RESEARCH REVIEW JOURNALS
Volume-04
Issue-09
September-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[Peer Reviewed Journal]

Secure Data Splitting Merging Techniques in Cloud Computing System

[1]G.Priya & [2]Kawsalya .S

[1]*Assistant professor Dept of computer science, Sri Ramalinga Sowdambiga College of science and commerce coimbatore (India)*
[2]*Assistant professor and head, dept of computer applications.kovai Kalaimagal College of arts and science Coimbatore (India)*

ARTICLE DETAILS

Article History
Published Online: 16 Sep 2019

Keywords
Cloud computing; security; cloud storage; encryption; data storage; secure communication.

***Corresponding Author**
Email: kskapr[at]gmail.com

ABSTRACT

Cloud computing is a fastest growing technology. It permits business organizations to use or access completely different applications, store information without access their personal files. Whereas considering the ability, stability and therefore the security of cloud one can't ignore completely different threats to user's knowledge on cloud storage. File access assure in real technique to the file protection because of untrusted cloud servers. In cloud storage system file entrance mechanism is more difficult issue. This method in consequence produces redundant copies of comparable files or involves a totally reliable cloud server. Information sharing giving security and privacy preservation are still difficult problems, particularly for an untruth cloud because of the collusion attack inside the continuous dynamical of membership progress of knowledge. It's supported the secure key distribution without assuming any secure communication channel. Cloud storage services the vulnerabilities related to cloud-related information has increased. It affects the cloud distributed information servers that are not only used for knowledge storage, but also used for managing an enormous amount of knowledge with distributed file structures in collaborative sharing. A secure re-encryption scheme of information sharing theme without assuming secure communication channel for dynamic groups inside the cloud. Planned system give guarantee for secure sharing of knowledge files after they are outsourced with double coding and particular security key distribution mechanism. Re-encryption of message provides the data security and prevents different security attacks like man in middle attack. If an attacker tries to decrypt the massage using untruth cloud, it'll not possible for them. Users can do an effective and economical method for knowledge sharing among cluster members within the cloud with efficient manner and little management cost.

1. Introduction

Cloud computing provides on demand service and process resources to the Users. it's dynamic computing style wherever dynamically scalable and frequently virtualization resources are provided as a service over the web. Fundamental service offered by cloud providers is information storage. Servers of clouds are managed by cloud providers that are not fully secured. Users could store information files on cloud which can be sensitive and confidential, like business plans. To preserve information privacy, a basic solution is to encrypt information files, then transfer the encrypted information into the cloud [1]. The most significant difficulties is identity privacy for the wide deployment of cloud computing.

Several security mechanisms for information sharing on untrusted servers are proposed. In those approaches, information owners store the encrypted information files in entrusted storage and distribute the corresponding decryption. Users may not be willing to join in cloud computing systems without the guarantee of identity privacy, because their real identities could be simply disclosed to cloud providers and attackers. Identity privacy could incur the sabotage of privacy. For instance, a misbehaved staff will deceive others within the company by sharing false files without being traceable [2]. Therefore, traceability, that permits the cluster manager to trace over the real identity of a user, is additionally extremely desirable. extremely recommended for any member during a cluster ought to be ready to absolutely access hold on information and sharing services provided by the cloud, that might be defined because the multiple-owner manner a lot of broadly, every user within the group is {ready} to not solely read information, however additionally modify their a part of information within the entire file [3]. Finally, teams are usually dynamic in apply. Modification in membership makes secure information sharing very difficult. On the opposite facet, the assorted system challenges granted from new users to find out the content of information files stored before their participation, because it's impossible for new approved users to contact with anonymous information owners, and acquire the corresponding decryption keys [4]. an appropriate membership revocation mechanism without change the secret keys of the remaining users is additionally desired to minimize the complexity of key management [5].

2. Related Work

The paper [3] summarizes the benefits of using the cloud, provides a brief clarification about the preparation and delivery models and examines very well the knowledge connected problems within the Cloud viz., cost, storage location, security and availability. The aim is to bring into limelight some of the foundational information for associations who are able to relocate to the Cloud to use this most recent worldview of computing.

The paper [4] depicts totally different classifications of problems related to security emerging from the use of services offered by cloud. The authors have talked concerning security connected challenges, for example, security related to data storage, security related to data transmission, security related to application, security for trustiness of cloud and third-part resource security. Therefore on recognize the highly vulnerable nature of cloud security, a threat's chance is to boot inferred. It'll be deduced that therefore on boost the progression of cloud computing within net, it's basic to reinforce the protection capacities.

In [7] author developed efficient and secure re-encryption theme has been planned for info sharing in unreliable cloud environment. This scheme is formed on top of Cipher text-Policy Attribute-Based encryption (CPABE), fine-grained access management to share information. That theme will do user revocation without whole cipher texts re-encryption and key re-distributions also, re-encryption is not performed till a user requests for that information, that reduces overheads. Further, it doesn't want any clock synchronization.

3. Existing System

3.1 System Design and Model

The main purpose of the proposed mechanism is to design a secure storage and accessible framework for cloud computing that will offer a greater deal of privacy, confidentially and integrity. The framework is termed as "SSM" that stands for secure splitting and Storage data in knowledge Centers. The most objective of the system style is to develop a robust, secured storage and framework to boost accessibility in cloud computing. Security design within the cloud provides a multi-cloud security structure that permits a legitimate user to store or transfer data into a distributed cloud environment and retains it for his future work. at intervals the existing mechanism a large storage capability is required that cannot be fulfilled by a personal computer because it has constraints related to every process as well as storage. The unique feature of this design is that it uses a peculiar technique of encryption as well as decryption based on distributed key technique. The system design provides huge range of services to prevent vulnerable attacks. The aim of the work carried out is to supply a sophisticated security design that allows maintaining the info secure in multiple cloud applications to authenticate the user for any rogue activities. The anticipated goals of the work are as follows:

i) Validation: A dynamic authentication performs validation of the cloud application.

ii) Secure information storage: the system should produce some split key that provides secured data storage for the valid user.

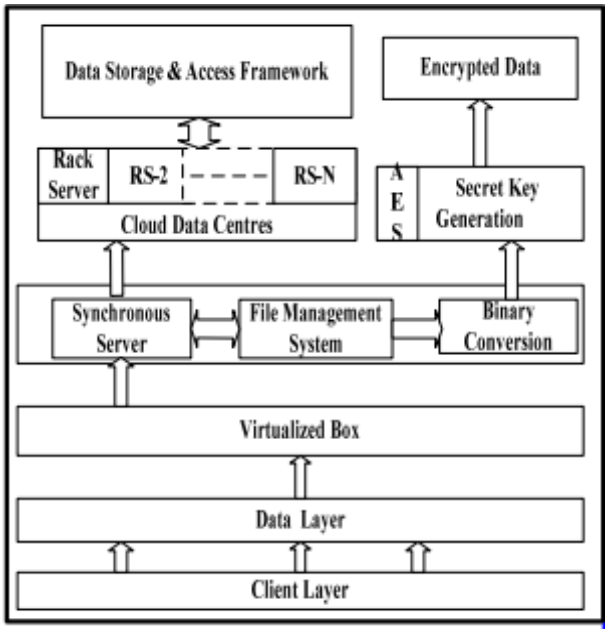
iii) Splitted key technique: The system provides splitted key method for storage of data along with splitted cipher for encryption and decryption of store and retrieval of data.

3.2 Research Hypothesis

The design of the mechanism where the design principles mostly include two important players that is customers and autonomous administrator severally. The following are the design processes of the proposed system:

i)Application Interface:

A common application interface is created using Java that permits all the essential actors (main customers) to transfer similarly as access their data. The application interface initially permits the user to endure a secure authentication policy by verifying the user ID and thus the confidential passwords of the customers. Once the validation of the user profiles is finished then, the customers enable uploading as well as accessing their personal knowledge that they choose to store on the cloud storage. Whenever the user wants either uploading or accessing their hold on knowledge and it is a dependency on the next component called as Synchronous Servers.



ii) Synchronous Servers:

The unique aspect of the proposed design principles is that the original information uploaded by the users isn't directly reposited on the cloud storage. The proposed system introduces a middleware system known as Synchronous Servers that creates its file systems and stores sequences of the customer's information. The synchronous server handles the autonomous information management system for multiple customers on a given cloud. The Synchronous Server is needed to maintain proper indexing of the client's file. Once Synchronous Server processes the file, the system performs two simultaneous. The outcome of the Synchronous Server component is that the indexed file with a particular file formats with an array to store the ordering of the data uploaded or requested by the online customers. The processed information undergoes encryption using lightweight cryptography.

iii) Lightweight Cryptography:

The term light-weight refers to adopt such a cryptographic technique, that isn't only faster in performing for each encryption/decryption, but also occupies less memory. However, directly it does not method information from Synchronous Server for encryption. The processed information from Synchronous Server is converted to binary values, those results in generation of a 128-bit secret key. The next step is to perform cryptography of the binary information with AES algorithm. For implementation, AES is chosen as i) it supports faster computation and ii) it's less liable to majority of the lethal

attacks on net with 64 bits. Once carrying out the encryption using AES rule, the system results in the encrypted version of the binary information, for information splitting process.

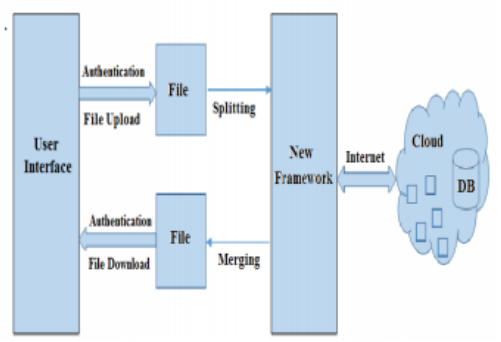
iv) Data Splitting:

This component handles splitting the information to the various data centers supported the availability of the rack servers. The core system connecting to the application interface also maintains a matrix for the information centers with the provision of the rack servers on the cloud. The system then splits the processed information of all the gross active customers supported the quantity of accessible rack servers. This method of knowledge splitting could also be illustrated as under. If there are 10 petabytes of the processed information, the information are going to be spitted as three petabytes, a pair of petabytes, 1 petabyte, 3 petabytes, and one petabyte, if there's accessibility of 5 rack servers at a given time instant. One in each of the distinctive aspects of the projected system is that the generated secret secrets encrypted with AES rule and is hold on randomly on the selected rack servers that are found to be on the market at that point instant. The system also provides higher service by storing the key inside the network that's fully unknown to the user further as administrator. Hence, the system performs storage of the client information in extremely distributed and secured manner.

4. Proposed System

The user is to provide data for storage over the cloud. During this the user has the option to encrypt the information if he desires to before uploading the same. This adds another layer of security to the users' data. When this point the user will transfer the Encrypted data to the Cloud. While doing identical, the user provides the value of Confidentiality, Integrity and availability. When user sends request together with username to access the information to cloud provider, the cloud provider first checks the user knowledge. Now the user has to enter into the information received for authentication, and when authentication access to the information will be provided.

4.1 Architectural Design



File content splitting: - This module used for splitting the content of file. It takes the file as its input. By using the user defined function it split the content of file in many elements is that the output of this module. File split uses the open operate is to open the file and file is divide into many elements using floor function. It also wants range of parts to be dividing as specified in program.

File storing:-This module used for store the split content of file randomly in different places. It takes the input from the „File content cacophonic module" the content is split in many elements module store it randomly in different places in the cloud storage.

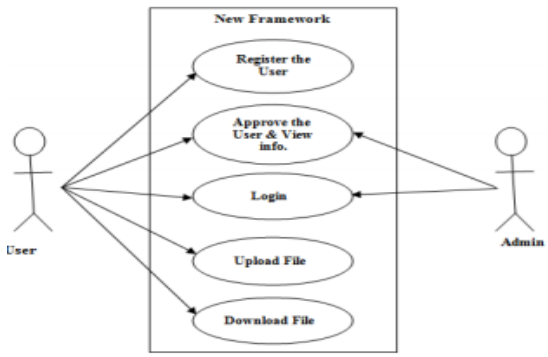
File security:-This module generates the accessing key for the user and sends to user. The generated key is utilized in the login of the user. Key confirms the user authentication.

File merge & download:- This module merges all spitted data of specific file. And it give authentication when retrieve file. It using hash operate and key for it. Only authenticate user download the merged files.

The target is to provide data security of cloud and their authentication techniques. The cloud knowledge security technique uses the symmetric encryption and asymmetric encryption algorithms with their strong authentication techniques. The use of relevant algorithm deals with the level of data safety in cloud as a result of knowledge security in cloud computing is a serious issue because the data centers are located worldwide. Authentication is that the most essential procedure to confirm the cloud knowledge during a secured manner. However, strong user authentication is that the main requirement for cloud computing that reduces the unauthorized user access of information on cloud. Knowledge security could be a lot of important issue of cloud computing. Symmetric algorithms are AES and asymmetric algorithms are Daffier Hellman and ELGamal. The Authentication techniques are one time password. Therefore a hybrid technique that could be a combination of those encryption techniques and authentication technique offers a lot of excellent and strong security on cloud data.

Use Case Realizations

- Use case diagrams are used to visualize, specify, construct, and document the behavior
- Of the system, during requirement capture and analysis.
- A use case is a contract of an interaction between the system and an actor.
- Provide a way of developers, domain experts and end-users¬ to communication.
- Serve as basis for testing.



- Use case diagrams contain use cases, actors, and their relationships use case.
- Use cases specify desired behavior.

- A use cases is a description of a set of sequences of Actions, including variants a system performs to yield an observable result of value to an actor.
- Each sequence represents an interaction of actors with the system.

This use case realization contains three parts User, Framework and Admin. In the first part user can register his info in framework page. Once registering admin will verify the user profile. Once verification user will login into the system. Then system shows successful registration notification. If user will enter with success then he will transfer his document or transfer the document.

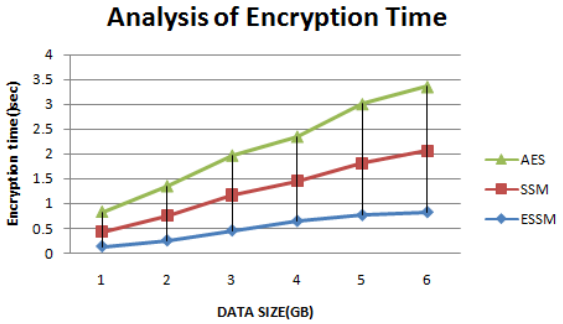
Advantages:

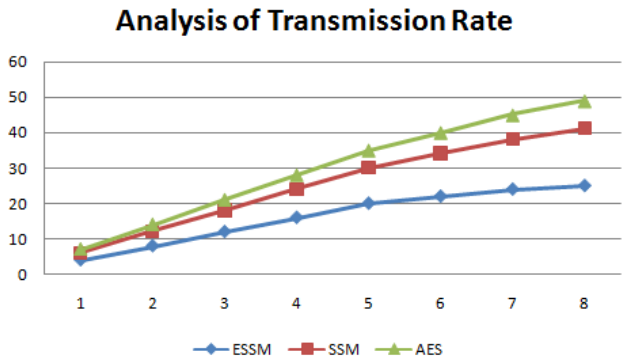
- Provide authentication.
- Data Security.
- Restrict direct access of files.
- The detection of masquerade activity.
- Data confidentiality.
- Efficiency.

5. Result

Comparing to existing computerized system, our system is gives more security and also System gives better user friendly environment for the users.

- Accurate information is available.
- It provides chances of such types of errors are much low and Provides security to the system & user data. User can easily work in project.
- Admin can decide and verify the registered user is Authorized or not authorized to access system.
- The most important is our system will provide more security to text files, i.e. the original file can split into different parts and store it into different location, when user may wish to download files user can download the original file hence it will provide the more security to the user data.





6. Conclusion

All the sharing files are secured keep in Cloud Servers and therefore the entire session key are protected. Cloud Servers" aid based file to dynamically change group key combine once there're group members leaving or change of integrity the group, the scheme will still do well which can delegate most of computing overhead to Cloud Servers without disclosing any security information. From the security and performance analysis, the scheme can achieve the planning goal, and keep a lower process quality and communication overhead in every group members" side.

Reference

1. Wang Cong, Wang Qian, RenKui, Cao Ning and Lou Wenjing , "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on ,vol.5, no.2, pp.220-232, April-June 2012.
2. Hsiao-Ying Lin; Tzeng, W.-G.; , "A Secure Erasure CodeBased Cloud Storage System with Secure Data Forwarding," Parallel and Distributed Systems, IEEE Transactions on , vol.23, no.6, pp.995-1003, June 2012.
3. Mahmood Z. Data location and security issues in cloud computing. InEmerging Intelligent Data and Web Technologies (EIDWT), 2011 International Conference on 2011 Sep 7 (pp. 49- 54). IEEE.
4. Meetei MZ, Goel A. Security issues in cloud computing. In Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on 2012 Oct 16 (pp. 1321-1325). IEEE.
5. W. Ren., L. Yu., R. Gao., F. Xiong., "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing", TSINGHUA Science and Technology, Vol. 16, No. 5, pp. 520-528, 2011.
6. X. Dong., R. Li., H. He., W. Zhou., Z. Xue., and H. Wu., "Secure Sensitive Data Sharing on a Big Data Platform", TSINGHUA Science and Technology, Vol. 20, No. 1, pp. 72-80, 2015.
7. NazatulHaque Sultan &Ferdous Ahmed Barbhuiya, "A Secure Re-Encryption Scheme for Data Sharing in Unreliable Cloud Environment,"978- 1-5090-2616-6/16 © 2016 IEEE
8. Kulkarni P, Khanai R. Addressing mobile Cloud Computing security issues: a survey. In Communications and Signal Processing (ICCSP), 2015 International Conference on 2015 Apr 2 (pp. 1463-1467). IEEE.
9. Arjun U, Vinay S. A short review on data security and privacy issues in cloud computing. InCurrent Trends in Advanced Computing (ICCTAC), IEEE International Conference on 2016 Mar 10 (pp. 1-5). IEEE.

10. H. Xiong., X. Zhang., D. Yao., X. Wu., and Y. Wen., “Towards end-to-end secure content storage and delivery with public cloud”, In Proceedings of the second ACM conference on Data and Application Security and Privacy, pp. 257-266, 2012.
11. P. Gasti., G. Ateniese., and M. Blanton., “Deniable cloud storage: sharing files via public-key deniability”, In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, ACM, pp. 31-42, 2010.
12. S. Kamara., C. Papamanthou., and T.Roeder, “Cs2: A searchable cryptographic cloud storage system”, Microsoft Research, Tech Report MSR-TR, Vol.58, 2011.

