ObfuCloud: An Enhanced Framework for Securing DaaS Services Using Data Obfuscation Mechanism in Cloud Environment

Article · January 2018

DOI: 10.1007/978-981-10-5523-2_31

CITATION
1

READS
250

2 authors:

Krunal Suthar
Sankalchand Patel College of Engineering
10 PUBLICATIONS **29** CITATIONS

SEE PROFILE

Jayeshkumar Madhubhai Patel
Ganpat University
96 PUBLICATIONS **215** CITATIONS

SEE PROFILE

ObfuCloud: An Enhanced Framework for Securing DaaS Services Using Data Obfuscation Mechanism in Cloud Environment

Krunal Suthar and Jayesh Patel

Abstract Cloud computing is now a day's become most attracted phenomena to use for a large-scale organization or for individual who need various network services with least cost. Normally, individual's information is stored on public Cloud which is available to everyone for access. This fundamental raise some issue opposite to flexible services provided by Cloud providers, like Confidentiality, Integrity, Availability, Authorization and many more. To protect the data, lots of options available now a days and most preferable way is to use encryption. Encryption only cannot provide enough protection while considering user's sensitive information, as well as it consumes more time to process encryption and decryption. To remove the burden of Cloud server, as well as to keep adequate security to user's information in Cloud environment, in this paper, we propose a methodology for combining both techniques, viz. obfuscation and encryption. The user data may be encrypted if it requires security for its files or document, and the DaaS service of Cloud must be secured using obfuscation techniques. Using this two-way approach, we can say that the proposed scheme offers enough security towards anonymous access and preserve privacy even of the information available on Cloud Servers. We also aim to provide proper integrity checking mechanism, better access control mechanism which lessens the burden of Client as well as service provider.

Keywords Cloud storage · Data protection · Integrity · Obfuscation
Access control · Privacy preservation

K. Suthar (✉)
Computer Engineering Department, Sankalchand Patel College of Engineering, Visnagar, Gujarat, India
e-mail: krunal_bece@yahoo.co.in

J. Patel
Computer Science Department, AMPICS, Kherva, Gujarat, India
e-mail: jayeshpatel_mca@yahoo.com

Y.-C. Hu et al. (eds.), *Intelligent Communication and Computational Technologies*, Lecture Notes in Networks and Systems 19,
https://doi.org/10.1007/978-981-10-5523-2_31

1 Introduction

Cloud computing is the term related to the internet-based high computing whose aim is to provide devices with a shared pool of resources, information or software on demand and pay per-go basis anytime anywhere. The Cloud models come with mainly important characteristics like the pooling of resource, services on demand, access of the broad network, quick elasticity and precise service. A service provider of Cloud provides service models like PaaS, SaaS, IaaS, DaaS that come with a pack of three basics deployment models that are private, public Cloud and hybrid Cloud [1].

1.1 Cloud Services

Services provided by the Clouds are broadly divided into four major categories which are shown in Fig. 1.

1.2 Database and Document Security in Cloud Environment

Users' information security is one of the main concern in Cloud environment. Data protection [2] includes various issues like manage confidentiality, integrity, provides authentication, achieve availability and many more. Data confidentiality means that only authenticated user has access of data. Data integrity means the information must be unchanged while available on a remote system or on the local system. Authentication refers to the method of checking whether the user who tried

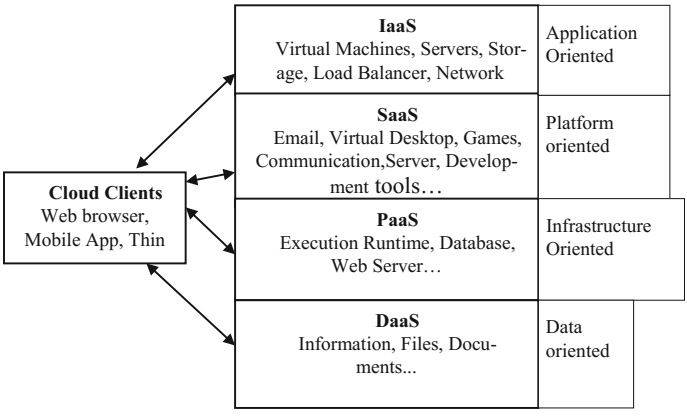

Fig. 1 Services offered [10, 11]

to access information is valid or not. Data availability means to achieve the data anytime whenever required.

Normally, confidentiality achieved by encryption technique, but for the Cloud environment when user data and user personal information are separated from each other. Encryption is only important when we think about the security of user-stored document, but when the personal information is targeted by any attacker then it is required to preserve the privacy of database on Cloud server. Here the encryption scheme can be worked but it consumes lots of time for encryption and decryption process because thousand of processes are done simultaneously. So, to achieve speed and security both required a framework, which deals with users' and Cloud servers' issue using technique mentioned [3].

1.3 Why Data Obfuscation Required in Cloud Computing Environment?

i. Data Confidentiality Protection
Confidentiality guarantees that the sensitive information has not become available to the person who is not authentic or to other processes, or Devices. The information details should be considered as broken if any of the following conditions are violated: (1) The physical availability of the user data is known to the user (2) Provider able to access the personal information of the Cloud user (3) Meaning of user-uploaded information are disclosed to the user [4].

ii. Some of the major issues in current Cloud system are as follows:

A. Every provider of Cloud work as a provider of different layered services like platform, software layer and infrastructure layer. The user is only able to use the infrastructure service provided as it is while using a Cloud application, and because of this dependency, the service provider knows where the users' data is located and has full access privileges to the data.

B. The providers force a user to only use the interface provided by them, so the users need to submit their data in a fixed format. And because of this, a service provider has an adequate idea about how to access the user information and is able to control this information.

By combining four entities we can achieve protection in Cloud environment: Cloud, Infrastructure Cloud, Encryption, Data Obfuscation and Data De-Obfuscation.

(1) Cloud: A Cloud provides database as a service upon users' requests.
(2) Infrastructure Cloud: An Infrastructure Cloud provides virtualized system resources, such as CPU, memory and Database. An authenticated user can request to retrieve information or files which the user sent to the Cloud.
(3) Encryption: This technique provides an efficient way to covert user information into an unreadable format.

Table 1 Obfuscation techniques [8, 12]

Strength of obfuscation technique [13]: domain	Techniques	Potency	Resilience	Cost
Transform	Code	Medium	One-way	Free
Transform	Data	High	Two-way	Cheap
Transform	Control	Medium	Partial one-way	Costly

(4) Data Obfuscation: its a mechanism that the data converted into a format which makes reverse engineering difficult for the attacker as well as for any automated software [5] (Table 1).

2 Literature Review

Arockiam and Monikandan in [6] proposed a novel technique to achieve confidentiality to address the issue of data security. The author aims to provide confidentiality using two important techniques that are identified as obfuscation and encryption. The key used for encryption purpose is: to keep secret with the user and access of this data is only permitted by passing a corresponding decryption key. Authors not only aim to use encryption but also offer an obfuscation mechanism to increase the security of data.

Atiq ur Rehman, M. Hussain SZABIST in [7] presented a model for managing DaaS confidentiality of data stored in Cloud database. The model consists of two main features. The first focus is on how the user data will be stored in the server. A second feature provided regarding how a user can send query so that even data will be fetched using DaaS service. The database admin has no idea about this process and also about what type of data requested by the user. The model performs query execution on the encrypted and obfuscated data.

Arvind Narayanan and Vitaly Shamatikov in [8], in this, the methodology for achieving privacy are discussed. The owner who want to share the information with different users does not need to hide each data entry separately but to obfuscate the database entry, which provides execution of only particular types of queries. Even if the database details are provided still the database is only accessible with reference to the designed privacy model. Here, the novel concept of database privacy is proposed, other than that, for managing secrecy of individual records only some of the queries are permitted and realized it using provably secure obfuscation technique.

Krunal Suthar [9], in this research has proposed a model to have proper confidentiality, security and integrity of user information. In the proposed scheme, encryption is basically done in client side and obfuscation is done for the Cloud service providers. By using encryption the data which is in transition becomes secure. Data obfuscation helps data which is on rest in the machine of the service

provider to get secured. To achieve user as well as server control mechanism authors have also proposed an algorithm which proves that this technique together provides adequate security. From the implementation analysis, authors argue that compared to existing schemes the proposed scheme provides better protection towards stored information on a Cloud which is based on encryption only.

3 Proposed Methodology

The approach mainly focuses on three sections that are uploading, integrity management and secure access control with proper rights management. Figures 2, 3 and 4 give detail description of operations that are carried out.

Upload Data on Cloud

1. CU > CSP (Input Login Detail (Assume that user is already registered))
2. CSP verify > CU (Detail verified at server. If user replies accordingly)

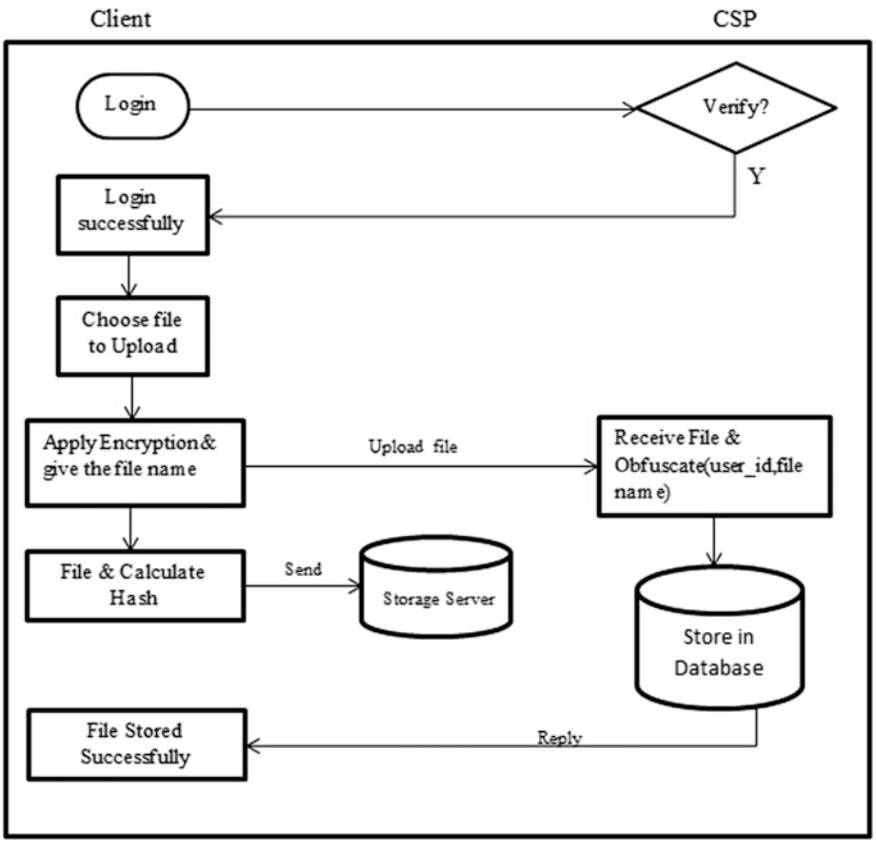

Fig. 2 Uploading

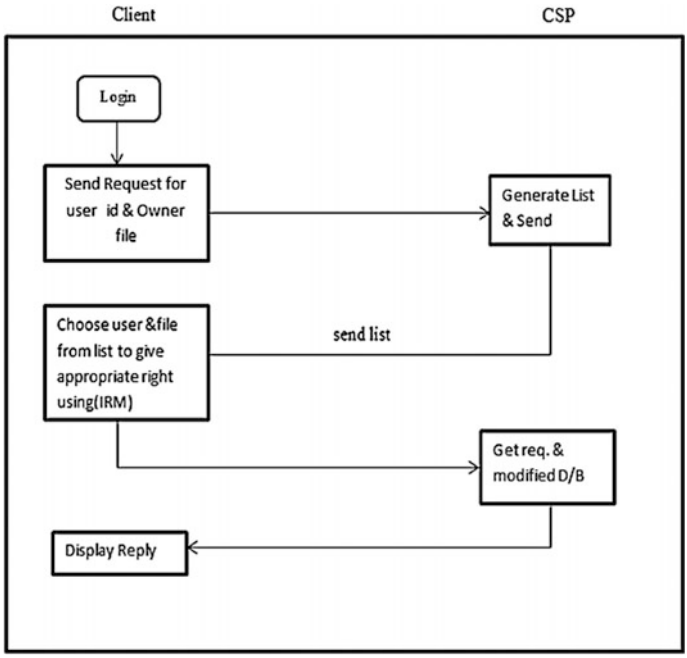

Fig. 3 Right management

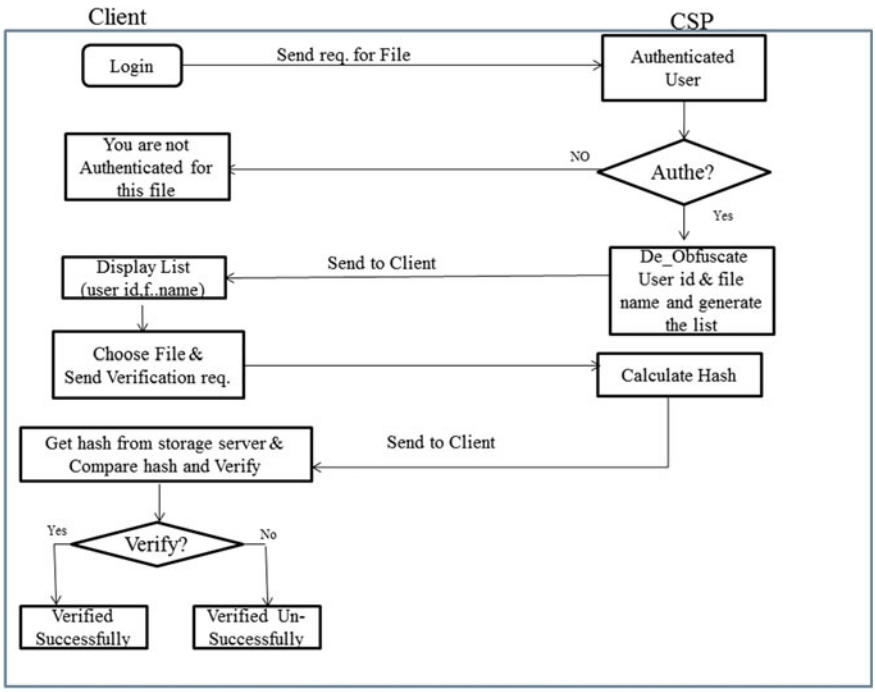

Fig. 4 Integrity management

3. CU Upload > (User uploads the file, this includes encryption mechanism provided by the server to the client interface.)
4. CSP obfuscates and stores (store this information in database after obfuscating it)
5. CU store hash (Hash of that file and store on the storage server)

For Right management

1. CU *Id & Owner file req.* > CSP (Client send request for owner's file list to CSP)
2. CSP *File List* > CU (CSP generate list of owner's file and send to the client)
3. CU *File & IRM* > CSP (Client choose user and file and apply IRM policy then sends to the CSP)
4. CSP un-obfuscate and update (CSP modify database).

For Integrity

1. CU *Req. File* > CSP (Client sends request for files to CSP)
2. CSP *Verify* > CU (Check the user is athenticated or not and reply accordingly)
3. CSP *De-obfuscate files* > CU (CSP De-obfuscates files and sends to the client)
4. CU *File & verify request* > CSP (Client sends verification req. to server)
5. CSP *Hash* > CU (CSP calculates Hash and sends to the client)
6. CU compares and verify (Client compare Hash code store on storage server)

4 Result and Discussion

We run our model on a system with Intel Core I3 processor with 4 GB RAM, system running 64-bit windows and using Cloudsim simulator.

Basic analysis
In the basic analysis, consider a table containing sample information shown in Table 2 and the obfuscated data stored on server shown in Table 3.

Performance analysis
In Performance analysis phase, we analysed developed system using different evaluation parameter shown in Fig. 5 in terms of execution speed. First, demonstrate the result regarding consumption of time for encryption and obfuscation

Table 2 Sample data

User_Id	File name	Upload date	Hdd_name
first@gmail.com	C:\Users\obfu1.txt	10-9-2016	F drive
second@gmail.com	C:\Users\obfu2.txt	10-9-2016	F drive
third@gmail.com	D:\Files\obfu3.txt	17-9-2016	E drive

Table 3 Obfuscated data

User_Id	File name	Upload date	Hdd_name
AnVfdjlkjl88sf8aads=	RTpcQR6haZGVtaWMgRlxkYXRhXNoX0kjQn4lcncopJyL4dA=	MKol3bSxyNg ==	PKk=
Op5nagDjjWnxjk56f=	RTpcQR6lcnNcU09OWS1qA1xEZXNrdG4rtXGNsb3Vkc2lccmNc=	MKol3SaxyNg ==	PKk=
Yu4MashAjh2hdkjsm=	QzpcQZNlcnNcU09OWJ61QQ1xEZXNrdG88c2lFxWRzaEl3Snz=	Kolw7zRSyNg ==	Fzl=

process on different size of the file. We have also shown a comparison between the system that uses obfuscation and the system without obfuscation by varying the file size. This proves obfuscation only increases the little bit time and reduces the burden of Cloud server.

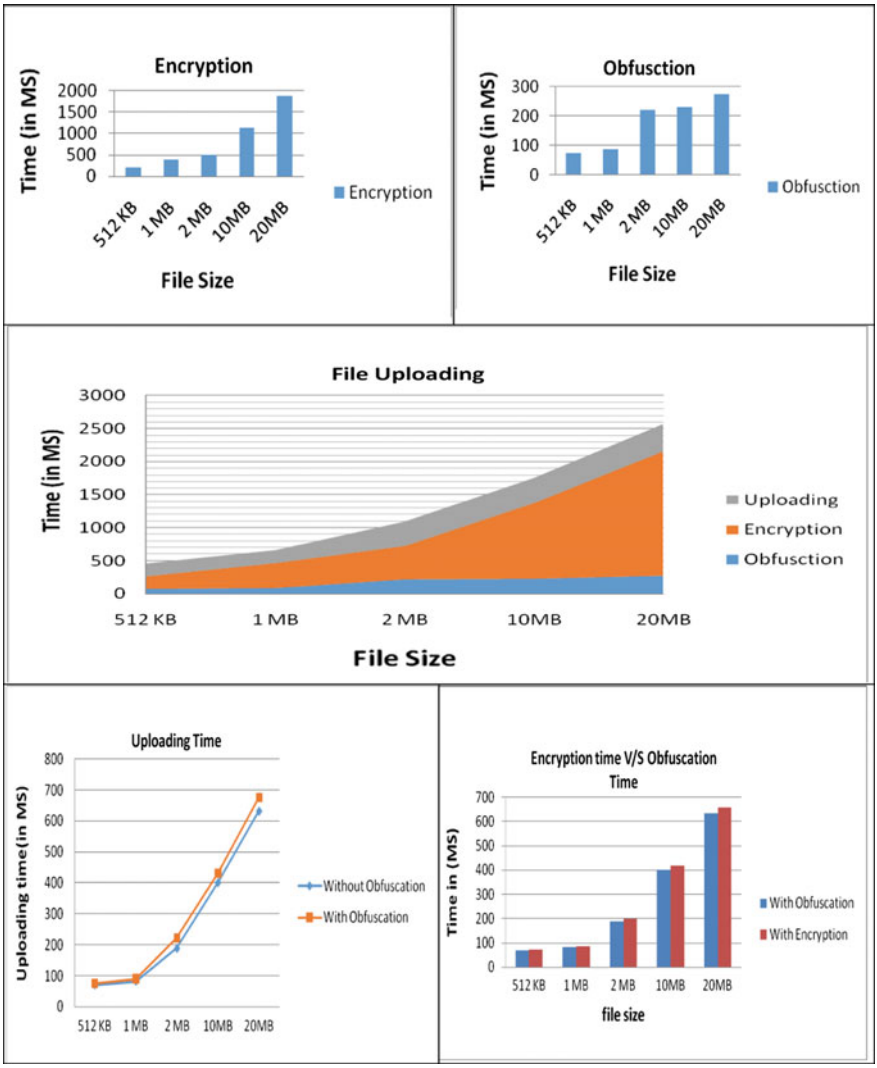

Fig. 5 Result analysis

5 Conclusion

Even Cloud computing provides numerous advantages to the user, but still, due to security issues many users hesitate to adopt it, as well as, the service provider may have an issue about unauthorized access. So, to solve an issue related to both user and service provider, we developed a new framework by proposing a combination of encryption and obfuscation technique together. Before sending data on Cloud encryption provides security to the data which is on transition in the network by which user ensures the confidentiality of his data. We also proposed a secure storage server which keeps track of user keys as well as hash of the document uploaded on the server. For the Cloud providers, we propose efficient obfuscation technique by which the secret information of client like password, contact details, etc. are not tempered by the third party.

We also figure out the steps for an algorithm which ensures that all this operation working efficiently. We are also providing detailed analysis about the outcome provided by the implemented model by considering a very important parameter that is time. From the comparison between the model with and without obfuscation we must say that even the obfuscation may increase small amount of time but for the Cloud provider, this time become negligible when the security of users is to be considered. Instead of using encryption process on the server which is proposed in some model, we must say obfuscation decreases the burden of server and so the provider can provide better services to its user. We also provided some other features in the model that are secure sharing and Integrity verification which increase the overall satisfaction level of the user and increase the trust towards Cloud providers.

References

1. Anca A., Florina P., Geanina U., George S., Gyorgy T. (2013) "Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud" Recent Advances in Applied Computer Science and Digital Services ISBN: 978-1-61804-179-1- Page 118–123.
2. Xiaojun Yu, Qiaoyan Wen (2010) "A View about Cloud Data Security from Data Life Cycle", International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, pp 1–4.
3. Juli C., Jayesh M. (2016) "A Framework to Secure Cloud Data Server Information Using Data Obfuscation" Technix International Journal for Engineering Research, Volume 2 Issue 08.
4. Martin M, Agnew G., Bole. J, Page M,, Rhodes W(2012) "Information Right Management & Digital Right Management" Published on the IEEE Emerging Technology Portal. (http://www.ieee.org/go/emergingtech).
5. Muhammad H., Ahmed E. (2012) "Cloud Protection by Obfuscation: Techniques and Metrics," IEEE Seventh International conference on P2P, Parallel, Grid, Cloud and Internet Computing.

6. Dr. L. Arockiam, Monikandan S. (2014) "Efficient Cloud Storage Confidentiality to Ensure Data Security" IEEE International conference on Computer communication and Information, jan. 03–05, coimbatore, India.
7. Atiq R., Hussain M. (2011) "Efficient Cloud Data Confidentiality for DaaS," International Journal of Advanced Science and Technology Vol. 35, October.
8. Arvind N., Vitaly S. (2013) "Obfuscated Database and Group Privacy", The University of Texas at Austin{arvind,shmat}@cs.utexas.edu.
9. Suthar K., Patel J (2015) "EncryScation: A Novel Framework for Cloud IaaS, DaaS security using Encryption and Obfuscation Techniques" In 5th Nirma University International conference on Engineering (NUiCONE) Dec.
10. Rabi P., Manas R., Suresh S. (2011) "Cloud Computing: Security Issues and Research Challenges". (IJCSITS) Vol. 1, No. 2.
11. Shilpashree Srinivasamurthy, David Q. Liu (2010) "Survey on Cloud Computing Security" Department of Computer Science, Indiana University – Purdue University Fort Wayne, Fort Wayne, IN 46805.
12. A Net 2000 Ltd. White Paper, "Data Masking: What You Need to Know" (http://www.Net.2000Ltd.com & Info@Net2000Ltd.com).
13. Christian C., Clark T., Douglas L. (2012) "A Taxonomy of Obfuscating Transformation", Department of computer science, The University of Auckland, Private Bag 92019 Auckland, New Zealand. {collberg,cthombor,dlow001}@ cs.auckland.ac.nz".