International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Reliable and Efficient Revocation and Data Sharing using Identity based Encryption over Cloud

Vishal S. Baviskar[1], Prachi S. Dhage[2], Omkar U.Khot[3],Prof.Bhushan Patil[4]

[1,2,3]Student.Computer Science Department Rajiv Gandhi Institute of Technology Mumbai, India
[4]Prof, Computer Science Department Rajiv Gandhi Institute of Technology Mumbai, India

Abstract—*Tons of data is to be shared everyday, but directly outsourcing this data may lead to various security issues. The data that is to be shared must be stored securely and cloud computing is the convenient way for this purpose. Security has always been concern when it comes to data sharing in cloud computing. This Paper discuss about the prominent method for data sharing which is Identity based Encrytion. Any of the User's personal information will be used to generate the Encryption Key, thus there is no need for the users to specifically share the key previously. Once the authorization or the subscription of the user is exhausted, he/she will be revoked and thus will not be able to access the files thereafter.*

Key Words—Identity based Encryption, Encryption Key, and authorization, subscription, revoked.

1. INTRODUCTION

Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. [4]

A. Identity Based Encryption

Identity Based Encryption is a type of the public key in which the public key of the user is generated by some unique information about the identity of the user's (e.g email address). This means that while encrypting the file the user will use this key as a encrytion key. The receiver or the user again will obtain its decryption key from a central authority, which has needs to be trusted as it generates secret keys for every user. The main advantage of the identity based encryption is that if there are only finite number of users, after all users have beenissued with keys the third party's secret key can be destroyed. [5]

B. Revocable Storage

The Revocation means that Capable of Cancellation. The non-revocable data sharing system provide confidentiality and backward secrecy. [5]. Further-more, the method of decrypting and re-encrypting all the shared data can ensure for-ward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. To avoid this problem, the revocation storage makes use of cloud server.

2. LITERATURE SURVEY

- C. Wang S.S Chow Q. Wang Ren W. Lou proposed Pri- vacy preserving public auditing for secure cloud storage Propose a privacy preserving public auditing system for data storage security in cloud computing. This method eliminates the burden of cloud user from expensive auditing task and reduces the outsourced data leakage. The main problem of this method is cannot robustly cope with large amount of data. [2]

- K.Chard K.Bubendorfer S.Caton O.F.Rana introduced Social cloud computing: Vision for socially motivated resource sharing. It demonstrates the approach using a social storage cloud implementation in Facebook applica- tion. The main advantage of this technique is that, it pro- vides infrastructure and enables sharing of heterogeneous resources. Sharing resources within social cloud is not feasible and exchanged resources should be symmetric. [6]

- Jianghong Wei, Wenfen Liu, Xuexian Hu proved the security of the proposed scheme in the standard model, under the decisional -Bilinear Diffie-Hellman Exponent (-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure. [4]

- K. Bharathi, G. K. Roopa provided formal definitions for RS-IBE and its corresponding security model; and backward/forward secrecy simultaneously. [5]

- Kedar G. Pathare and Prof. P. M. Chouragade proposed a system that uses meta-data file technique to improve the security of file storage on cloud with implementation of identity-based encryption scheme. [7]

3. PROPOSED SYSTEM

Our main motto is to provide secure cloud storage system with the help of RSIBE (Revocable storage identity-based encryption). If user left the system his authorization should be revoked so that he/she should not be able to access files encrypted under his/her keys. We are using User's information for generating the Encrytion key. i.e Email address is being used in order to generate the Encryption Key.

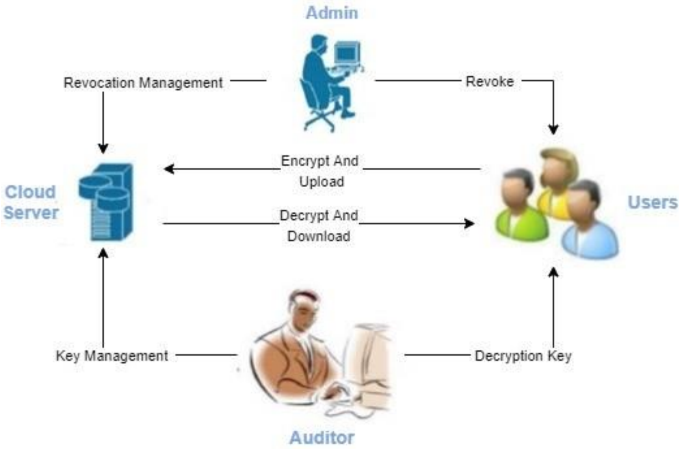


Fig. 1. Proposed System.

The Proposed System works as follows-

- The Users initially registers and select the files that are to be secured. Once the files are selected he can encrypt them and the cipher-text of the data is uploaded to the cloud server.

- When the User wants to get the data, she or he can down- load and decrypt the corresponding cipher-text. However, for an unauthorized user and the cloud server, the plain text of the shared data is not available. Decryption Key will be sent to the User by Key Authority.

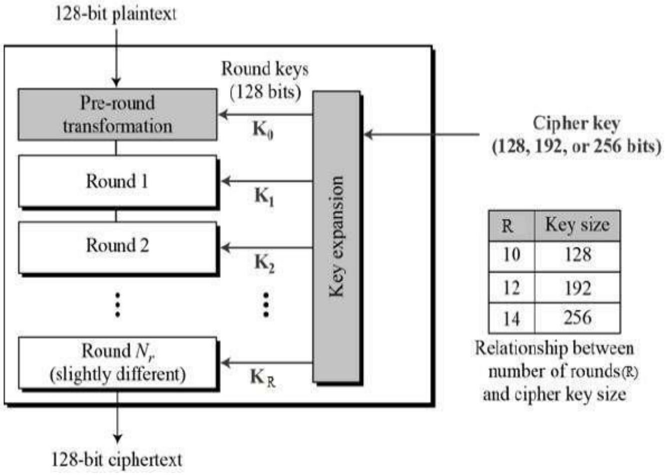
- In some cases, user's authorization gets expired; Admin will revoke that user and thus ensures that he or she is not able to access the data unless the user is authorized again.

A. Algorithm

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. AES Analysis In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discov- ered.

Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

The schematic of AES structure is given in the following illustration-



R	Key size
10	128
12	192
14	256

Fig. 2. AES Structure.

B. Advantages of Proposed System

- Data Security: The files will be encrypted using the Encryption key generated from individual's informa- tion. AES Algorithm is been used to Encrypt the files and thus ensure more security.

- Speed: The Algorithm Used for Encryption is AES and as shown in the graph, we could conclude that the speed of encryption for small file size is approximately equal for all the algorithms but as the file size increases the encryption time is less for AES as compared to other algorithms.

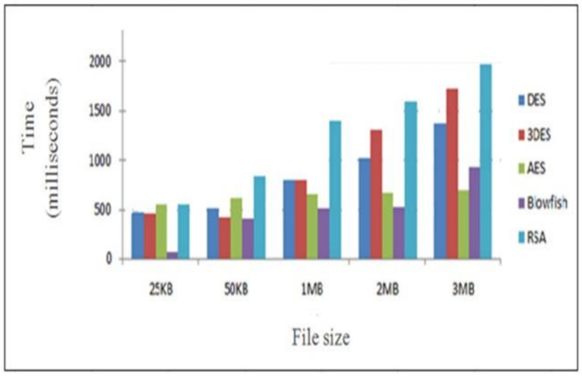


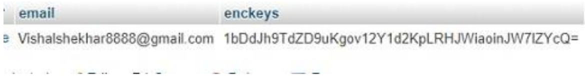
Fig.3. Algorithm Comparison

- Backward secrecy: According to Backward Secrecy, when a user's authorization or subscription is expired, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

- Forward secrecy: Forward secrecy means that, when a user's subscription is expired, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

4. RESULTS

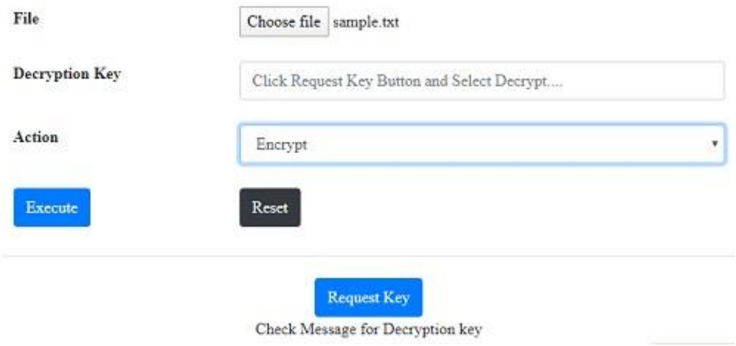
- Key Generation: Once the User registers successfully his/her Encryption key will be generated.



email	enckeys
Vishalshekhar8888@gmail.com	1bDdJh9TdZD9uKgov12Y1d2KpLRHJWiaoinJW7lZYcQ=

Fig.4.Key Generation

- Manage Files: This section allows User to Encrypt the file as well as to request the Decryption Key and then Decrypt the file.



File: Choose file sample.txt

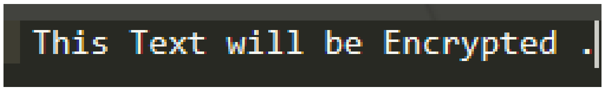
Decryption Key: Click Request Key Button and Select Decrypt....

Action: Encrypt

Check Message for Decryption key

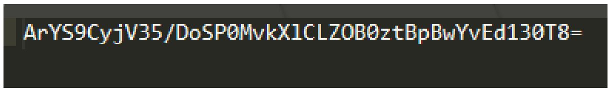
Fig.5.Manage Files

- The File will be Encrypted and a .crypto file will be generated. Fig(6) shows the original text of the file whereas Fig(7) is the cipher-text.



```
This Text will be Encrypted .
```

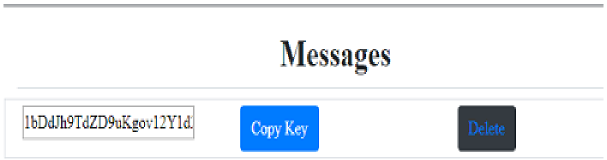
Fig.6.Original Content



```
ArYS9CyjV35/DoSP0MvkX1CLZOB0ztBpBwYvEd130T8=
```

Fig.7.Cipher-text

- The requested Decryption key will be available for the users in the Messages Tab, once it is sent by Auditor.

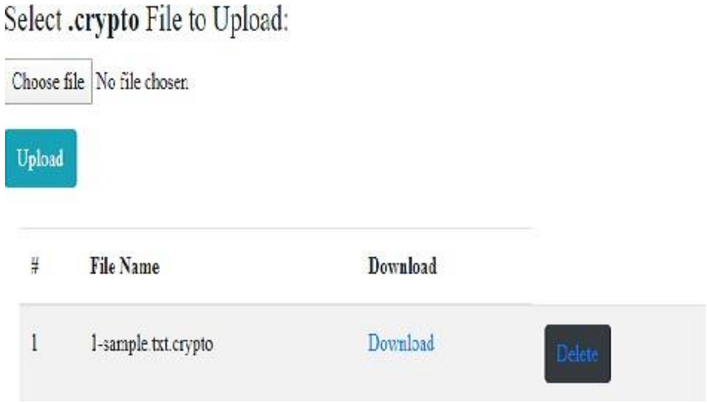


Messages

1bDdJh9TdZD9uKgov12Y1d

Fig.8.Decryption Key

- User can Upload the .crypto file from the Upload and Files Tab.



Select .crypto File to Upload:

#	File Name	Download	
1	1-sample.txt.crypto	Download	Delete

Fig.9.Upload .crypto File

5. CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity based encryption and revocation simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

REFERENCES

[1]A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in cryptology. Springer, 1985, pp. 47–53.

[2]C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, ”Privacy- Preserving Public Auditing for Secure Cloud Storage,” in IEEE Trans- actions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[3]D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[4]J. Wei, W. Liu and X. Hu, ”Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption,” in IEEE Transac- tions on Cloud Computing, vol. 6, no. 4, pp. 1136-1148, 1 Oct.- Dec. 2018.

[5]K. Bharathi, G. K. Roopa, “Secure Cloud Computing: Data Sharing using Revocable-Storage Identity-based Encryption” in International Journal of Research in Engineering, Science and Management Volume- 2, Issue-1, January-2019.

[6]K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, “Social cloud computing: A vision for socially motivated resource sharing,” Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[7]Kedar G. Pathare ,Prof. P. M. Chouragade “Reliable Data Sharing Using Revocable-Storage Identity-Based Encryption in Cloud Storage ” 2017 International Conference on Recent Trends in Electrical, Electronics and Computing Technologies,978-1-5090-6266-9/17.