Two ways Verification for Securing Cloud Data

Manisha A. Pradhan[1], Pratiksha P. Bhagat[2], Prajakta U. Bakhade[3]

[1,2,3] Student, Department of CSE, Des'scoet, Dhamangaon Rly, Maharashtra, India

---***---

Abstract - *Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. The management of the deployed applications can also bring three major challenges as network feasibility, computational feasibility and data security. After the application is pushed to the cloud infrastructure, the additional persuasion of security auditing must be integrated in order to protect the data. Various research attempts are made towards enabling the auditing features on the cloud based data by various researchers. Nevertheless, the complexity of the audit process proven to be the bottleneck in improving performance of the application as it consumes the computational resources of the same application. The proposed framework demonstrates a significant reduction in the computational load on the cloud server, thus improves the application performance leveraging the infrastructure use.*

Key Words: Cloud Storage, Data Security, Two-Way Security, Consumer Security, Computation Cost Reduction.

1. INTRODUCTION

Cloud computing refers to provision of computational resources on demand via a computer network. cloud computing provides various services which includes software as a service, platform as a service, infrastructure as a service. In traditional model of computing, user's computer contain both data and software; while in cloud computing there is no need to contain data and software only the system needs operating system and web browser. Cloud computing provides various advantages which include economies of scale, dynamic provisioning, increased flexibility, low capital expenditure and many more[1]. As cloud computing share resources over the network, security is the basic concern. Data owners store their data on external servers so data confidentiality, authentication, access control are some of the basic concerns. To protect user's privacy one way is to use authentication technique such as username and password. Authentication is to check user's identity, means whether the person is same as he pretends to be. There are various authentication methods and techniques[2]. It is also important to secure the access to all IT system and services. Access control is a procedure that allows or denies access to a system or services. In this paper an efficient access mechanism using capability list is introduced. The identification of user's are done using an extra security layer i.e. two factor authentication mechanism in order to provide cloud access. The data are outsourced to cloud after encryption with symmetric key by the data owner. Considering the recent growth in the space of computing with the introduction of cloud computing, Internet-of-Things, Grid Computing, Internet and information security, the newer dimensions are introduced for research.

The notable work outcomes M. Armbrust et al on cloud computing, M. Whaiduzzaman et al. on vehicular cloud computing, P. M. Mell et al. on NIST, G. Han et al. on routing algorithms and T. Qiu et al. on IoT have motivated number of research enthusiast in the recent era. With the introduction of cloud computing, the industry received a huge attention due to the benefits and advantages. Various companies, ranging from small to minimum to large enterprises migrated their applications on the cloud. Some companies migrated their data on the cloud due to the large size of the data and high cost of the dedicated storage facilities. The work by M. Ali et al. has demonstrated the challenges of storing data on the cloud and security issues. The practical approaches of the security implementations are discussed by T. A. Velte et al., which enabled the research dentations for various researchers. The trend followed by Z. Xia et al. by proposing rank based search scheme over encrypted data, Z. Fu et al. by demonstrating personalized search operations over encrypted data and again with Z. Fu et al. by secure searching operations on cloud data. Nevertheless, the data owners demand for the continuous proof of the correctness of the data so that the consumers of the data can receive the secure and correct data from the services. A number of research attempts are been made to ensure the remote monitoring and auditing of the data. Few distinguished work established the thought to ensure the correctness with data integrity verification by Y. Ren et al on provable auditing of data, B. Chen et al. on remote verification of the data based on network coding and G. Ateniese et al. on prevention of untrusted access of the data.

Firstly, it is to allocate computational loads in optimal among the data processing and security features. Secondly, as third party companies host the data, hence the protection is also the responsibility of that company and the data owner company need to decide upon the access of the data to the service provider. Thus, building the public auditing system with the benefit of preserving the privacy of the data is the major goal of this work. Additionally, this work also proposes a method to collect and store the access history for further statistical analysis.

2. RELATED WORK

- **Ateniese et al.[3]** proposed a proxy re encryption technique which is a secure distributed storage scheme. The blocks of content are encrypted by data owner with symmetric content keys. The content keys are all encrypted with a master public key. Master private key and user's public key are used to generate proxy re-encryption keys by the data owner, using which the semi trusted server can then convert the ciphertext into plaintext for a specific user.

- **Zhoa et al.[4**] proposed a progressive elliptic curve encryption scheme. In this pieces of data are encrypted number of times using multiple keys and later decrypted using only one key. The main problem with this technique is that it requires data owner to be online at all times.

- **Miklau et al.[5]** proposed a framework for access control on published xml documents. This can be accomplished by using different cryptographic keys over different portions of xml tree. They also presented metadata nodes in the structure to enforce access control.

- **Bennani et al.[6]** proposed a model in which the database is replicated in cloud n number of times where n is the number of roles. When a role is revoked access rights, the database is removed. This leads in the worst case to the creation from scratch a new view and re-keying the corresponding database. The main problem with this model is that it is infeasible to implement due to high redundancy.

- **Naor et al.[7]** presented symmetric key primitives in an untrusted storage environment. This scheme is based on pre-keydistribution mechanism using scheme. This reduces the public key cryptography in software as a service model. The performance of the schemes are not evaluated in this model.

- **Weicao wang Z.Li et al.[9]** suggested to encrypt every data block with a different key so that flexible cryptography based access control can be achieved. The owner needs to maintain only a few secrets through the adaptation of key derivation methods but scheme for key management is not mentioned.

- **Zhou [10]** carried out study on privacy and security, work that can be done to prevent privacy and security breaches and outlines that security laws should also be taken into consideration

The cloud based data is generally accessed by the data owner, data consumers or the customers of the data owner, third party auditors and finally the cloud service provider. The owner is fully trusted in this scenario and it is the responsibility of the cloud service provider to ensure the security of the data while being accessed by the consumers. Nevertheless, the third party auditor and the cloud service providers can also access the data, while being partially trusted by the data owner. In such scenarios the challenge of data being accessed by any attacker in terms of audit information and statistical information of the cloud service provider is non-valuable. Thus making this model challenged by the researchers and demands improvements.

Secondly, the prime disrupt of these models are to consume the computational capacity of the cloud servers. The cloud server are configured to cater the consumer and data owner demands for higher loads, but the added computational processing for the security and auditing always tend to reduce the performance.

A. Evaluation of Generic Model

The above discussed model is the most popular existing framework [Fig – 1] in spite of the arguments for security.

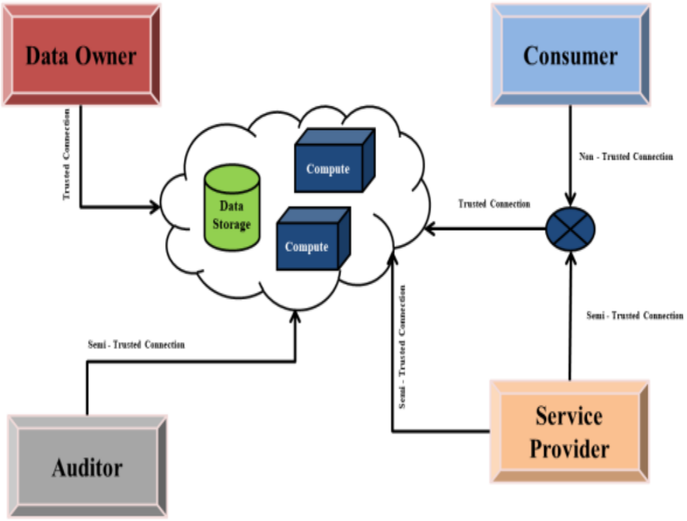

Figure 1: Three Party Verification and Cloud Data Security Model

The generic model is an association of the data owner, third party auditor and service provider. Along with these three parties, the consumer of the data is also to be considered. The first party, being the data owner, always can establish the secure and trusted connection to the data. In the other side, Auditor and Service Provider can also establish the connection to the data but those connections and access requests are considered to be the semi-trusted connections. Finally, the connections from the data consumers are completely untrusted and it is the responsibility of the cloud service provider to reduce the risk of unauthorized access by verifying the connections.

3. PROPOSED SYSTEM

The major identified drawbacks of the existing systems are semi-trusted access by the third party auditors and upon introducing the security measures for the auditor access to the data, the increase in the computing load on the cloud servers. Hence, this work proposes a two way security mechanism for cloud based data separately for data consumers and auditors based on different key based accessed. In this section, this work elaborates the two ways key based mechanism and also furnishes the comparative study in order to demonstrate the performance improvements [Fig – 2].

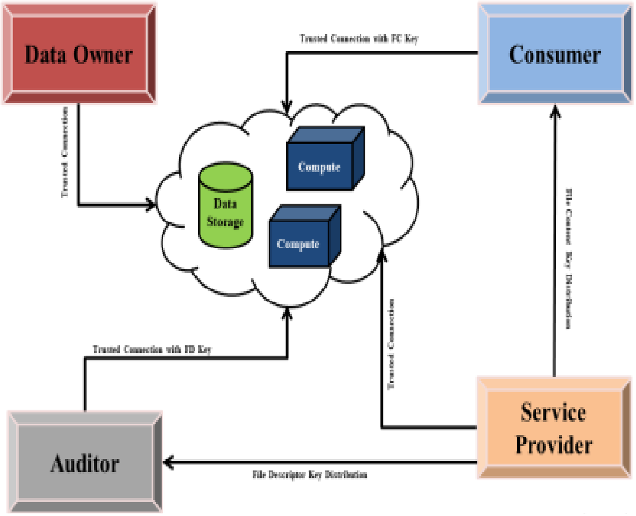
Data Owner
Consumer
Trusted Connection with FC Key
Trusted Connection
Compute
Data Storage
Compute
File Content Key Distribution
Trusted Connection with FD Key
Trusted Connection
Service Provider
Auditor
File Descriptor Key Distribution

Figure 2: Proposed Two Way Cloud Data Security Model

The proposed model algorithm is divided into four parts as generate the keys, upload the files with key based encryption, access request validation and finally the data decryption.

Step 1. Generation of the keys

Algorithm Part – 1: Key Generation

1. Randomize two prime number selection as A & B, where A is greater than B

2. Calculate the product of two prime numbers as K = A * B

3. Consider a random polynomial of order N as $\gamma(N)$

4. Calculate the intermediator of the key as $\gamma(N) = (A-1) * (B – 1)$

5. Calculate the public prime component as E such that GCD $(E, \gamma(N)) == 1$

6. Generate the Public Key PK as PK = $(E, \gamma(N))$

7. Generate the File Descriptor Private Key as FDPvK = $(D1, \gamma(N))$, where $D1 = E\gamma(N) / | \gamma(N)|$

8. Generate the File Content Private Key as FCPvK = $(D2, \gamma(N))$, where $D2 = \gamma(N)E/ | \gamma(N)|$

Nevertheless, the key generation algorithm can be replaced by any proprietary encryption and decryption algorithm in general and the modified algorithm will not change the performance improvements of this proposed framework.

Step -2. Encryption of the file data and uploading of the file

Algorithm Part – 2: Encrypt and Merge for Upload

1. Segregate the file descriptor and the file content as consider as FD and FC respectively

2. If FD is not encrypted, then encrypt with PK & FDPvK, else continue to the next part

3. If FC is not encrypted, then encrypt with PK & FCPvK, else continue to the next part

4. If FD & FC both are encrypted, then merge the encrypted FD & FC and upload the file to the cloud storage

Once the files are uploaded on to the cloud, then the access requests can be accepted and process for the validation

Step -3. Access request validation

Algorithm Part – 3: Access Request Validation

1. If the access request is been made for the auditing access, then verify the request with the key combination of PK & FDPvK.

2. Once, the verification is valid, and label the request as FDR. Else terminate the request.

3. Else If the access request is been made for the data access, then verify the request with the key combination of PK & PCPvK

4. Once, the verification is valid, and label the request as FCR. Else terminate the request.

This step will significantly reduce the computational overload of the security process and also ensure semi-trusted access to the core components of the cloud data.

Step -4. Decryption of the file

Algorithm Part – 4: Decryption of the Content

1. If the requester label is FDR, then process the file descriptor and decrypt.

2. Else If the requester label is FCR, then process the file content and decrypt file descriptor and content both.

4. CONCLUSION

This paper presented a set of security procedures to secure the data of a data owner in cloud. The combined approach of access control and cryptography is used to protect outsourced data. The acceptance of the cloud computing is due to the nature of the applications and services to be scalable during the fluctuation of the demands. This characteristic alone gained a lot of popularity and acceptance of cloud computing. This proposed method not only enhances the security measures, also demonstrates the reduction in response time as far as the encryption and decryption is concerned. This improvement will certainly help the researcher community to rethink on the security protocols those are used and predict the newer research dimensions.

5. REFERENCES

1. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage”, ACM Transactions on Information and System Security, Vol. 9, No. 1, Feb 2006, pp. 1-30.

2. Zhao G, Rong C, Li J, Zhang F, Tang Y (2010) “Trusted data sharing over untrusted cloud storage providers” IEEE second international conference cloud computing technology and science(CloudCom) 2010, pp 97–103.

3. G. Miklau, and D. Suciu” Controlling access to published data using cryptography”, Proc. 29th VLDB, Germany, Sept 2003, pp. 898-909.

4. Bennani N, Damiani E(2010)” Towards cloud based key management for outsourced databases” IEEE 34th annual computer software and application conference workshop 2010 pp. 232-236.

5. Dalit Naor, A. Shenhav, and A. Wool” Toward securing untrusted storage without public-key operations”, Proc. 2005 ACM Workshop on Storage Security and Survivability (StorageSS), Virginia, USA, Nov 2005, pp. 51-56.

6. Rolf Blom, “An optimal class of symmetric key generation systems”, Proc. Eurocrypt 84 workshop on Advances in cryptology: theory and application of cryptographic techniques, Springer Verlag, NY, USA, 1985, pp. 335- 338.

7. Weicao wang Z.Li "On Securing untrusted clouds with cryptography”,Proceedings of the 9th annual ACM workshop on Privacy in the electronic society.,ACM, 2010.

8. Zhou M, Zhang R, Xiew, Qian W, Zhou A (2010),” Security and privacy in cloud computing: a survey” Sixth International Conferences on Emantics Knowledge And Grid 2010.

9. Maninder Singh , Sarbjeet Singh, “Design and implementation of multi-tier authentication scheme in cloud”, International Journal of Computer Science Issues(IJCSI), ISSN (Online):1694-0814, Vol. 9, Issue 5, No 2, pp. 181-187, September 2012.

10. Abdul Raouf Khan, “Access control In cloud computing envirome.

11. P. M. Mell and T. Grance, ``The NIST denition of cloud computing,''Commun. ACM, vol. 53. no. 6, p. 50, 2011.

12. G. Han, A. Qian, J. Jiang, N. Sun, and L. Liu, ``A grid-based joint routing and charging algorithm for industrial wireless rechargeable sensor networks,'' Comput. Netw., vol. 101, no. 6, pp. 1928, 2016.

13. T. Qiu, D. Luo, F. Xia, N. Deonauth,W. Si, and A. Tolba, ``A greedy model with small world for improving the robustness of heterogeneous Internet of Things,'' Comput. Netw., vol. 101, no. 6, pp. 127143, 2016.

14. M. Ali, S. U. Khan, and A. V. Vasilakos, ``Security in cloud computing: Opportunities and challenges,'' Inf. Sci., vol. 305, pp. 357383, Jun. 2015.