An Effective Security Mechanism for on Demand File Storage in Cloud Computing

Anurag Raii[1*], Mayank Aggarwal[2], Anju Malik[3]

[1]Registrar, College of Engineering Roorkee, COER, Roorkee, Uttarakhand, India
[2]Professor and HOD, Department of Computer Science, Gurukul Kangri Vishwavidyalaya, Haridwar, Uttarakhand, India
[3]Assistant Professor, Department of MCA, COER, Roorkee, Uttarakhand, India
*Corresponding Author: rai_anurag@hotmail.com

Abstract: Cloud Computing is one of the recent efforts in delivering computing utilities as a service feature. Cloud services include all the applications and utilities that are provided to the user through the system software which runs on the different datacentre. These data centres include multiple virtual machines and their associated hardware. It represents immigration from computing utility in the form of a service that is delivered to the customers over the Internet through Cloud environment. Cloud is a subscription based service pattern where one may obtain resources according to the requirements and a user can decide the sensitivity of the file before storing. This paper discusses the security layer provided to the file which is stored in the cloud.

Keywords: Cloud computing, CSP, Data security, Cryptography.

I. Introduction

Cloud computing provides the facility to different service model and users to deploy their application fast, remove the problem of scalability and achieve benefits from reducing cost and pay only for the dedicated services. On the other hand customers can enjoy the services according to its need. The services may be grown and shrink as the requirements of the user. The service model of cloud Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) greatly enhances the popularity of big ventures like Google Apps, Amazon online move plan, S3 services and IBM Watson commercial products. In spite of this rapid growth, the remarkable features of cloud and the flexibility introduce multiple hurdles to cloud environment in the security aspect. It includes scalability, lock-in, isolation, privacy and dependency on CSP (Cloud Service Provider). The security mechanism should be the combination of cryptographic methods, user credentials and different key combination. Sometimes when a user is availing the services of a particular CSP then it depicts the dependency of user on service provider. For example, if a user changes from a CSP to some another CSP then it is not guaranteed that all details and credentials are deleted from the first provider. It would be used as a malicious use for the referenced user [3].

One of the major research issue on cloud security is still in the evolving step, and there in no standard model or methods that has been yet derived to attain the full security.

II. Definition

The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects. This definition describes cloud computing as having five essential characteristics, three service models and four deployment models [5]. The essential characteristics are:

i. *On-demand Self-service*: Computing resources can be acquired and used at anytime without the need for human interaction with cloud service providers. Computing resources include processing power, storage, virtual machines etc.
ii. *Broad Network Access*: The previously mentioned resources can be accessed over a network using heterogeneous devices such as laptops or mobiles phones.
iii. *Resource Pooling*: Cloud service providers pool their resources that are then shared by multiple users. This is referred to as multi-tenancy where for example a physical server may host several virtual machines belonging to different users.
iv. *Rapid Elasticity*: A user can quickly acquire more resources from the cloud by scaling out. They can scale back in by releasing those resources once they are no longer required.
v. *Measured Service*: Resource usage is metered using appropriate metrics such as monitoring storage usage, CPU hours, bandwidth usage etc.

As the framework has been changed from traditional client server architecture to cloud computing environments, the security

issues which are prevailing in the traditional environment are not sufficient for application of data in cloud environment. Now the boundaries are not confined to server or client. The nature of flexibility, combination of multiple heterogeneous network and openness nature introduced multiple threats to the security such as:

A. Scalability

The multiple resources in the cloud are shared by many users at the same time. As the numbers of users grow, it becomes complex to handle the multiple request and adjust in the computer model. Horizontal cloud scalability is the ability to connect and integrate multiple clouds to work as one logical cloud. Vertical cloud scalability is the ability to improve the capacity of a cloud by enhancing individual existing nodes in the cloud.

B. Interest Conflict

Different service model provides combined approach to different user. It may sometimes introduce a conflict in the interest of user. It is seen that because of invariant combination datamay be lost or robbed.

C. Virtualization

The concept of cloud is based on virtualization techniques. But it may produce some conditions that are not suitable for a user. As a single application may run on multiple machine, the whole or a part of data may be robbed by the intruder.

D. Velocity of Data

The openness nature of cloud may produce massive amount of data. As this data grows in exponential rate, it is a high challenging job to handle such data and provide security in the form of security as a service.

III. Current Security Solutions for Data Security and Privacy Protection

A number of methods have been introduced by big ventures of Information Technology firm and research laboratories which are related to the security and privacy. The classical approach which is just followed is the encryption and digitization trends. But as the data and nature of framework has been changed, it leads to issues related to openness nature and big data concepts like Map Reduce and Hadoop performance parameters. First IBM introduced a homomorphism encryption [1]. The data is stored in cipher text but it is used without decryption. The main problem in traditional security standard is the management of the key i.e. public key and private key. And the particular key must be secured between sender and receiver.

The service level agreement and privacy protection technology leads to differential standards that controls the flow and data generation. It calculates the stages in the processing of a file and stores it on the cloud [5].

It is a hectic job for Cloud Service Provider to maintain and manage multiple keys of various users. The Various International Organizations like the Organization for the Advancement of Structured Information Standards (OASIS), NIST and IBM Research centre are trying to solve these issues [6].

The virtual machines are responsible for processing the files. This is in fact not the job of a single process to handle all activities. Data Integrity makes the combined approach of verification, data communication, transferring, cost factor and finally the downloading of the key from the verified user. Public cloud on an extent can follows this approach up to a certain level.

Cong Wang in a research paper provides a mathematical model of the verification of data and Integrity. This aspect is highly related to storage and multiple stages of its uses. The model can be trusted as it is focused on user stages and cloud service provider [8]. The main focus is on pre computation of the fine grained values. These values are then combined with graph amortization, root analysis and verifier signature of the agency.

Data Security basically concerns for CIA (Confidentiality, Integrity, Accountability). The challenge of data privacy is the online observation of shared data. This paper proposed a framework which is based on the accountability. Here the type of data and type of users are identified. Agents are observing the accessibility options like the means and the type of data and set of users. When any scrupulous conditions exist, then the agent defines a set of methods to hold the appropriate actions.

Apart from the above mentioned approaches, the security in cloud is the combined approach which may have so many loopholes because these frameworks are not bounded to some particular criteria. Growing need of Internet and data size makes it more complicated to accomplish.

IV. Security Model

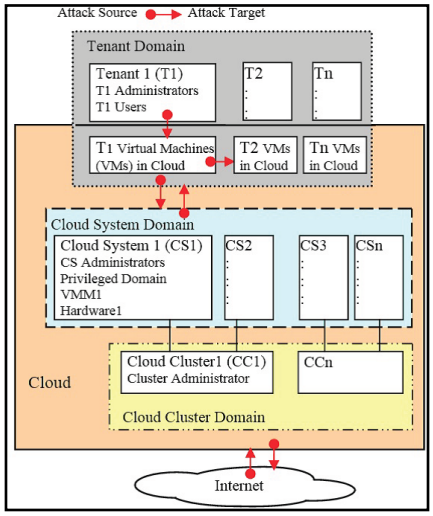

Fig. 1: Security Model

The security model consists of layered architecture of different steps. CSP have the information of administrative rights, information of the user and tenants. Cloud providers are the peer entities which are involved in the each activity of whole architecture. The threat model looks at the different attacks that have the measured attack and counted value.

V. Proposed Methodology

To achieve the secure data storage in the cloud, we use an effective technique to perform secure data storage in the cloud server. This technique allows data owners to securely store their data files in the cloud server. Initially the user sends a file storage request to store a file in a cloud server provider (CSP). They will check the file if it is blank file and checking the file space and availability of cloud server also check if the input file is confidential sensitive file or normal file if it is a sensitive file then it will be split and store in a different cloud if is a normal file then it will be assigned in a single cloud. The sensitive data retrieval needs an encryption process. If the data owner stores the sensitive data to cloud server, the data owner will encrypt their document in the proposed method. Here the double encryption technique is used to encrypt the user document. Here RSA and Optimal Elliptic Curve Cryptography (OECC) algorithm is used to encrypt the documentwith high security. Here cuckoo search algorithm is used to identify the optimal key in ECC. The research also proposes a novel cryptography approach for delivering mass distributed storage by which users' original data cannot be directly reached by cloud operators.The proposed method will be implemented in Cloud simulator which is a working platform based on Java language. Our proposed work will give better securable data storage with solving the security issues.

Difference between previous research and proposed research.

- File storage on cloud environment introduces security concerns. Data confidentiality is the issue which inculcates the observation of data in online manner. It is observed that it is equally important to provide security for the stored data.
- The service model of private cloud is useful as well as hazardous to the user because data is equally available to all technical people of insider as well as network hacker. Service also involves in the transmission, processing and storage of data.
- The main two issues in data storage server is the user feasibility towards the services available in cloud environment and availability of application to the user. It is also an overhead to unnecessary encryption of the data without any modification.
- In our previous research the encryption process is to be performed with the aid of RSA-ABC algorithm for encryption process but in our proposed research we are utilizing a RSA and ECC algorithm with the aid of this algorithm to encrypt the document in high security [13].
- In our proposed research it allows data owner to securely store a file in a cloud server provider and the ASP checks whether the file is confidential sensitive file or normal file and if it is sensitive means then it will be split and stored in a different cloud and if it is normal then it will be assigned in a single cloud. If this procedure is not followed it will reduce memory space.
- The proposed attribution system can efficiently add or revoke users. To reduce the computational cost of the proposed method, here we have to split the information and store them in two different servers.

VI. Conclusion

Cloud Computing is an environment which is the need of today's computing era. It is gaining popularity in spite of its some lacking security features. If its security concerns are fulfilled then it will be in more growing stage. This paper proposes a security layer to the files which is stored in the cloud. A user can also decidewhether the file is sensitive or not. Multiple virtual machines are used in storing a single file that will enhance the security of the file.

References

[1] J. Chen, Y. Wang, and X. Wang, "On-demand security architecture for cloud computing," *Computer*, vol. 45, no. 7, pp. 73-78, July 2012.

[2] D. Chen, and H. Zhao, "Data security and privacy protection issues in cloud computing," *International Conference on Computer Science and Electronics Engineering, ICCSEE*, 23-25 March 2012.

[3] B. Prince, "IBM discovers encryption scheme that could improve cloud security, spam filtering," *eWeek*, June 2009. Available: http://www.eweek.com/security/ibm-discovers-encryption-scheme-that-could-improve-cloud-security-spam-filtering

[4] I. Roy, H. E. Ramadan, S. T. V. Setty, A. Kilzer, V. Shmatikov, and E. Witchel, "Airavat: Security and privacy for MapReduce," In *Proceedings of the 7th USENIX Symposium on Networked Systems Design and Implementation,* USENIX Association, San Jose, pp. 297-312, April 2010.

[5] T. Cox, S. Saha, and R. Lockhart, "OASIS Key Management Interoperability Protocol (KMIP) TC,". Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

[6] K. Zeng, "Publicly verifiable remote data integrity," In *Proceedings of the 10th International Conference on Information and Communication Security (ICICS)*, Springer, Berlin, Heidelberg, pp. 419-434, 20-22 October 2008.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," In *17th International Workshop on Quality of Service (IWQoS)*, pp. 1-9, 13-15 July 2009.

[8] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW)*, ACM, pp. 43.54, 2009.

[9] V. M-Mulero, and J. Nin, "Privacy and anonymization for very large datasets," In *Proceedings of the 18th ACM Conference on Information and Knowledge Management (CIKM),* pp. 2117-2118, November 2009.

[10] R. Gajanayake, R. Iannella, and T. Sahama, "Sharing with care: An information accountability perspective," *IEEE Internet Computing*, vol. 15, no. 4, pp. 31-38, July-August 2011.

[11] National Industrial Security Program Operating Manual (NISPOM), February 2006.

[12] R. Kissel, M. Scholl, S. Skolochenko, and X. Li, "Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology," NIST Special Publication 800-88, September 2006.

[13] A. Malik, and V. K. Jain, "Effective renewal and signing method to achieve secure storage and computation using Hybrid RSA-MABC algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 9, no. 3, pp. 11-20, 2006.