Abstract:
In Cloud computing, user can remotely store and fetch their data based on-demand service, without the burden of local data storage and maintenance. However, the protection of the confidential data processed and developed during the computation is becoming the major security concern. It indicates that every user in the different groups can securely share data with others on untrusted cloud. The dynamic groups are also supported by this scheme. Once we are added in the group by the admin then thereis no need to contact admin every time while sharing file on cloud and while accessing the files. We can easily revoke the user through a novel revocation list without changing or updating the secret keys of other members. The reckoning and size overhead of encryption are constant neither depends on the number of revoked users. We provide a security and privacy-protect access control to all the users, which guarantee any member in different groups can request for accessing any file from other groups, then the receiver of that group will respond to the request sender. The actual information like identities of user can be shown by admin when clash occurs. We provide strong security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of computation overhead and storage. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services),which can be rapidly provisioned and released with minimal management effort. Using the cloud computing we can share group resources with different group members or we can say cloud user which is efficient and economical. Unfortunately, due to intermittent changes in membership, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue.

Keywords: cloud computing, Identity-based encryption (IBE), revocation, outsourcing, DES, user group

I. INTRODUCTION

Cloud consists of a large pool of easily usable and available virtualized resources. The users can access these resources based on their needs. Cloud computing is the delivery of computing services over the Internet. Cloud services grant individuals and businesses to use software and hardware that are managed by third parties at remote locations. These features have made cloud computing more beneficial. The expeditious usage of cloud has led to various security issues. The cloud computing model allows access to information and computer resources from anywhere where the network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications [1]. The beauty of cloud computing we don't need to buy equipment to use the services. In cloud computing the main drawback is internet connection is week service is not available, and can't provide integrity for client's data but in all the cases. Cloud security is the major drawback for its adoption. The various security issues include Data loss, DDOS attacks, militancy issues, availability etc. Users are more concerned about their data stored into cloud and retrieval of the data from the cloud. Thus, effective measures need to be taken to secure the users data. Cloud computing is an emerging technology that is gaining fast acceptance day by day. In recent years, cloud storage service has become a faster profit growth point by implementing a comparably low-priced, scalable, position independent platform for clients' data [4]. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to inculpate multiple internal and/or external cloud services together to provide high interoperability. A key barrier preventing organizations from with success exploitation services on the cloud is that they need leading internal policies, also as legal and statutory constraints that need compliance [3]. Such policies square measure these days depends on internal resources controlled by the organization. Once exploit remote services, it needs important human intervention and negotiation -- folks have to be compelled to check whether provider's service attributes guarantee compliance with their organization's constraints. When the supplier is composing services, some of which it gets from other providers get extremely advanced [1]. A connected issue is the lack of associates is integrated methodology and the service lifecycle on a cloud.

II. LITERATURE SURVEY

Cyber crime's effects are poke throughout the Internet, and cloud computing is an easy target for many reasons. Providers such as Google, Microsoft, and Amazon have the existing infrastructure to cover up and survive cyber-attacks, but not each and every cloud has such capability. If the provider identified by a cyber-criminal whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. Earlier all the data was hosted directly on cloud and for uploading and downloading, we used encryption and decryption mechanism. This was very hectic for the user to decrypt the data before accessing it. All the data hosted

directly on cloud causes less security for data and there is no proper management of files. We did not put any filter criteria on the files and authentication on it as per the content in the files. So in the proposed system we have revised all the possibilities. On cloud we have created separate groups and each group has different files. User need to request for the other group's file before accessing it and then the request is received by the receiver. If it is a known user then the file owner will approve his request accordingly. And also it has a good functionality; the file which is downloaded from one group cannot be uploaded to any other group. User need to upload it in a same group. This prevent from Mismanagement of data. Cloud services work on multi-tenancy model where the same resources are shared by multiple independent cloud users. Frequently this would lead to a situation where competitors are present as co-exist on the same cloud. Such an environment opens up a whole lot of possibility of data stealth.

III. PROPOSED METHOD

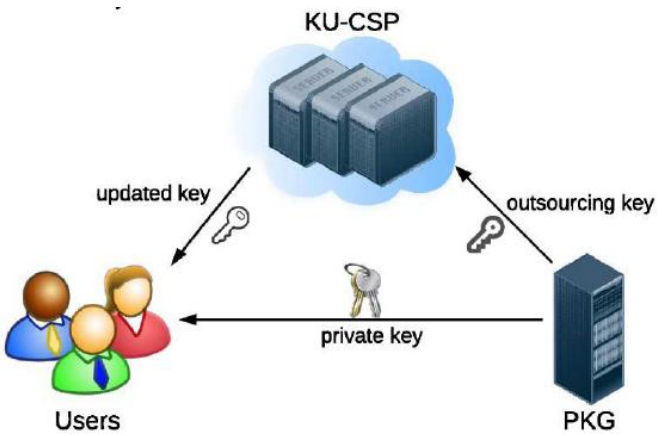

Figure.1.[3]System Model

The Proposed System is a scheme Identity Based Encryption with outsources revocation [3]. Our main focus is to make this system easy for dynamic groups in the cloud. For making this groups as a dynamic group we have used a group signature and dynamic broadcast encryption techniques, in this any cloud user can share his data without revealing the identity. This System ensures that any user in the group can securely share data with others by the entrusted cloud. We provide secure and privacy-preserving access control to users. It ensures that any user in the group can utilize the resources of cloud by obtaining a confidentiality and security. The System emphasizes on user revocation that is how to remove users of decrypt ability even if they have been received their private keys. For that we are embedding a time span into private key in an intellectual way for revocation. We can refer a example, ABC is a user which not encrypt only messages on xyz email id "xyz@gmail.com" but also it assume some time like (Thu June 21 2016) .Then xyz receives a encrypted email, that mail contains a 16 byte key, which is received by xyz user as a private key, that private key is associated with a time period component. When both appropriate components are available then email will be read. Suppose xyz is compromised, and then the KU-CSP update the all users old time component by new time span like (Fri June 24 2016). After that message should be sent to xyz's mail address with the updated time span .that time since xyz is don't having a updated time period then the system is not giving the access to xyz for decrypting a message. The challenge in designing the outsourced unsettled IBE scheme is how to prevent collusion between xyz and other unrevoked untruthful users. Specifically, a untruthful user (named pqr) can share his updated time component like (Fri June 24 2016) with xyz, and help xyz decrypt cipher text even if xyz just has the previous one like (Thu June 21 2016).

IV. SYSTEM MODULES

SYSTEMIMPLEMENTATION

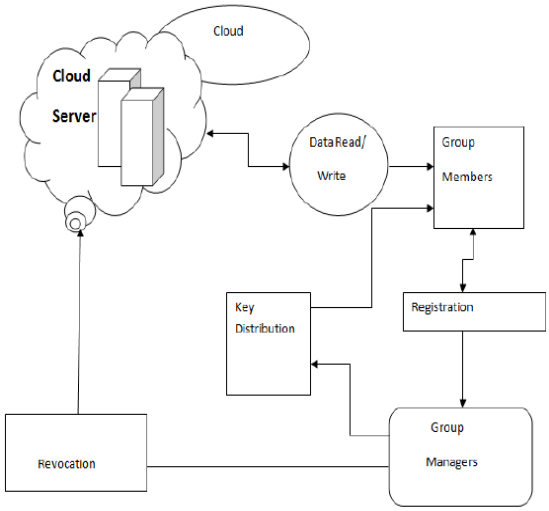

Figure.2.System Flow

1. User Registration:

User registrations can be done by collecting secure credentials of user, in that user have to register email id and they have to choose a specific group from number of available groups. In the registration group module created, for that group by doing user registrations we can add a number of users to that group. Group manager randomly selects some number as a group signature and sends it to all users in a group to the registered user mail id. After the registration, user gets a private key which will be used for group signature generation and file decryption

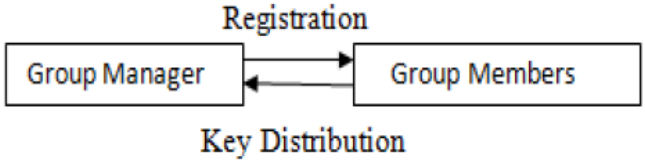

Figure . 3. [1] Registration

2. User Revocation:

Group manager or admin will have rights to perform user revocation in this system. Firstly group manager have to maintain a list of groups and its user and group manager also traces the users of a group. Group manager first selects a group and enter group signature, after that it should displays a list of users available that group and Manager also have rights to revoke user from any of the specific groups. Revocation list is maintained by group manager so that he can encrypt their data files and ensure that it wills hidden from revoked user it should be confidential from all revoked user. Group manger updates the revocation list each day and enters the information like which user have been revoked. In other words, the others can verify the originality of the revocation list from the contained current date.

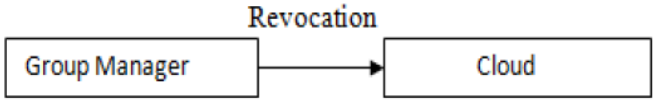

Figure .4. [4]User Revocation

3. File Generation and Deletions:
To store and share a data file on the cloud, a group member performs to getting the revocation list from the cloud for security purpose. In this step, the member sends the group identity ID group as a request to the cloud to verify that he is not a revoked user. File stored in the cloud can be deleted by either the group manager or the data owner.

4. File Access and Traceability:
User need credentials of group signature for his authentication to accessing cloud recourses. The member group signature can be regard as an alternative of the short group signature which inherits the inherent enforceability property, tracking capability and anonymous authentication. When a data conflict or clash occurs, manager performed the tracing operation to identify the real identity of the data owner. As in [4] IBE eliminate the need for a Public Key Infrastructure (PKI). Any setting, PKI- or identity-based, must give a means to remove users from the system. Efficient revocation is a well-studied problem in the traditional PKI setting. As mentioned in the setting of IBE, there has been studying work on the revocation mechanisms. The most practical result requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been adjust or not) to update their private keys regularly by contacting the trusted authority.

5. Sharing files with other groups in cloud
In the proposed system we have revised all the possibilities. On cloud we have created separate groups and each group has different files. User need to request for the other group's file before accessing it and then the request is received by the receiver. If it is a known user then the file owner will approve his request accordingly. And also it has a good functionality; the file which is downloaded from one group cannot be uploaded to any other group. User need to upload it in a member group. This prevent from Mismanagement of files or data. And using there is no chance of access file from outside not even from other group member without permission.

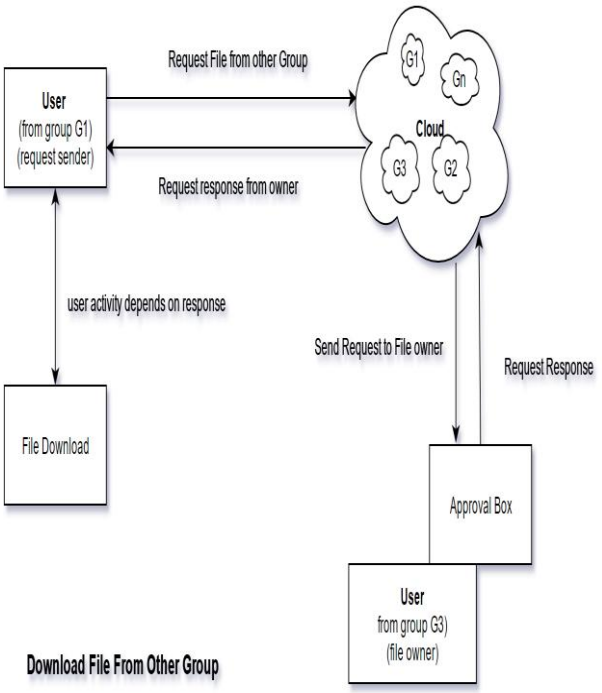

Figure.5. Sharing files with other groups

We present the first development of (non-interactive) forward-secure public-key encryption schemes [5]. Our main construction obtain security against chosen-plaintext attacks in the standard model, and all parameters of the scheme are poly-logarithmic in the overall number of time periods. Some extensions and variants of this scheme are also given. We also introduce the concept of binary tree encryption and construct a binary tree encryption scheme in the standard model. Our construction involves the first (hierarchical) identity-based encryption scheme in the standard model.

V. ALGORITHM

AES Algorithm
AES involves three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192,256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the process was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so the sender and the receiver must know and use the same secret key. All key lengths are deemed enough to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192-bit or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A round consists of many processing steps that include substitution, transposition and mixing of plaintext as input and convert it into cipher text of final output. AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule. For encryption, each round consists of the following four steps:

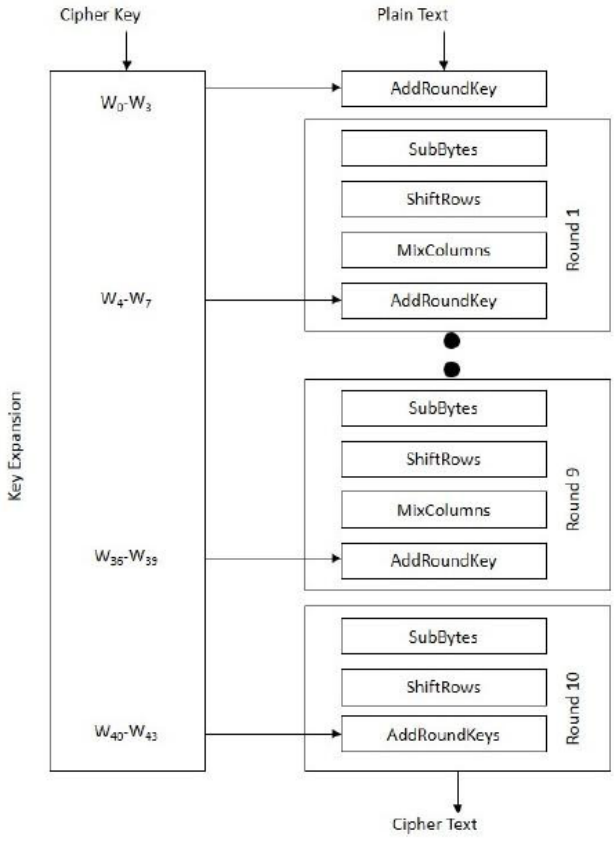

Figure.5. AES Encryption

- SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
- ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times
- MixColumns – a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

For the final round only three steps are performed: SubBytes, ShiftRow and AddRoundKey.

1. SubBytes

The purpose of this step is to give ample resistance from differential and linear cryptanalysis attacks. This is byte-by-byte substitution where each byte is substituted independently using Substitution table (S-box). Each input byte is divided into 24-bit patterns, representing an integer value between 0 and 15 which can then be interpreted as hexadecimal values. Left digit defines the row index and right digit defines the column index of S-box. At the intersection of row and column, value given is substituted. There are sixteen distinct byte-by-byte substitutions. S-box is constructed by a combination of GF (28) arithmetic and bit mangling.

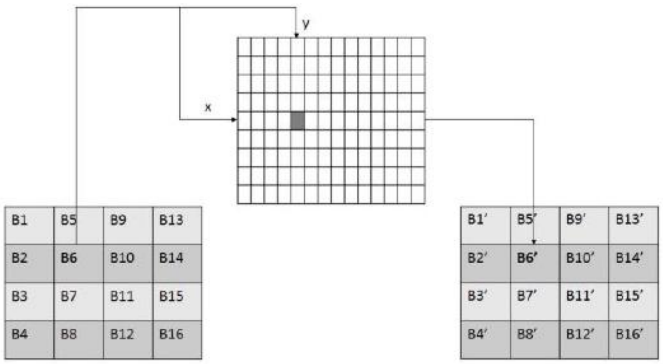

Figure.6. SubBytes Transformation Step

2. Shift Rows

The purpose of this step is to provide diffusion of the bits over multiple rounds. The row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, row 2 is circular left shifted by two bytes, and row 3 is circular left shifted by three bytes.

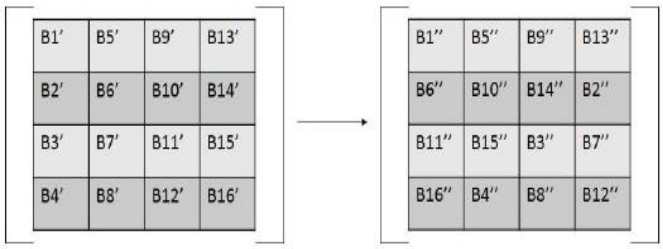

Figure.7. ShiftRows Transformation Step

3. MixColumns

Like previous step, the purpose of this step is to provide diffusion of the bits over multiple rounds. This is achieved by performing multiplication one column at a time. Each value in the column is multiplied against every row value of a standard matrix. The results of these multiplication are XORed together. For e.g. value of first byte B1'' is multiplied with 02, 03, 01 and 01 and XORed to produce new B1''' of resulting matrix. The multiplication continues against one matrix row at a time against each value of a state column.

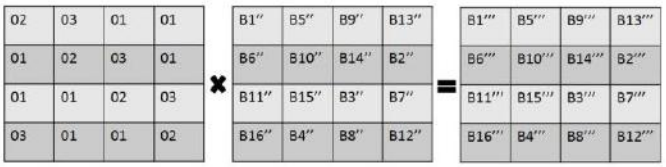

Figure.4. MixColumns Transformation Step

4. AddRoundKey

In this step, the matrix is XORed with the round key. The original key consists of 128 bits/16 bytes which are represented as a 4x4 matrix. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3] The rest of expanded key i.e. W[4] to W[43] is generated as follows:-

```
for (i=4; i<44; i++)
{
T = W[i-1];
if (i mod 4 = = 0)
T = Substitute (Rotate (T)) XOR RConstant [i/4];
W[i] = W[i-4] XOR T;
}
```

Here

Rotate means - perform a one byte left circular rotation on the 4-byte word.

Substitute means - perform a byte substitution for each byte of the word, using S-box, also used in the SubBytes step. RConstant means – Round Constant (size of 4 bytes) which is XORed with the bytes. The rightmost three bytes of the round constant are zero. In this way, W [4]… W [43] of the key schedule is generated from the initial four words. Although, overall, the same steps are used in decryption, as in encryption, the order in which the steps are carried out is different.

VI. CONCLUSION

This System proposes Identity Based Encryption scheme, it is based on dynamic groups in the cloud. It can be done by using a group signature and it uses dynamic broadcast encryption techniques, in this System any cloud user can anonymously share data with others on cloud. At that time the storage overhead and encryption computation cost of our scheme is totally self-determining as the number of revoke users is available. In this way the system mainly focusing on the user revocation which should solve the problems of efficiency and storage. And also provide the secure file sharing among the groups in cloud.

VII. REFERENCE

[1]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation,"in Advances in Cryptology (CRYPT O'98). New York, NY, USA: Springer, 1998, pp. 137–152.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557–557.

[4]A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. 15thACMConf. Comput. Commun Security (CCS’08), 2008, pp. 417–426..

[5] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology (EUROCRYPT’03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656,pp. 646–646.

[6] How to securely outsource cryptographic computations,Z. Kong, C.-Z. Xu, and M. Guo, “Mechanism design for stochastic virtual resource allocation in non-cooperative cloud systems,” in*Proc. 4th IEEE Intl. Conf. on Cloud Computing*, 2011, pp. 614–621.

[7] Sanchez-Avila, C., and R. Sanchez-Reillol. "The Rijndael block cipher (AES proposal): a comparison with DES." Security Technology, 2001 IEEE 35th International Carnahan Conference on. IEEE, 2001.

[8] NIST, FIPS PUB 197, “Advanced Encryption Standard (AES),” November 2001 [Online]. Available: http://csrc. nist.gov/publications/fips/fips197/fips-197.pdf.

[9] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit .com/ news/ technology/1112692915/cloud-computing-growth-paas-saas-091212/

[10] Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast [Online]. Available: http://www.idc. com/get doc.jsp ?containerId=236552

[11] John Harauz, Lori M. Kaufman and Bruce Potter, ―Data security in the world of cloud computing ―, 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[12] Jensen, Meiko, et al. "On technical security issues in cloud computing." Cloud Computing, 2009. CLOUD'09. IEEE International Conference on. IEEE, 2009.