An Enhanced Secure Data Outsourcing using RBAAC Model in Cloud Computing

S. Abarna[1], V.R. Shashanthini[2], M. Jeeva[3], S. Devadharshini[4]

[1-4]*Department of Computer Science and Engineering Raak College of Engineering and Technology, India.*

---***---

ABSTRACT:- Data outsource in cloud computing is raising trend among many firms owing to its monetary advantages. Data that are publicly accessible must be kept confidential and protected against manipulation. Cryptography provides solutions to all these problems. Although ABE and IBE encryption allows for privacy-preserving keyword search over encrypted data in public cloud, fine-grained access control over encrypted data is considered as a critical challenge. In our project, we have enhanced both exact keyword search and fine-grained access control using RBAAC Cryptography to enhance security without loss of data confidentiality. By RBAAC cryptographic encryption technique, the server side encryption and client side decryption are acknowledged and file access is supported only to the authenticated users in order to avoid malicious access.

Keywords: RBAAC, ABE, IBE.

1. INTRODUCTION:

Cloud computing is the on-demand availability of computer system resource, especially data storage and computing power, without direct active management by the user. Clouds may be limited to a single organization (enterprise clouds), be available to many organizations (public cloud), or a combination of both (hybrid cloud).Cloud computing relies on sharing of resources to achieve coherence and economies of scale. Cloud storage works by enabling user's access and to download image on any chosen device, such as a laptop, tablet or smartphone. Cloud storage users can also edit documents simultaneously with other users as well, making it easier to work away from the office. Cloud services are broadly divided into three categories:

- IAAS
- PAAS
- SAAS

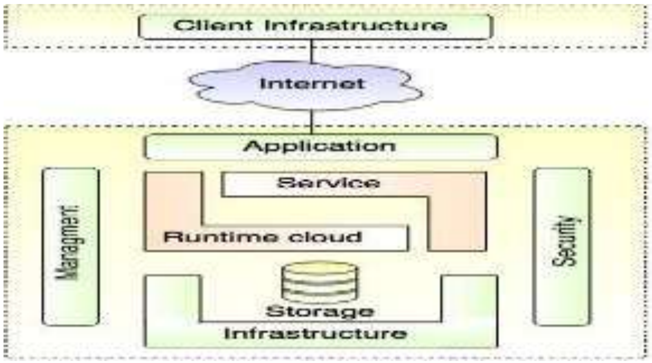


Fig1: Cloud Computing Architecture

Characteristics of Cloud Computing

- On-demand self-service. Cloud computing resources can be provisioned without human interaction from the service provider.
- Broad network access.

2. EXISITING SYSTEM

In the existing system, searchable encryption is deployed using IBE and ABE without loss of data in public cloud. However it could not work effectively for supporting fine-grained access control over encrypted data and detect the malicious users. Moreover, IBE and ABE encryption algorithm is used for authentication to provide security for data. This is considered as a drawback under a hybrid architecture in which a public cloud is used as an access interface between users and public cloud. Here, data are said to be accessible by the hackers.

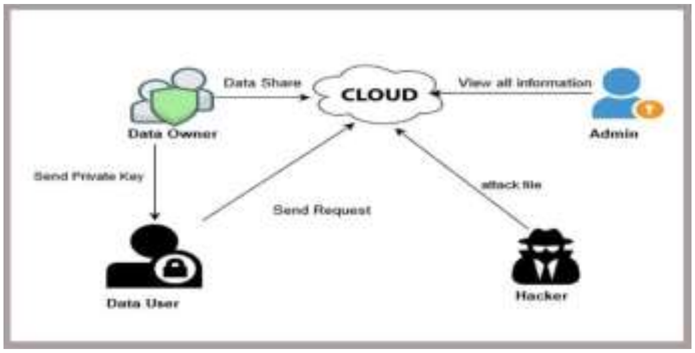


Fig 2.1: Existing System Architecture

DISADVANTAGES:

- Developing a False Sense of Security.
- Only supports AND gates (positive and negative attributes) which is low expressive.
- It could not analyze whether the users are authenticated or unauthenticated.

3. PROPOSED SYSTEM:

Efficient data sharing and searching with security is of critical importance. In our project, the secure way of enabling privacy protection were held through the RBAAC algorithm which is used to verify the role of each user and grant the file access as per their role with Private key generation scheme. Our new primitive provides flexible keyword update service for each user. And the multi-keyword search is used here to search or sort out the particular data that are need to access by the authenticated user. By this cryptographic technique, data that are not accessible by the unauthenticated person are aborted and the malicious users (hackers) are identified easily. This mechanism is applicable to many real-world applications, such as electronic health record systems.

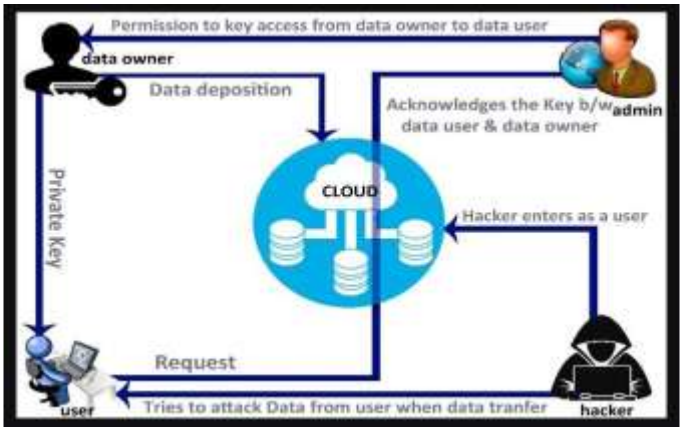

Permission to key access from data owner to data user
data owner
Data deposition
Acknowledges the Key b/w data user & data owner
admin
Private Key
CLOUD
Hacker enters as a user
Request
user
Tries to attack Data from user when data tranfer
hacker

Fig 3.2: Proposed System Architecture

ADVANTAGES:

- Minimize the effect expressiveness.
- Reduces computation and communication cost.
- Protects data across devices.
- Malicious users are detected.

4. SYSTEM DESIGN Modules Description:

1. Authenticated Data Owner
2. Authenticated User
3. Trusted Authority
4. Cloud Server

4.1. Authenticated Data Owner:

In this module, after completion of register process the data owner can able view and update profile information. In case of unregistered users, registration process should be made clear first. Then owner proceeds to upload the file records to the cloud storage in where we store the data. This is used to view the details of user who has sent request for data access. Data owner gives permission to user to access the file from the cloud. And also help to view the information of upload files and attacked files.

4.2. Authenticated User:

In this module, Authenticated Data User create an account to become a new data user and only after analyzing their role, they can able to find the file record ,only after the authentication process completed. By this way, user can search the required file through multi-keyword search scheme. The users now send request to the file which is needed to them. After getting access permission, they can download the file record and also view top file information.

4.3. Trusted Authority:

In this module, Admin or Trusted authority can view the information of data owner, user details, uploaded file information, details of requested files and details on files which are tried toattack.

4.4 Cloud Server:

In this module, cloud server have access to view the details of data owner and requested file by users. This cloud storage assigns key to the file record which are uploaded by the owner and grants permission to the users to access the file record. It can view the leaked file details.

5. ALGORITHM

```
Algorithm I – Key Generation for RBAAC
//Key generation
Step 1: Let Key size be 128 bits or 16 Bytes
Step 2: K (or) IdP = identity Attribute of the participant.
Step 3: Let K = size (IdP)
Step 4: If K >16
Step 5: K = substring (IdP, 16)
Step 6: Else if K <16
Step 7: K = 16 - K
Step 8: For x= 1 to K
Step 9: K = K +x;
Step 10: End for K
Step 11: End if K
//Encryption
Step 1: Let M=4, N=18
Step 2: Prepare P-array with N number of 32 bit sub keys from the input Key (K)
Step 3: Generate M number of S-boxes each of 256 bit size.
Step 4: Input plaint data is D may be of any size
Step 5: Convert the plaintext as a sub data of 64bit up to Size (D)
Step 6: Now Sub {L, R} = D /2{32bit, 32 bit}
Step 7: For Y= 1 to 16 rounds
Step 8: If Y<16
Step 9: L =L
Step 10: R =R
Step 11: Increment Y
Step 12: Swap (L, R);
Step 13: Update P with S-boxes elements;
Step 14: Else If Y=16
Step 15: L =L ¬|]ɔ
Step 16: R =R ¬|]ɔ
Step 17: Increment Y
Step 18: Swap (L, R) ;
Step 19: Update P with S-boxes elements;
Step 20: D = merge {L , R}
Step 21: End if Y; Step 22: End for Y;
```

6. PERFORMANCE ANALYSIS

In this sector, the experimental results of existing and proposed algorithms are evaluated and compared by using various performance measures.

6.1 TIME CONSUMPTION

Response time is defined as the amount of time difference from the release time and the finishing time of a given task. Here, the response time is calculated for both existing and proposed techniques with respect to varying detection probability. It is calculated as follows:

Response time = Task receiving time –

Task assigning time

6.1.1 Encryption memory

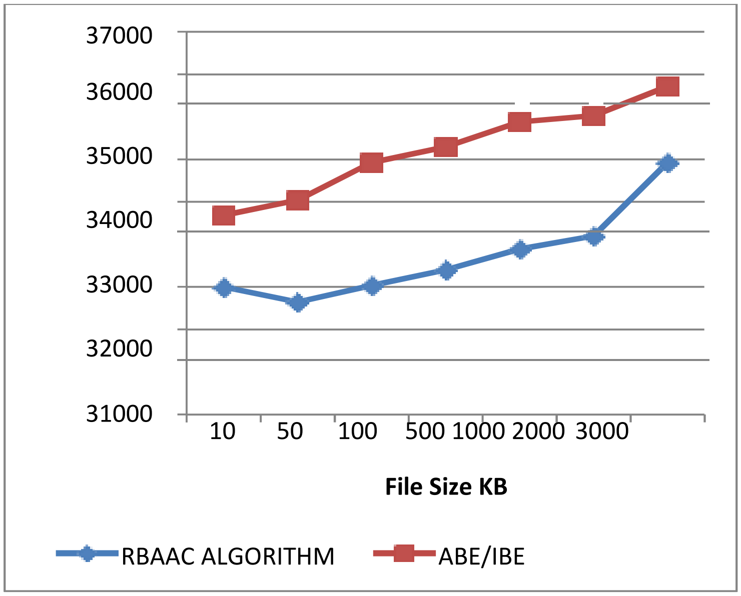
The amount of main memory required to execute the

File size (KB)	RBAAC technique	ABE/IBE
10	30992	32681
50	30638	33039
100	31028	33924
500	31394	34292
1000	31884	34881
2000	32194	35028
3000	33920	35719

Table6.1.1: memory consumption

encryption algorithm, where the input amount of data depends on the user input is known as the encryption memory. The encryption memory is also termed as the time complexity of algorithm. The computed file size is given here in terms of milliseconds (MS). According to the made observation in the experimental results the proposed algorithm consumes fewer resources as compared to the traditional encryption technique.

Graph6.1.1



The mean performance of the techniques is calculated using the following formula.

N Mean Encryption TIME = 1 Σ O

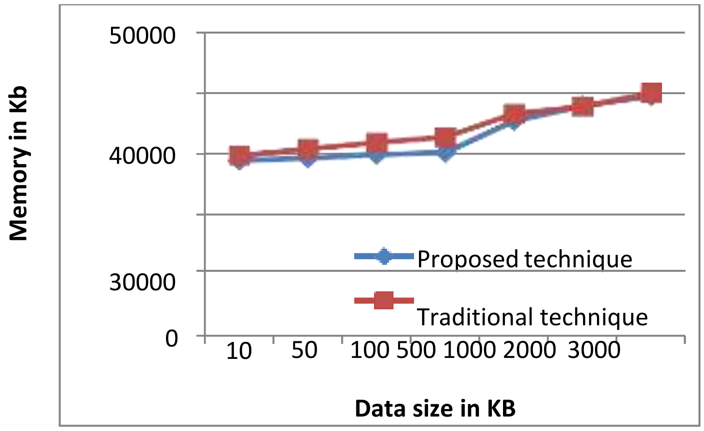
i.. (Eq1)

Ni=1

Where the 0i is the observation made and N is the number of observation is taken. The figure 5contains the mean performance of the algorithms. The given figure contains the methods implemented, in X axis and the Y axis, is reported mean encryption time in milliseconds. According to the evaluated results the memory consumption of the ABE/IBE algorithm is higher enough as compared to proposed RBAAC algorithm.

6.1.2 Decryption memory

The amount of main memory required, to recover the original text from cipher is defined as decryption memory. That can also be termed as space complexity of decryption.



Graph6.1.2

Table6.1.2: Decryption Memory

File size	Proposed technique	Traditional technique
10	29019	29847
50	29383	30924
100	29981	31947
500	30284	32844
1000	35472	36649
2000	37918	37845
3000	39519	40029

6.2 DECRYPTION TIME:

The time difference between initialization of data recovery and finishing the recovery work is termed here as decryption time. This can also be termed as the decryption time complexity

File size	RBAAC	ABE/IBE
10	0.331	0.547
50	2.04	3.38
100	4.12	6.21
500	18.14	28.42
1000	34.93	46.52
2000	68.25	112.53
3000	105.39	158.45

Table6.2: Decryption Time

6.3 ENCRYPTION TIME:

The encryption time is measurement of time interval, computed between initialization of the encryption process and the end of process. That is also termed as the encryption timecomplexity.

File size	Proposed system	Traditional system
10	0.473	0.947
50	2.94	5.38
100	5.32	8.47
500	23.42	31.53
1000	47.82	59.41
2000	92.31	142.53
3000	135.33	198.44

Table6.3: Encryption Time

6.4 PERFORMANCE EVALUATION:

S.no.	Parameters	RBAAC	ABE/IBE
1	Encryption time	Low	High
2	Decryption time	Low	High
3	Encryption space	Low	High
4	Decryption space	Low	High

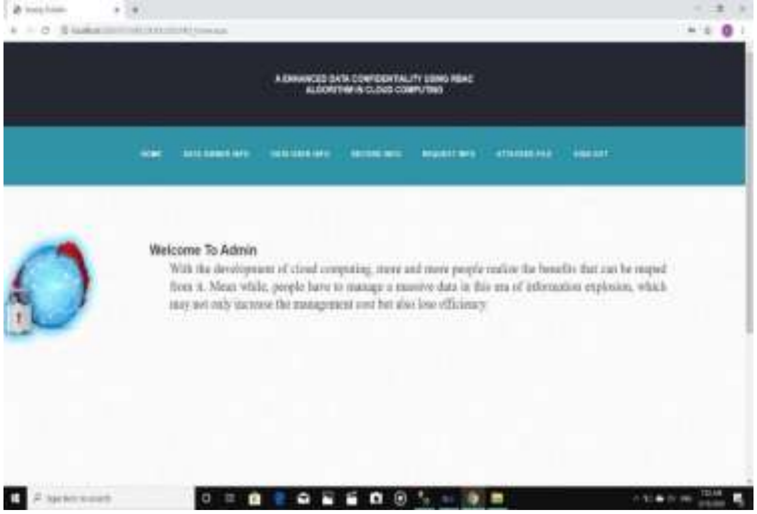
Table6.4: Performance Evaluation

7. SYSTEM REQUIREMENTS

7.1 FUNCTIONAL REQUIREMENTS

The purpose of system requirement specification is to produce the specification analysis of the task and also to establish complete information about the requirement, behaviour and other constraints such as functional performance and so on. The goal of system requirement specification is to completely specify the technical requirements for the product in a concise and unambiguous manner.

7.2 RESULT



A ENHANCED DATA CONFIDENTIALITY USING RBAC
ALGORITHM IN CLOUD COMPUTING
HOME
DATA OWNER INFO
DATA USER INFO
REQUEST INFO
ATTACKER FILE
LOGOUT

Welcome To Admin

With the development of cloud computing, more and more people realize the benefits that can be reaped from it. Mean while, people have to manage a massive data in this era of information explosion, which may not only increase the management cost but also lose efficiency

8. CONCLUSION

Making use of cryptographic techniques will enables the data protection. Asymmetric encryption method are not alone sufficient to achieve and enhance the security of the cloud environment. Hence our project has aimed at introducing a role based policy with acknowledgement which can be employed for various hierarchical file access as well as outsourcing methods. In order to achieve a clean insight of the domain, the upcoming threats should be mapped. Hence, securing these data outsourcing with a strong role based policies and cryptographic technique can enables optimized security in the cloud. In this manner, we have improved the efficiency of data outsourcing and prevent them from the hackers

9. REFERENCES

1. Mahdi Ghafoorian, Dariush Abbasinezhad- Mood, Hassan Shakeri A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud - VOL. 30, NO. 4, APRIL 2019.

2. R. Li et al., “A lightweight secure data sharing scheme for mobile cloud computing,” IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344–357, Apr./Jun. 2018.

3. R. Li et al., “A lightweight secure data sharing scheme for mobile cloud computing,” IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344–357,Apr./Jun. 2018.

4. Z. Ying et al., “A lightweight cloud sharing PHR system with access policy updating,” IEEE Access, vol. 6, pp. 64611–64621, 2018.

5. J. Li et al., “Industrial Internet: A survey on the enabling technologies, applications, and challenges,” IEEE Commun. Surv. Tuts., vol. 19, no. 3, pp. 1504–1526, Thirdquarter 2017.

6. Q. Huang, Y. Yang, and L. Wang, “Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things,” IEEE Access, vol. 5, pp. 12941–12950, 2017.

7. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloudbased augmentation for mobile devices: motivation,

taxonomies, and open challenges," IEEE Commun. Surveys Tutorials, vol. 16, no. 1, pp. 337–368, Jan.-Mar. 2014.

8. I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," MDPI Comput., vol. 3, no. 1, pp. 1–35, 2014.

9. Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing,"J. Inf. Security Appl., vol. 19, no. 1, pp. 45–60, 2014.

10. M. Portnoi and C. Shen, "Secure zones: An attribute based encryption advisory system for safe firearms," in IEEE Conference on Communications and Network Security, CNS 2013, 2013. IEEE, 2013, pp. 397–398.

11. N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future Generation Comput. Syst., vol. 29, no. 1, pp.84– 106, 2013.

12. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

13. P. Paillier, "Paillier encryption and signature schemes," in Encyclopedia of Cryptography and Security, 2nd Ed., H. C. A. van Tilborg and S. Jajodia, Eds. Springer, 2011, pp. 902–903. [14]V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryptionfor fine- grained access control of encrypted data," in ACM CCS'06, 2006,pp. 89–98.

14. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology, Proceedings of CRYPTO '84, 1984, Proceedings, 1984, pp. 47–53.

AUTHORS

S.Abarna M.tech, MISTE, Department of Computer Science and Engineering Raak College of Engineering and Technology, India.

V.R.Shashanthini, Department of Computer Science and Engineering Raak College of Engineering And Technology, India.

JEEVA M, Department of Computer Science and Engineering Raak College of Engineering And Technology, India.

S.Devadharshini, Department of Computer Science and Engineering, Raak College of Engineering And Technology, India.