Securing Public Data Storage in Cloud Environment

D. Boopathy and M. Sundaresan

Department of Information Technology, Bharathiar University,
Coimbatore, Tamilnadu, India
{ndboopathy,bu.sundaresan}@gmail.com

Abstract. Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources. It implies a service oriented architecture type (SOA), reduced information technology overhead for the end-user, great flexibility model, reduced total cost of ownership, on-demand service providing structure and many other things. One of the main concerns of customers is Cloud security and the threat of the unknown. The lack of physical access to servers constitutes a completely new and disruptive challenge for investigators. The Users are store, transfer or exchange their data using public cloud. This paper represents the encryption method for public cloud and also the cloud service provider's verification mechanism using the third party auditors.

Keywords: Secured Data Storage, Public Cloud Service Provider, Cloud Service Provider, Cloud Encryption, Cloud Decryption, Third Party Auditor.

1 Introduction

Cloud computing is a natural evolution of the widespread adoption of virtualization service, service-oriented architecture (SOA), autonomic, and also utility computing. Cloud computing is the broader concept of infrastructure convergence [5]. This results in reduced cost of the services. Quality of services also gets better as the organization can spend the saved amount and time on improving it [1]. In cloud environment, resources are shared among all of the servers, users and individuals [3]. As a disarray invention with foreseen implication, cloud computing is mending way it uses business with IT [4]. Security and Privacy issues are of more concern to cloud service providers who are actually hosting the services [14]. Cloud computing models are of two types: Deployment model and Service model. Deployment model is further classified into four type's namely private cloud, community cloud, public cloud and hybrid cloud. Cloud computing service providers provide their services in a number of fundamental models [13]. Cloud computing is a term which is often used with synonyms like grid computing, cluster computing, autonomic computing [12]. For the organization, the cloud service provider offers data centers to move their data globally [11]. It is up to the clients to decide the vendors and also depending on how willing they are to implement secure policies and be subject to 3rd party verifications [10]. Another factor of concern is that the cloud is still under development process and there are no set standards for the data storage and application communication [6].

S.C. Satapathy et al. (eds.), *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI - Volume I*, Advances in Intelligent Systems and Computing 248,
DOI: 10.1007/978-3-319-03107-1_61, © Springer International Publishing Switzerland 2014

In Private cloud, the cloud infrastructure is operated solely for an organization. This cloud model may be managed by the organization or a third party and may exist on premise or off premise. In Community cloud, the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. In public cloud, the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. In hybrid cloud, the cloud infrastructure is a composition of two or more clouds.

1.1 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The cloud applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including like network, servers, storage, operating systems or individual application capabilities, and with the possible exception of limited user-specific cloud based application configuration settings. It is also referred as Resource Code; provide (managed and scalable) resources as services to the user- in other words, the service providers basically provide enhanced virtualization capabilities. Accordingly, different types of resources may be provided via a service interface [6].

1.2 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the service provider. The consumer does not able to manage or control the underlying cloud infrastructure including like network, servers, operating systems, or storage, but has control over the deployed cloud applications and possibly application hosting environment configurations.

1.3 Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, networks, storage and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can also include the operating systems and applications. The consumer/client does not manage or control the underlying cloud infrastructure but has control over operating systems; deployed applications, storage and possibly limited control of select networking components (e.g., host firewalls).

2 Cloud Computing Types

There are four different types of cloud are in use, they are:

2.1 Private Cloud

The private cloud infrastructure is operated solely for an organization. It may be managed or maintained by the service acquiring organization or a third party and may exist on organization premise or off premise.

2.2 Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

2.3 Community Cloud

The community cloud infrastructure is shared by the several organizations and supports a specific community purpose that has shared concerns.

2.4 Hybrid Cloud

The hybrid cloud infrastructure is a composition of two or more clouds (i.e. private, community, or public) that remain unique resource entities but are bound together by standardized or proprietary technology that enables data and application portability [1].

The Security goals of cloud data storage include three important points namely: Data Availability, Data Confidentiality and Integrity.

3 Problem Statement

Information security is a critical issue in cloud computing environments [9]. The public cloud is widely accessed and utilized by the many users for their own purpose, small organizations to manage their data and so on. The public cloud services providers are mostly make the trust among the users by some attraction advertisement and avail their service in very low cost. The data transferred, stored or exchanged in public cloud is mostly unsafe due to the untrust environment. The cloud Computing provides an undemanding and non ineffectual Solution for Daily Computing [5]. The aspect of security and confidentiality must intervene to protect the data from each of the enterprises [10]. Share resources, software and information are provided to computers and other devices on demand [8].

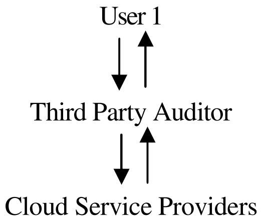
While the benefits of storage networks have been widely acknowledged, consolidation of enterprise data on networked storage poses significant security risks [2]. Hackers adept at exploiting network-layer vulnerabilities can now explore deeper strata of corporate information [2]. Its unauthorized disclosure could seriously and adversely impact the organization and its employees [16]. The Cloud Security Alliance's initial report contains a different sort of taxonomy based on different security domains and processes that need to be followed in general cloud deployment [15].

To bring the users data into safer side the secured data storage model is proposed.

4 Secured Data Storage

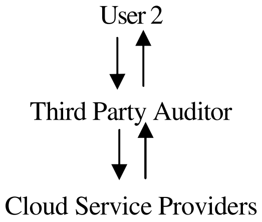
The secured data storage is used the third party auditor as an intermediate person to connect and helps to transfer the secure data transfer between the data destination place to data accessing place. In this model both the data accessing user and data storing user are uses the secured process by using the encryption algorithms. The RSA algorithm is used to encryption style, but the process is made in moderate style. The data hijack and data stolen is not possible in this secured data storage model, due to the RSA algorithm moderate style.

The user1 verifies the public cloud service provider using the third party auditor. When the third party auditor will issue the status of the selected service provider, user1 will ready to upload the files into that public cloud service provider.



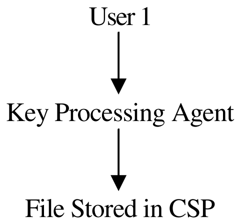
User Verification Model at Data Upload

When user wants to download the file from the public cloud service provider again the verification process will be taken place to verify that the provider still in the live status or not.



User Verification Model at Data Download

The User 1 encrypt the file using the private key and store it to the CSP with public key access, then the User 2 required the file which was stored by the User 1 in the CSP. The User 2 retrieving the file from the CSP using his/her private key to get the decrypted file. The access made through the public key and the encryption took place through the User 2 private key.



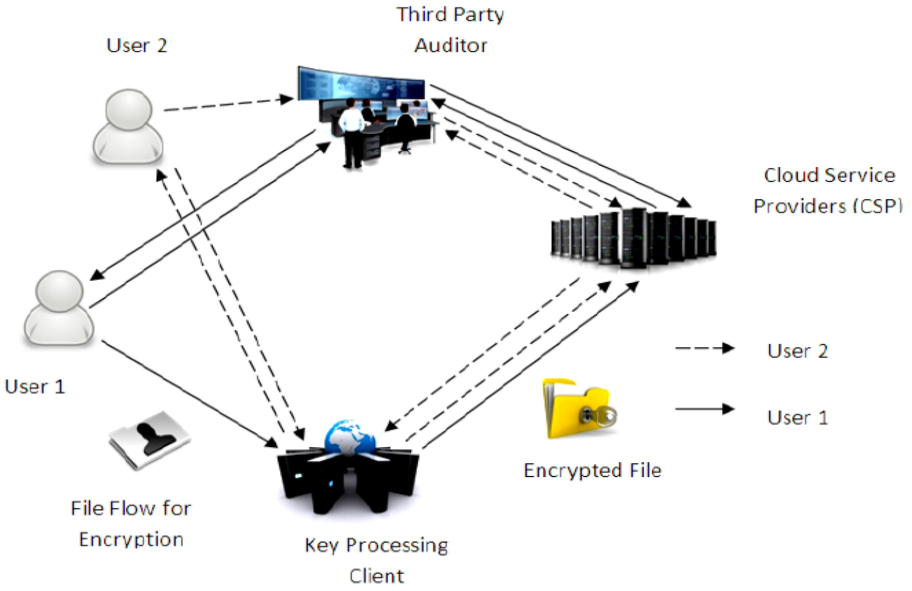
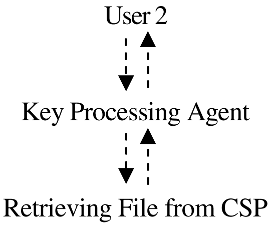


Fig. 1. Secured Data Storage

File stored in the public cloud service provider in the encrypted format using the RSA algorithm.



The user2 retrieve the file from the public cloud service provider and decrypt the file using his/her private key.

4.1 The Mechanism Working Style

Step 1: The RSA algorithm is used in this method. The User 1 send the file to the key processing client using his private key, then the file encryption taken place, public key was fixed and moved to CSP.

Step 2: When the user 2 required the encrypted file which was stored in the CSP by the User 1. So the User 2 used his/her private key to access the key processing client. The key processing client recognizes the User 2 request by his/her private key. Then the file was decrypted by using the public key then transfer to the User 2.

4.2 The Working Flow Code

User 2 = U2, User 1 = U1, Third Party Auditor = TPA, Public Cloud Service Provider = PCSP, Key Processing Client = KPC.

User1 storing the file in public cloud service provider:

1. U1 send request to TPA.
2. TPA analysis PCSP whether the service is available or not.
3. If the service is available TPA replies to U1 as positive.
4. U1 send the file to KPC using private key and encrypt the file.
5. After encryption KPC stored the encrypted file in the PCSP with the public key access.

User 2 access the file from the public cloud service provider:

1. U2 send request to TPA.
2. TPA analysis PCSP where the service is available If service is available TPA replies to U2 as positive.
3. U2 send the file to KPC using private key and decrypt the file.
4. The KPC access the file from the PCSP using the public key and decrypt the file using the U2 private key and send it to the U2.

$$\text{For Accuracy Level of Services} = \frac{\text{No. of Cloud Service Providers}}{\text{No. of Cloud Services Rendering}} \text{ X } \begin{array}{c}\text{No. of}\\ \text{Satisfied}\\ \text{Users}\end{array}$$

The result of the accuracy level of services is calculated based on the third party auditor report format. If any error or mistakes was taken place in the upload or download of the file, it is also taken into the accuracy level report. According to the information collected at the time of data accessing, uploading the data by main user and also data downloaded by end user. All are taken into the accuracy calculation.

5 Discussion

The Secured Cloud Storage mechanism is using the RSA algorithm for encryption and decryption. So the users can encrypt the file using their private key and stored the file in the public cloud service provider using public key. The public key is used to store and access the file from the public cloud service provider. The important thing is the public key is only used to access the file. The user required private key to decrypt the file.

The processing methods take lesser steps when compared to the existing model.

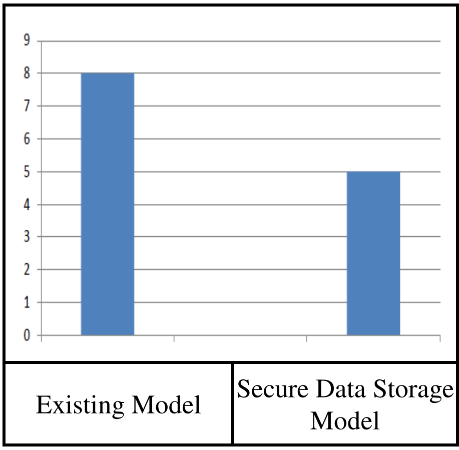


Fig. 2. No. of steps in Encryption the file

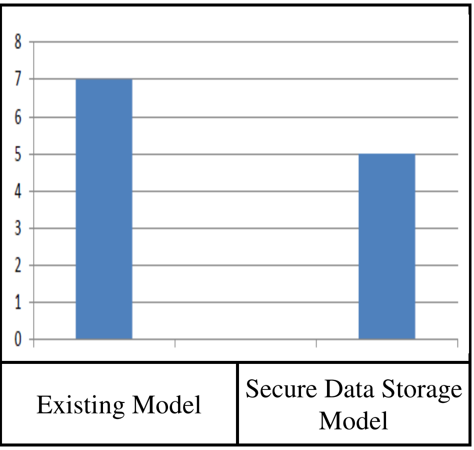


Fig. 3. No. of steps in Decryption the file

6 Conclusion and Future Enhancement

The Secured Cloud Storage takes fewer steps to encrypt and decrypt the files. The existing models are still not entered into the real world service environment. The many encryption models for cloud environment are still in developing stage. The Secured Cloud Storage model will provide the maximum level of Secured structure in the cloud environment. In future the Secured Cloud Storage, the remaining algorithms will take into development to provide the better security to this model. The remaining algorithms results will take into consideration and compared to provide the maximum level of security in the cloud environment.

References

1. Tripathi, A., Yadav, P.: Enhancing Security of Cloud Computing using Elliptic Curve Cryptography. International Journal of Computer Applications (0975 - 8887) 57(1), 26–30 (2012)
2. El-Khameesy, N., Rahman, H.A.: A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems. Journal of Emerging Trends in Computing and Information Sciences 3(6), 970–974 (2012)
3. Nafi, K.W., Kar, T.S., Hoque, S.A., Hashem, M.M.A.: A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture (IJACSA) International Journal of Advanced Computer Science and Applications 3(10), 181–186 (2012)
4. Govinda, K., Gurunathaprasad, V., Sathishkumar, H.: Third Party Auditing for Secure Datastorage in Cloud through Digital Signature using RSA. International Journal of Advanced Scientific and Technical Research 4(2), 525–530 (2012) ISSN 2249-9954

5. Kaur, M., Mahajan, M.: Implementing Various Encryption Algorithms to Enhance the Data Security of Cloud in Cloud Computing. VSRD International Journal of Computer Science & Information Technology 2(10), 831–835 (2012)
6. Kaur, S.: Cryptography and Encryption In Cloud Computing. VSRD International Journal of Computer Science & Information Technology (VSRD-IJCSIT) 2(3), 242–249 (2012); Kaur, A., Bhardwaj, M.: Hybrid Encryption tor Cloud Database Security. International Journal OF Engineering Science & Advanced Technology 2(3), 737–741 (2012)
7. Sudha, M., Monica, M.: Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Data Secuity. Advances in Computer Science and its Applications 1(1), 32–37 (2012)
8. Gampala, V., Inuganti, S., Muppidi, S.: Data Security in Cloud Computing with Elliptic Curve Cryptography. International Journal of Soft Computing and Engineering (IJSCE) 2(3), 138–141 (2012) ISSN: 2231-2307
9. Tebaa, M., El Hajji, S., El Ghazi, A.: Homomorphic Encryption Applied to the Cloud Computing Security. In: Proceedings of the World Congress on Engineering (WCE 2012), London, U.K., July 4-6, vol. I, pp. 536–539 (2012)
10. Bhagat, A., Sahu, R.K.: Using Third Party Auditor for Cloud Data Security: A Review. International Journal of Advanced Research in Computer Science and Software Engineering 3(3), 34–39 (2013)
11. Saravanan, N., Mahendiran, A., Venkata Subramanian, N., Sairam, N.: An Implementation of RSA Algorithm in Google Cloud using Cloud SQL. Research Journal of Applied Sciences, Engineering and Technology 4(19), 3574–3579 (2012)
12. Bhosale, P., Deshmukh, P., Dimbar, G., Deshpande, A.: Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption. International Journal of Engineering Research & Technology (IJERT) 1(8), 1–8 (2012)
13. Radhika, G., Satyanarayana, K.V.V., Tejaswi, A.: Efficient Framework for Deploying Information in Cloud Virtual Datacenters with Cryptography Algorithms. International Journal of Computer Trends and Technology 4(3), 375–380 (2013)
14. Marwaha, M., Bedi, R.: Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing. IJCSI International Journal of Computer Science Issues 10(1(1), 367–370 (2013)
15. Nigoti, R., Jhuria, M., Singh, S.: A Survey of Cryptographic Algorithms for Cloud Computing. International Journal of Emerging Technologies in Computational and Applied Sciences 4(2), 141–146 (2013)
16. Mishra, A., Gupta, D.K., Sahoo, G.: BIT Mesra Ranchi, Jharkhand. The Secure Data Storage in Cloud Computing Using Hadamard Matrix. International Journal of Engineering Science and Innovative Technology (IJESIT) 2(2), 389–395 (2013)