Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

A Survey on Nominal Duplication of User Data Incorporating Anti-Collusion Schemes in a Cloud Group

Ambreen N. T [1], Anusha Gandhi J [2], Mythri Devi G [3] , Mrs. J. Deepa B.E., M.Tech. (PhD)[4]

[1,2,3] *B.E., Final Year, Department of Computer Science and Engineering.*

[1,2,3] *Panimalar Institute of Technology, Chennai, India.*

[1] khanithambreen@gmail.com

[2] anushagandhi1996@gmail.com

[3] mythrivijay6@gmail.com

[4]*Assistant Professor, Department of Computer Science and Engineering.*

Panimalar Institute of Technology, Chennai, India.

[4] deeparavindhran@gmail.com

ABSTRACT - Interestingly, cloud computing incorporates client terminals which are light weighted in nature, hence the OSs, applications, and the data are centrally stored in servers that can be shared among a variety of users within a cloud. This sort of centralization and file sharing within a group can lead to collusion attacks in an insecure cloud. The objective of this survey is to identify various Anti-Collusion Schemes incorporated in a cloud group to achieve a nominal reduction in duplication of user data. The Analysis and evaluation of the existing schemes help to identify a solution that ensures security, privacy, and file access while preventing hacking and collusion attack prevailing in a cloud using ABE algorithm. The proposed solution provides distribution of key without the need for a secure communication channel using a group manager. Here the client/user is authenticated using an image as an attribute which uses a pseudo-random generator technique. Hence, data de-duplication and prevention of unauthorized access to a file using graphical passwords.

KEY WORDS-Collusion Attack, De-Duplication, Group Manager, ABE Algorithm, Pseudo Random Generator Technique.

I. INTRODUCTION

Cloud computing is considered to be a popular technology that comprises a higher level of computational power including a large storage capacity with the promise of lower expenditure on hardware and software. In simpler terms, it could be said that a cloud computing environment improves storage and retrieval of a file and other services over the internet by reducing the need for a well-equipped terminal at the user side.

The key concept of cloud computing has helped us avail services and resources using a **pay-as-you-go** model. However, this uniqueness has brought new challenges in security and the privacy of the files being accessed on a cloud.

The storage and distribution of keys are more problematic in the cloud because it requires a secure communication channel which is difficult for practice. The current cloud schemes use a Secret Sharing technique to store and distribute the key among a group of recipients. The recipients with the key can regenerate the original secret sent by the sender.

This technique suffers when revocation of user privileges are possible in the group. Thus the proposed system uses a Group manager and a Group Admin to ensure key distribution and authentication in a cloud group.

Fig.1 Cloud Security

II. LITERATURE SURVEY AND PROBLEM IDENTIFICATION

A. Cong Wang, Qian Wang, and Kui Ren AND Wenjing Lou "Ensuring Data Storage Security in Cloud Computing"

This paper focuses on cloud storage security that has always been an important issue in quality of service. To ensure the integrity of the users' data in the cloud; the author proposes an efficient and flexible distributed scheme with two aspiring features, in contradiction to its predecessors. This system uses a homomorphic token that is distributed ensure coded data, thus achieving the storage integrity insurance along with data error localization, i.e., the identification of malfunctioning servers.

B. A. Juels, S. Kaliski, and J. Burton, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS'07, pp. 584-597, 2007.

This paper produced a formal "proof of retrievability" (POR) for large blocks of user data; this formal model thus enables remote data integrity. This system combines a spot checking and the error localizer algorithm to ensure the retrieval of files on any archived service systems.

C. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession, " Proc. of SecureComm '08, pp. 1-10, 2008.

Here a PDP scheme that uses a symmetric key cryptography is suggested by the author. This method provides a lower-overhead than their previous counterparts and allows the Updation, deletion and append of blocks to the stored file, which has also been supported in the proposed solution.

D. Tao Peng, Qin Liu & Guojun Wang, "A Multilevel Access Control Scheme for Data Security in Transparent Computing", IEEE Trans. Computing in Science & Engineering, Vol. 19, Issue 1, 2017.

Here a transparent environment is said to have light-weighted client terminal and so a Multilevel Access Control Scheme in transparent computing to protect user data at different security levels, and provide valid identity authentication is proposed. The proposed scheme is efficient in multilevel data security, flexibility in authorized resource sharing, and is also secure against various attacks.

E. Sayalee Shinde & Dr. S. S. Shaikh, "A Survey on Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IJIRCCE, Vol. 4, Issue 12, December 2016.

Interestingly, this paper suggests that the users can achieve an effective and cost-efficient approach for data sharing among the members of a group in a cloud with the characteristics of a low maintenance and ever so little management cost. The proposed system must henceforth provide security guarantees in terms of data sharing since they are gathered.

F. Anandu Jayan, Akash Nair, Bhargavi R. Upadhyay & Supriya M, "Performance Analysis of Modified RC4 Cryptographic Algorithm Using Number of Cores in Parallel Execution", IJCTA, Vol. 9, pp. 225-231, 2016.

Here a modified RC4 algorithm that can be implemented parallel using CUDA, MPI and OpenMP is proposed. The proposed algorithm exhibits a better performance in comparison to its counter parts such as AES, DES, and RSA algorithms which are currently in use.

III. PROBLEM IDENTIFICATION

Data Confidentiality inside the groups of the cloud is difficult to track and manage. Cloud computing establishes a user-friendly environment of a cloud group to share documents among the users of the group and avail miscellaneous services via internet and so it is vital to ensure data integrity and security to its users. The data stored in a common space is always in threat as it is accessible to a number of users including the *Cloud Service Provider (CSP).* This lack of control over the data causes a great security issue than the generic cloud computing. Encryption doesn't promise full control over the centralized data but it is somewhat better than the plain text. The *fig. 2* provides the top security concerns in cloud computing.

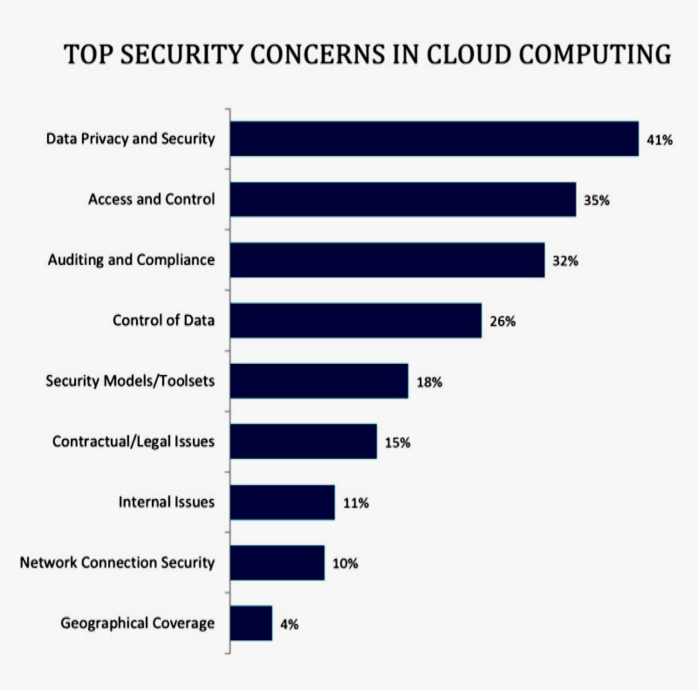


Fig. 2 Security Concerns in Cloud Computing

IV. PROBLEM SOLUTION

A user accesses the Group Manager to gain access to a group. When a user wants access to a group, the client sends a request to the group manager along with a private key generated by the system, once the key is verified by the group manager, the user's key to be used in the group is activated. This system uses a fine-grained access control to prevent revoked users from gaining access to confidential files.

The group manager performs the below tasks when a new user joins the group or a user has left the particular group,

A. Update the whole user name-list.
B. Generate a secure key and encrypt the key without activation and send to the updated user list.
C. Update the rights on the cloud server.

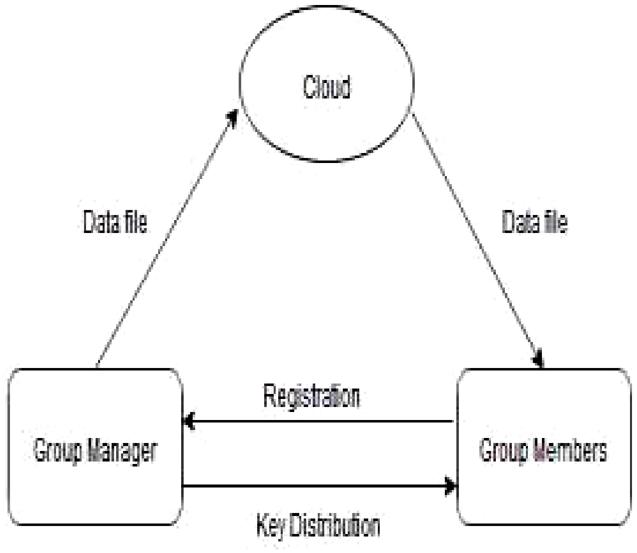


Fig. 3 System Model

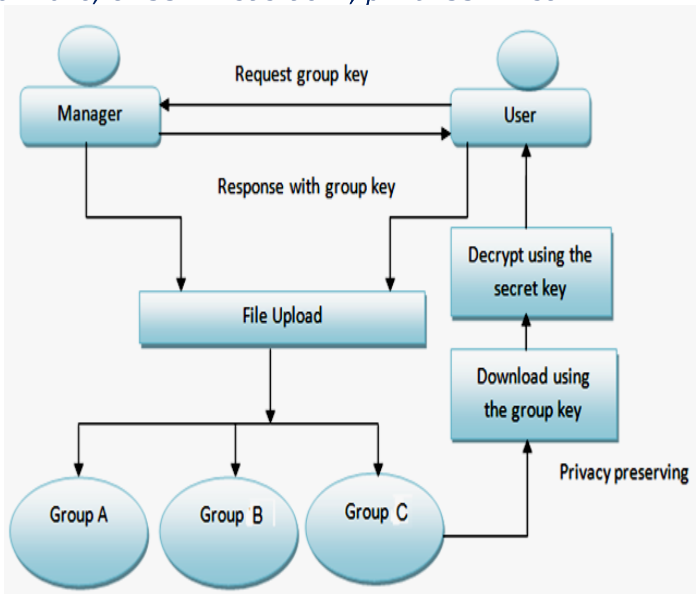


Fig. 4 Anti-Collusion using Group Manager

V. ENCRYPTION with ABE

Attribute-Based Encryption (*ABE*) is a public-key based encryption playing a new and vital role in maintaining the integrity of an uploaded file. This mode of encryption enables the cloud users to encrypt and decrypt their data based on user attributes which are specific to the respective client/user. Here the secret key of the user and the ciphertext are dependent on the user-specific attribute. In such a case, the decryption of a ciphertext is made possible only if the set of attributes of the user key matches the attributes of the ciphertext. Collusion-resistance that reduces duplication in the cloud is a crucial security feature in *ABE*. An adversary that holds several keys should only be able to access data if at least one of the individual keys grants access. The overhead in *ABE* scheme is that the data owner has to use every authorized user's public key to encrypt data. *ABE* is applied only in real time as it is monotonic in nature. Once the public and private keys are generated the proposed solution follows *RC4* based encryption and decryption.

A. In *ABE,* the user initially sends Id_i, pk, v1 as a request to the group manager, where Id_i is the identity value of the respective user, pk is the generated public key.
B. The request thus received helps the group manager to generate a random number *r* of size n=8.
C. The encryption is then done using AENCpk (KEY, v2) by the group manager and is stored in the local storage space.
D. The received Id_i message is compared with the identity Id_i by the group manager by decrypting AENCsk (Id_i, v1, ac).
E. And at last, the user get to decrypt the message AENCpk (KEY, v2) by using his private key in ECC obtained from private key (xi, Ai, Bi). After successful creation of account, the user becomes a group member.

V. ENCRYPTION with RC4

The mostly preferred stream cipher algorithm designed by *Ron Rivest* in *1987* is vastly famous for its use in the RSA security model. The byte-oriented algorithm generates random key-streams to encrypt and decrypt the user data. The key-stream is of size *n*=8 and the number of permutations performed is given by 2^8=256 permutations.
Thus the array is of size 256 starting from 0 to 255. It is relatively an easily approached encryption method for one of the following strengths.

A. STRENGTHS OF RC4

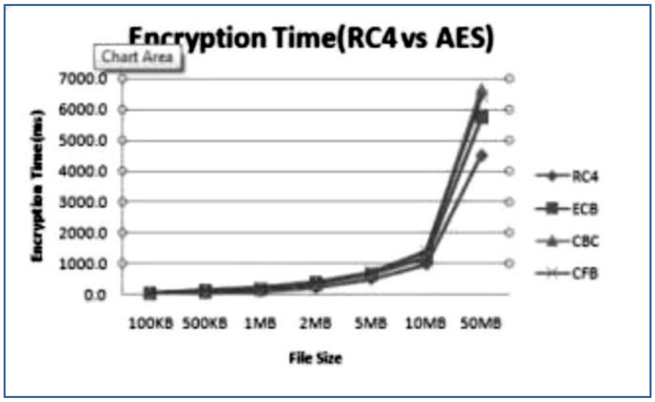
i. Encryption is of complexity *n*, i.e., O (n).
ii. It is 10 times as fast as *DES* algorithm.
iii. It generates a random key for every new session and so the past sessions cannot be tracked.
iv. The encryption and decryption take place using Exclusive-OR.

B. ADVANCED ENCRYPTION STANDARD (AES)

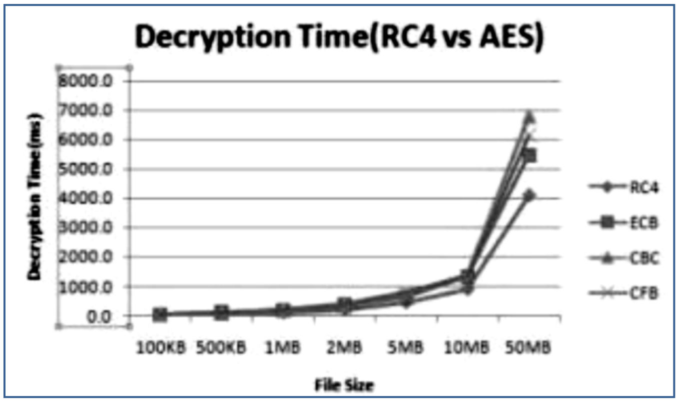
The standard *AES* proposed by *National Institute of Standards and Technology* encloses various modes such as *ECB*, *CBC*, *CFB*, *OFB*, and *CTR*. Unlike the stream cipher *RC4*, *AES* encrypts data as large blocks or chunks.

C. PERFORMANCE ANALYSIS of RC4 and AES

The *graph.1* shows the encryption time of *RC4* vs. *AES* among the various cryptographic algorithms used followed by the decryption time used by *RC4* and *AES* illustrated in the *graph.2*. These comparisons are made between various packet sizes of the file to be encrypted or decrypted

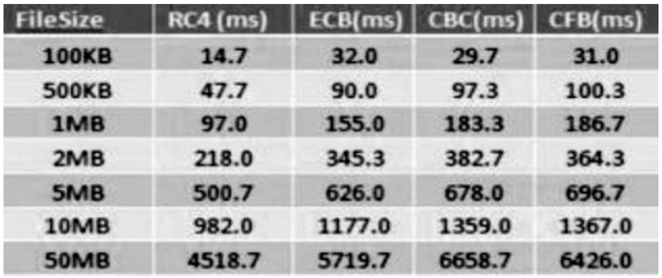


Graph.1 Encryption Time of RC4 vs. AES



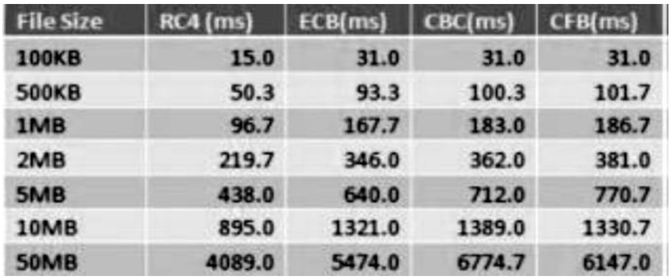
Graph.2 Decryption Time of RC4 vs. AES

The table.1 provides the plotted values of the Encryption time graph draw between *RC4* and *AES* modes of encryption in milliseconds (ms). Similarly, table.2 provides the plotted values of the decryption time noted between the *RC4* and *AES* algorithms observed among various files of different sizes.



FileSize	RC4 (ms)	ECB(ms)	CBC(ms)	CFB(ms)
100KB	14.7	32.0	29.7	31.0
500KB	47.7	90.0	97.3	100.3
1MB	97.0	155.0	183.3	186.7
2MB	218.0	345.3	382.7	364.3
5MB	500.7	626.0	678.0	696.7
10MB	982.0	1177.0	1359.0	1367.0
50MB	4518.7	5719.7	6658.7	6426.0

Table.1 Encryption time of RC4 vs. AES



File Size	RC4 (ms)	ECB(ms)	CBC(ms)	CFB(ms)
100KB	15.0	31.0	31.0	31.0
500KB	50.3	93.3	100.3	101.7
1MB	96.7	167.7	183.0	186.7
2MB	219.7	346.0	362.0	381.0
5MB	438.0	640.0	712.0	770.7
10MB	895.0	1321.0	1389.0	1330.7
50MB	4089.0	5474.0	6774.7	6147.0

Table.2 Decryption time of RC4 vs. AES

VI. SYSTEM MODULES

The system implementation is segregated into the corresponding modules.

A. Authorized User Verification
B. Image Based Authentication
C. Privacy-preserving
D. Key Distribution & Access Control
E. Detect Duplication
F. Collusion Attack
G. Secure Data Sharing
H. Cloud Storage.

VIII. FUTURE WORK AND CONCLUSION

De-Duplication in cloud groups enables various industries to remove replication of data and thus improve storage capacity. Providing the user with an image based authentication adds a security feature to user authentication making it difficult for unauthorized users to gain access to a file. Removing the need for a secure channel to distribute the encryption key makes it less complicated and provides confidentiality.

IX. REFERENCES

[1] Wenhao Li, Yun Yang, and Dong Yuan, “Ensuring Cloud Data Reliability with Minimum Replication by Proactive Replica Checking”, IEEE Transactions on Computers, Volume: 65, Issue: 5, May 2016.

[2] Tao Peng, Qin Liu & Guojun Wang, “A Multilevel Access Control Scheme for Data Security in Transparent Computing”, IEEE Trans. Computing in Science & Engineering, Vol. 19, Issue 1, 2017.

[3] Tao Jiang, Jianfeng Ma, & Xiaofeng Chen, “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”, IEEE Transactions on Computers, Volume: 65, Issue: 8, 2015.

[4] Mazhar Ali, Eraj Khan, and Revathi Dhamotharan, “SeDaSC: Secure Data Sharing in Clouds”, IEEE Systems Journal, Volume: PP, Issue: 99, 2015

[5] Rahul S. Nandanwar, Vijendrasinh P. Thakur, “Review On Secure Anti-Collusion Data Sharing For Dynamic Group In The Cloud”, IJECS, Volume 5 Issues 6, Page No. 16886-16888, June 2016.

[6] Ch. Ramesh Kumar, B. Prasanna Jyothi & Ireni Sathish Goud, “A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud”, IJMETMR, Volume 5 Issue 11, October 2016.

[7] Naresh Vurukonda & B. Thirumala Rao, “A Study on Data Storage Security Issues in Cloud Computing”, ICCC, page no-128-135, 2016.

[8] Xu An Wang, ZhihengZheng & FatosXhafa, “Identity Based Proxy Re-Encryption Scheme (IBPRE+) for Secure Cloud Data Sharing”, International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2016.

[9] Sayalee Shinde & Dr. S. S. Shaikh, “A Survey on Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud”, IJIRCCE, Vol. 4, Issue 12, December 2016.

[10] Ankita Ajay Jadhav, Poonam Doshi (Lambhate) & Mohan V. Pawar, “Anti Collusion Data Sharing Schema for Centralized Group in Cloud”, IRJET Certified Journal, Vol. 4, Issue 01, Jan 2017.