Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/99030, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Group Data Verification for Enhancing the Storage Security in Cloud Computing

Ajith Markose, S. Vigneshwari, S. Gowri and D. Usha Nandhini

Faculty of Computing, Sathyabama University, Chennai - 600119, Tamil Nadu, India; markmarkose93@gmail.com, vikiraju@gmail.com, gowriamritha2003@gmail.com, ushaduraisamy@yahoo.com

Abstract

Objectives: A privacy-preserving mechanism for public auditing of shared data in cloud storage has been proposed. This boosts up the effectiveness of the verification task which is meant for auditing multiple tasks. It also reduces the response time and auditing time and thereby improves data integrity. **Methods/Analysis:** A privacy preserving methodology has been proposed which sustains the social interaction and examination on the data which is being mutually shared across the cloud. In scrupulous, ring signatures have been utilized to enhance the verifiability of the computed metadata and to improve the accuracy of the group data analysis. The proposed system maintains the secrecy of the mutual data. The confidentiality of the specific user in the group is ensured by data filtering mechanism. This mechanism masks the user's private data from being accessed publicly across the cloud. The proposed system also supports multi-group audits simultaneously. **Findings:** A distinct privacy preserving mechanism is rarely available in the cloud storage especially for shared data. Also the personal information should not be disturbed by public verifiers. The ring mechanism shares only the verified information instead of sharing the entire file. This improves the integrity of the confidential data. The mechanism boosts the potency of substantive multi-group analysis to support the entire data cluster. This improvises the real time cloud data distribution. The identity of the signer is traceable by the group owner. **Novelty/Improvement:** Only registered users can login to the cloud. This prevents the unauthorized access to the cloud. Data is secured during cloud upload. Other users in the group have no permission to modify the data. Except the signer other users have got read-only permission.

Keywords: Auditing, Authenticators, Batch Auditing, Potency, Privacy, Shared Information

1. Introduction

The users are provided with affordable data storage[1,2]. The cloud users are intended to share data globally. Some of the group cloud storage providers are Google drive, Drop box, iCloud etc. The data stored in the cloud is subjected to scepticism and scrutinity. There is also a possibility of data loss due to human errors or package-loss[3,4]. The integrity of knowledge is subjected to scrutiny and scepticism so that the cloud data may be sometimes lost due to unexpected failures[3,4]. The users should be notified about the errors in order to avoid any data loss. The data in the cloud need to be verified prior to the data manipulation tasks. As a quality check, entire cloud storage needs to be explored and to be verified with the help of cryptographic algorithms like MD5 or RSA[8]. This process enables secured and authenticated data retrieval in the cloud. Most cloud users would not prefer to transfer the entire data from the cloud storage to their native devices.

Author in[10] created a novel application for accessing huge data set from a web service provider. The system follows semantic search mechanism for retrieving user preferred data. The personalization scheme is the

*Author for correspondence

prominent criteria which are enhanced in the proposed system.

Author in[11] proposed specific document comparison mechanism which employs multiview point clustering. The multi view data comparison aspect initiates multi group data audits in the proposed system.

Author in[12] proposed data retrieval across multi ontologies. Storage of shared social information in the cloud which is given as the future enhancement of the proposal is being considered for group data access and retrival in the cloud.

2. Materials and Methods

The user module is based on Consumer Relationship Management (CRM). CRM is a business strategy which enables the creation of rappot between the consumer and the business organization. It maintains a record of the amicability of the management with respect to the specific customer. It aims at the promotion of business through services and field support. The consumers will judge the validity of the supplier. Personalization is the key to promote business accordance with that of the consumer. CRM is the way to understand the competitive nature of the organizations. The user needs to register with the CRM system. Once registration is completed the confidential information like passwords are encrypted and stored in a separate information base. The encrypted data can be handled only by the personalized user or by the cloud administrator. Other users in the cloud group are thus excluded from the entire data storage and management. But they are provided with essential information alone.

Figure 1 gives the CRM structure with various stages of customer relationship and management.

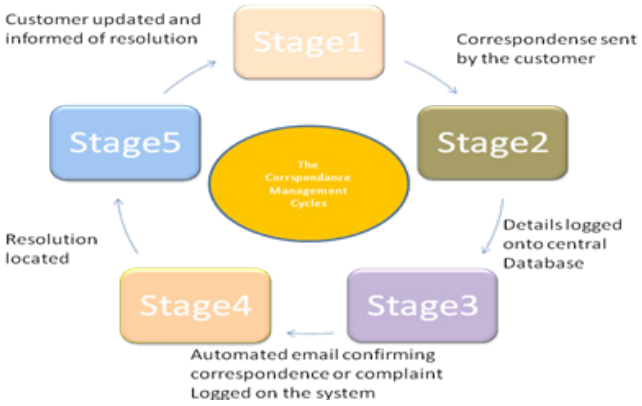


Figure 1. CRM structure.

2.1 Encryption/Decryption Service

AES is the standard block ciphering algorithm. It is an asymmetric algorithm where public key and private key are utilized for double encryption and decryption. The modern cryptographic systems uses AES algorithm. AES algorithm uses a single shared key[7,8]. This key is maintained as a secret key.

Ring signature is a group data sharing mechanism where all the users are provided access to the group with their public keys and endorse the data modifiability with the help of their private keys.

2.1.1 Description about the Algorithm

Step 1: Generate the CRM module with login credentials.
Step 2: Perfom AES encryption mechanism for data encryption.
Step 2.1: Obtain the round keys using standard key scheduling algorithm.
Step 2.2: Bitwise XOR is used to combine the state with round key.
Step 2.3: Bytes are replaced and substituted using a look up table.
Step 2.3.1: Row shifts are performed at regular intervals.
Step 2.3.2: Column mix is performed by binding four bytes per column.
Step 2.3.3: Round key is added.
Step 2.4: In final phase sub bytes are combined, rows are shifted and round key is added without column mix.
Step 3: Ring Signature is provided for group data.
Step 4: The confidential data is filtered and is modifiable only to the intended user in the group.

The encryption service module describes key selection and decryption technique for the initial information. The key selection technique is needed to store and retrieve information from the cloud, with the help of a secret key. The CRM sends the user login and authentication to the cloud server through secured encryption algorithms. Thus the data stored in the cloud becomes encrypted and confidential.

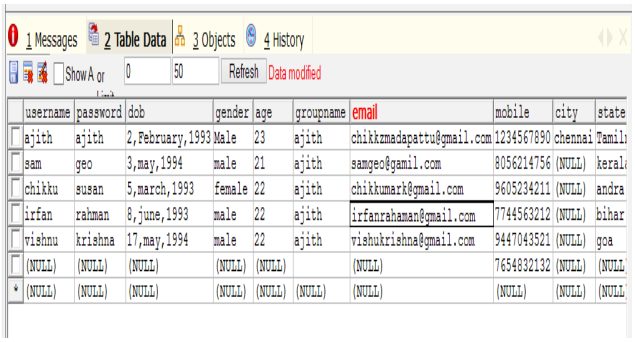
3. Results and Discussion

CRM sends the user login credentials to the cloud storage. The original data is encrypted and stored across the cloud. This data wrapping mechanism builds confidentialty to the cloud consumer community. Thus the data is protected from unethical hackers in the cloud.

Throughout the data retrieval process, the CRM plays a major roll in secured storage and retrieval thereby maintaining integrity and confidentiality. This acts like a firewall protection mechanism thanks to the advanced encryption algorithm. There is a need of personalized web data extraction. Mining huge information across the web is not an easy job. A variety of reduction techniques need to be undertaken to remove unnecessary data[5] and to grab the useful information from the web source. Ontology is the best way to define the useful information[6].

The information stored in the cloud is encrypted. When the user requests the confidential and encrypted data, the CRM asks for user secrecy credentials and checks the validity of it. Only if match is found the data is decrypted. The cloud service whether it may be a banking application or a shopping cart application is thus enhanced with encrypted data storage. Due to personalization, the search efficiency is also improved. The secured data storage and service is applicable for both ERP and CRM systems.

Figure 2 depicts the database structure of the user registration module. In Figure 2, the confidential data like email can be viewed by the other users but it can be edited only by the person with authentication credentials. This proves to be an example for group data verification.



username	password	dob	gender	age	groupname	email	mobile	city	state
ajith	ajith	2,February,1993	Male	23	ajith	chikkzmadapattu@gmail.com	1234567890	chennai	Tamil
sam	geo	3,may,1994	male	21	ajith	samgeo@gamil.com	8056214756	(NULL)	kerala
chikku	susan	5,march,1993	female	22	ajith	chikkumark@gmail.com	9605234211	(NULL)	andra
irfan	rahman	8,june,1993	male	22	ajith	irfanrahaman@gmail.com	7744563212	(NULL)	bihar
vishnu	krishna	17,may,1994	male	22	ajith	vishukrishna@gmail.com	9447043521	(NULL)	goa
(NULL)	(NULL)	(NULL)	(NULL)	(NULL)		(NULL)	7654832132	(NULL)	(NULL
(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL

Figure 2. User registration in database.

3.1 Enhancements in the Proposed System

In the proposed system, ring signatures are constructed to improve the authenticity of business transactions across the cloud. The ring signature enhancements distinguishes the confidential and non confidential information in the cloud storage to provide user specific service. The proposed system also ensures group data validation with multi task support. Tractability and personalization[6,9] are the two aspects to be considered in the development of the proposed system. Tractability deals with the discharge of authentic information only to the legitimate user. Personalization is best the way for the improvement of CRM.

Overall focus of the proposed system is as follows:

- The proposed system can perform multiple auditing tasks at identical time intervals.
- The confidentiality of group data is enhanced with ring signatures.
- High security is assured for file sharing.

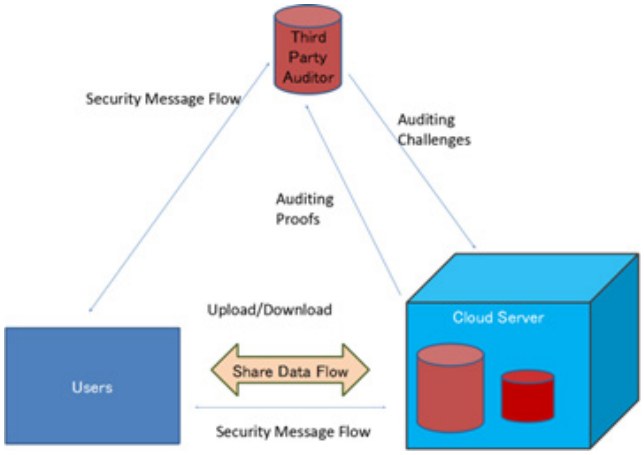


Figure 3. Architecture diagram for the proposed system.

Figure 3 gives the overall architecture of the proposed system. The user module supports both tractability and personalization. The user should prefer distinctive user id for login. The passwords are encrypted with AES and stored in the cloud. When the authenticated user requests for the confidential data, the secret key provided by the user is decrypted and mapped with the original data. Only users with secret key have the access right to modify the shared data in the cloud. Other users are provided with read only access and thus they are prohibited from unwanted modification of the owner's data. This improves the affinity and reduces the undesirable data modifications. Thus the data is safe from hackers, since the initial data cannot be traced back without providing proper secret keys. This is because of the assymetric nature of the algorithm.

A class diagram gives an over view of the entire system by showing its classes and the relationships among them. The class diagram below defines a user registration and the authentication process. The class diagram of the proposed system is given in Figure 4.

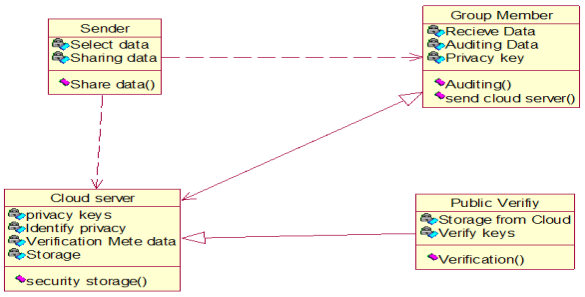


Figure 4. Class diagram for proposed work.

Sequence diagram is an interaction diagram that provides fine points about how operations are carried out, when messages are sent and what messages will be sent. The full execution of the entire process is concluded. Sequence diagrams are created according to time. The time progresses in depth as the page is moved down. The objects involved in the below process are scheduled from left to right according to their positions in the message sequence. The sequence diagram of the proposed system is given in Figure 5.

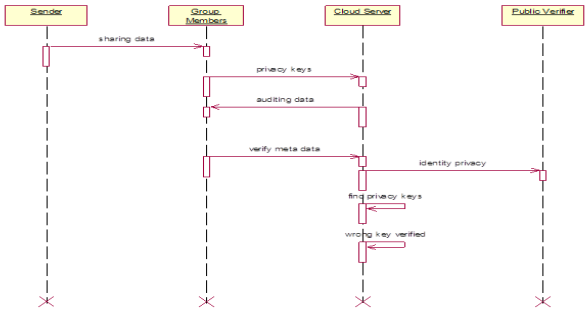


Figure 5. Sequence diagram for proposed system.

When compared with the existing public storage-retrieval mechanisms, the proposed system shows reduced response time and auditing time. Figure 6 depicts this.

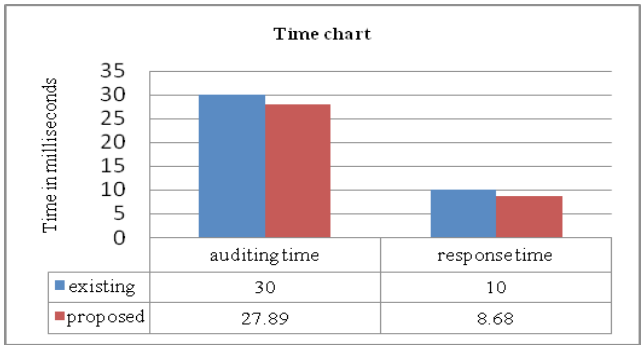


Figure 6. Time chart.

4. Conclusion

The proposed system provides a novel approach for ensuring privacy in the shared data across the cloud. Muli batch audits are the innovative preferences of the proposed system. The system also helps in improving the tractability and personalization of the confidential data stored in the cloud by utilizing ring signatures. CRM module in the proposed system improves the customer relationship thereby proving the proposed system is worth for real time confidential data storage and access in the cloud environment.

5. Acknowledgement

I would like to take this opportunity to express my profound gratitude and deep regard to Sathyabama University and Dr. S. Vigneshwari. M.E., Ph.D, for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Her valuable suggestions were of immense help throughout my project work. Her perceptive criticism kept me working to make this project in a much better way. Working under her was an extremely knowledgeable experience for me.

I would also like to give my sincere gratitude to all the friends who were involved in the survey, without whom this research would be incomplete.

6. References

1. Wang B, Li B, Li H. Oruta: Privacy- preserving public auditing for shared data in the cloud. IEEE Transactions on Cloud Computing. 2014 Apr; 2(1):46–53.
2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. A view of cloud computing, communications of the ACM. 2010 Apr; 53(4):50–8.
3. Ren K, Wang C, Wang Q. Security challenges for the public cloud. IEEE Internet Computing. 2012 Jan; 16(1):69–73.
4. Song D, Shi E, Fischer I, Shankar U. Cloud data protection for the masses. Computer. 2012 Jan; 45(1):39–45.
5. Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of the IEEE INFOCOM; San Diego. 2010 Mar. p. 1–9.
6. Vigneshwari S, Aramudhan M. Web information extraction on multiple ontologies based on concept relationships upon training the user profiles. Artificial Intelligence and

Evolutionary Algorithms in Engineering Systems. 2014 Nov; 1–8.
7. Wang B, Li M, Chow SS, Li H. Computing encrypted cloud data efficiently under multiple keys. 2013 IEEE Conference on Communications And Network Security (CNS); 2013 Oct. p. 504–13.
8. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM. 1978 Feb; 21(2):120–6.
9. Vigneshwari S, Aramudhan M. Personalized cross ontological framework for secured document retrieval in the cloud. National Academy Sciences Letters-India. 2015; 38(5):421–4.
10. Saranya R, Gowri S, Monisha S, Vigneshwari S. An ontological approach for originating data services with hazy semantics. Indian Journal of Science and Technology. 2016 Jun; 9(23). DOI: 10.17485/ijst/2016/v9i23/95145.
11. Kalpana S, Vigneshwari S. Selecting multiview point similarity from different methods of similarity measure to perform document comparison. Indian Journal of Science and Technology. 2016 Mar; 9(10). DOI: 10.17485/ijst/2016/v9i10/88903.
12. Vigneshwari S, Aramudhan M. Social information retrieval based on semantic annotation and hashing upon the multiple ontologies. Indian Journal of Science and Technology. 2015 Jan; 8(2):103–7.