

Enhanced Encryption and Decryption Gateway Model for Cloud Data Security in Cloud Storage

D. Boopathy and M. Sundaresan

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

Abstract. The Cloud computing technology is a concept of providing online multiple resources in the scalable and reliable method. The user will access cloud service as per their requirement of computing level. There is no capital expenditure involved in computing resources for cloud user. The users have to pay as per their storage, network and service usage. The cloud computing have some highlighted issues like compliance, cross border data storage issues, multi-tenant and down time issues. The most important issues are related to storage of data in cloud. Data confidentiality, data integrity, data authentication and regulations on data protection are major problems that affect user's business. This paper discusses about encryption and decryption data security issues in cloud and its safety measures and comes out with a novel research work of cloud data security model.

Keywords: Cloud Security, Cloud Computing, Cloud Data Security, Data Security, Cloud Data Storage, Compliance Issues.

1 Introduction

The cloud service providers are widely spreading their service with their own business models. This own business model is basically designed and extracted from some open source model [1]. But the core things of cloud computing has never changed [3] [4]. The user's data will be stored outside the user's premises so the users easily lose their control over the data which are stored in cloud storage. When the user loses their control over their data [5], then the user is systematically locked in with their cloud service provider or third party service vendor [7].

There are no standardized international laws and regulations to protect the user's data stored in cloud. Some countries framed rules and regulations to protect their country data, but the existing rules and regulations are not sufficient to protect the data in cloud.

2 Problem Statement

The cloud security has many phases and they are identified as availability issues, data security issues, identify and access management issues, government issues and compliance issues [8].

There are number of cloud data security related issues associated with cloud storage.

- The data holding or storing service provider may illegally use the client data to develop their business.
- The cloud service providers give access to their local government and their authorities as per their jurisdiction regulations and standards.
- The service provider may bankrupt or vanish from the service providing market.
- The unauthorized access cannot be avoided in an effective manner.

While the user, must ensure that the provider has taken the proper security measures to protect their information or data in cloud.

3 Cloud Computing

National Institute of Standards and Technology defined cloud computing as follows:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2].”

3.1 Cloud Service Models

Software as a Service (SaaS) is a model provided to the consumer to use the cloud service provider’s applications on a cloud infrastructure. The cloud running applications are accessible from different client devices through an interface such as a web browser [2].

Platform as a Service (PaaS) is a model provided to the consumer to deploy onto the cloud infrastructure consumer created or else consumer acquired applications, created using multiple programming languages and different tools supported by the cloud service providers [2].

Infrastructure as a Service (IaaS) is a model provided to the consumer to provisions like processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run based on random choice software, which can include different operating systems and multiple applications [2].

3.2 Cloud Deployment Models

Private Cloud is the cloud infrastructure model operated solely for an organization [6]. It may be managed or controlled by the deployed organization or a third party service providers and may exist on premise or off premise model [2].

Public Cloud is the cloud infrastructure made available to the general public or a large industry group purpose and it is owned and managed by an organization selling cloud services [2].

Community Cloud is the cloud infrastructure model shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party and may exist on premise or off premise [2].

Hybrid Cloud is the cloud infrastructure model that is a composition of two or more clouds (i.e. private, community, or public) that remain unique entities but are bound together by standardized or technology proprietary [2].

4 Encryption and Decryption Gateway Server (E&DGS)

The Encryption & Decryption Gateway Server (E&DGS) is used to encrypt the data storing in cloud storage before crossing the data ownership country border. The schema used for encryption and encrypted keys are stored within the data ownership country border itself. If any user try to access the encrypted data stored in cloud storage, that users request is redirected to the Encryption & Decryption Gateway Server (E&DGS). If the users have credentials to access the encrypted data then the

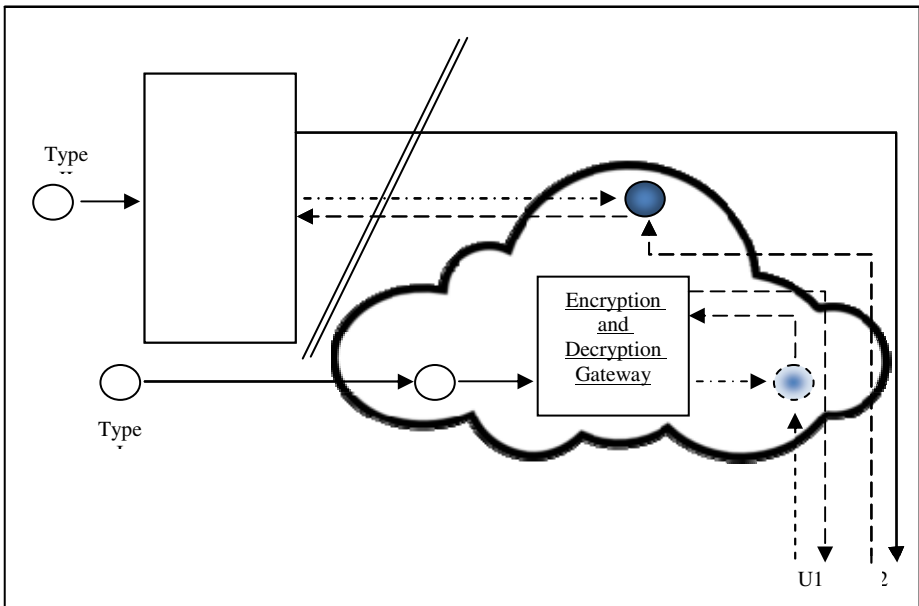

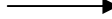







Fig. 1. Cloud Encryption and Decryption processes types

-  User Data before Encryption
-  Data Flow without Encryption
-  Data Encrypted Using Within Border Limit
-  Data Flow after Encryption
-  Data Encrypted Within Cloud Storage
-  User Request Data
-  Data Transfer to User after Decryption Using Within Country Border

encrypted data will be decrypted and sent to the data request user. This method avoids the unauthorized data usage without data owner’s knowledge. If any government legally has rights to view the data stored in their country territory, they also need permission from the Encryption & Decryption Gateway Server (E&DGS) to view the data which is stored in their country. The process of this Encryption & Decryption Gateway Server (E&DGS) model reduces the security threats on data stored in cloud storage and multi-tenant model.

Procedure for Data Storage Process and the Process Explained in Figure 2

1. Process started.
2. Data transferred from user to E&DGS.

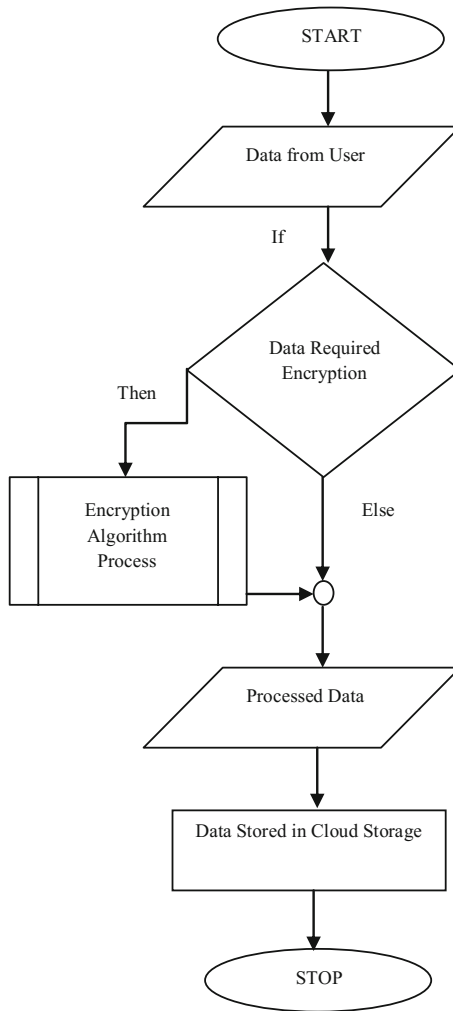


Fig. 2. Data Storage Process Flow Chart Chart

3. If data requires any encryption, then the data is transferred to the encryption algorithm process and then transferred to processed data state.
4. Else the data is transferred to processed state.
5. Data gets stored in cloud storage
6. Process stopped.

Procedure for Data Retrieval Process and the Process Explained in Figure 3

1. Process started.
2. Data access request from user.
3. Requested data retrieved from the cloud storage.
4. If the selected data requires any decryption then it is transferred to decryption algorithm process. Else the data sent to the request person as a processed data.
5. In decryption process, first it checks the user credentials. Whether the user has rights to decrypt it and access it or not.
When the user is valid then the decryption takes place and then processed data transferred to the data request person.
6. Else the user is not valid then the request is cancelled and the process stops.
7. Process stopped.

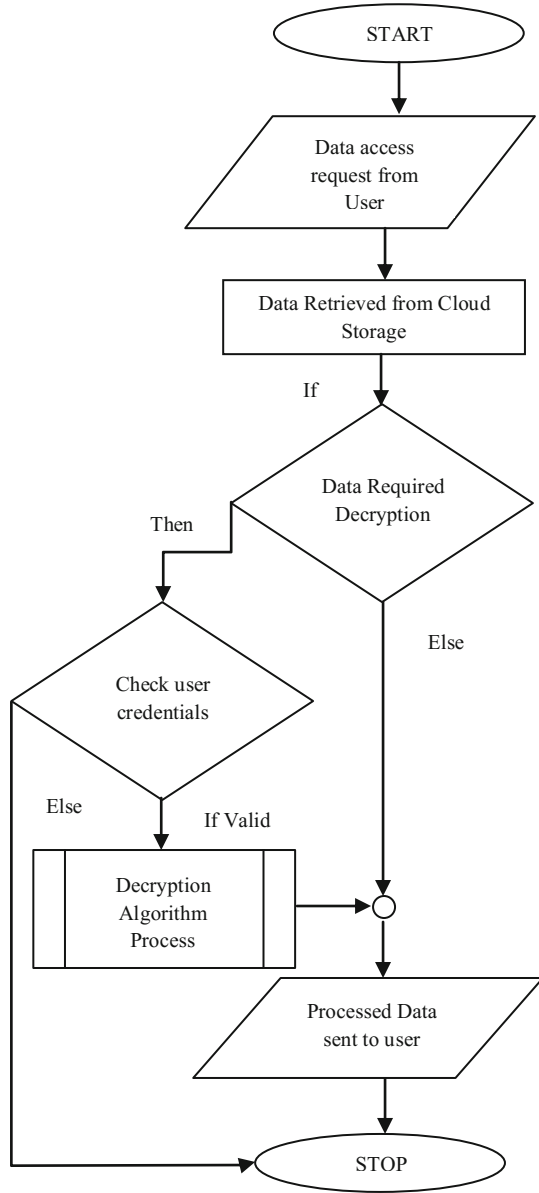


Fig. 3. Data Retrieval Process Flow Chart

5 Discussion

The Network Simulator 2 (NS2) is used to simulate the Encryption and Decryption Gateway Server Model (E&DGS). Figure 4 shows the data flow design of data storage and data retrieval model. Figure 5 shows the data transfer from the E&DGS to cloud server. Figure 6 shows the data storage in cloud multiple server and the user send request to access the data in cloud. That request is transferred to E&DGS and then data transferred to the data request user through cloud service. Figure 7 shows the processing time taken for data storage and data retrieval in cloud storage using proposed model.

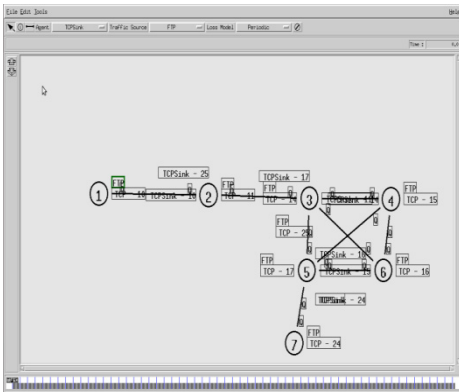


Fig. 4. Data storage and Retrieval Process Flow Design

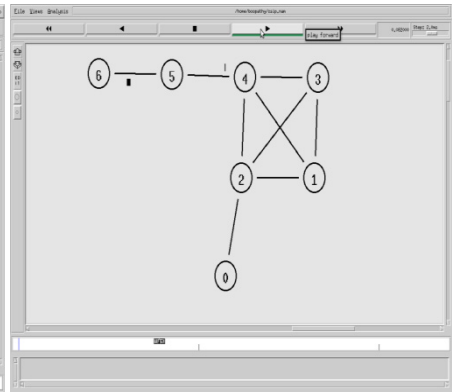


Fig. 5. Data storage Process Flow Design

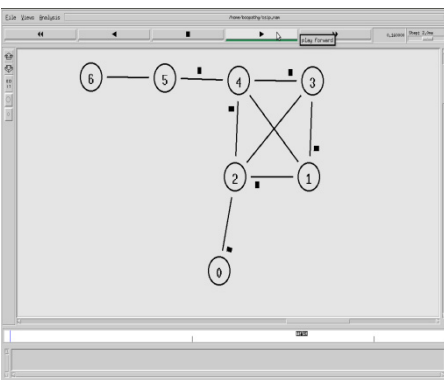


Fig. 6. Data Retrieval Process Flow Design

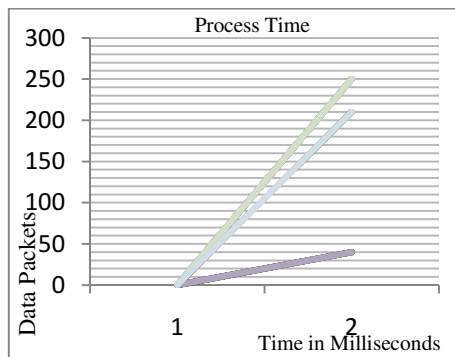


Fig. 7. Processing time taken for data storage and retrieval in proposed model

6 Conclusion and Future Scope

The proposed Encryption and Decryption Gateway Server (E&DGS) model works effectively on data encryption and decryption during data transfer across the country. If the user's request is redirected to the E&DGS model, it will avoid unauthorized and illegal data access and usage. This model works very effectively when additional security check points like digital watermark allocation and verification added to it. Despite these security check points, it is also necessary to make some revisions regarding the standards, rules and regulations on cloud service to provide maximum level of security for cloud service providers and cloud service users.

References

- [1] Yu, X., Wen, Q.: A View About Cloud Data Security From Data Life Cycle. In: International Conference on Computational Intelligence and Software Engineering (CiSE), December 10-12, pp. 1-4 (2010)
- [2] NIST Definition (February 02, 2014),
<http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>
- [3] Boopathy, D., Sundaresan, M.: Data Encryption Framework Model with Watermark Security for Data Storage in Public Cloud Model. In: International Conference on Computing for Sustainable Global Development, March 5-7, pp. 903-907 (2014)
- [4] Boopathy, D., Sundaresan, M.: Location Based Data Encryption Using Policy and Trusted Environment Model for Mobile Cloud Computing. In: Second International Conference on Advances in Cloud Computing, September 19-20, pp. 82-85 (2013)
- [5] 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 For Cloud Database Security. International Journal of Engineering Science & Advanced Technology 2(3), 737-741 (2012)
- [6] Cloud Deployment Models, <http://bizcloudnetwork.com/defining-cloud-deployment-models> (retrieved March 05, 2014)
- [7] 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)
- [8] Vulnerability Rethink, http://www.cbronline.com/news/studycallsforvulnerability_030209 (retrieved January 02, 2014)