A Framework to Secure cloud Data Server Information Using Data Obfuscation

[1] Juli Chaudhari, [2] Jayesh Mevada
[1] M. Tech Student, [2]Assistant Professor,
[1] Department of Computer Engineering, MEC, Basna. India.
[2] Department of Computer Engineering, MEC, Basna. India.
[1]julichaudhari46@gmail.com,[2]jaymevada@gmail.com

Abstract - Cloud computing provide an high amount of virtual storage to the user. Cloud storage mainly help to small and medium scale industries to reduce their investment and maintenance of storage server. Users' data are sent to the cloud is to be stored in the public cloud environment. Data stored in the cloud storage might combine with other users' data. So, the issue about Security of cloud storage is ensured through confidentiality parameter. To ensure the confidentiality, the most common used technique is encryption. But encryption alone doesn't give maximum protection to the data in the cloud storage. To have efficient cloud storage confidentiality, this paper uses encryption and obfuscation as two different techniques to protect the data in the cloud storage. Obfuscation is same like encryption. Obfuscation is a process which disguises illegal users by implementing a particular mathematical function or using programming techniques. Obfuscation can be applied to a numeric type of data. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.

The proposed scheme, guarantees along with encryption, obfuscation technique is used to increase the confidentiality of data and also provide the right management .where the users data is secure on the server. We hope this paper will help quality analyst in pulling data, is secure to store in the cloud storage with more accuracy with higher speed and verify content by preserving privacy.

Index Terms - Cloud Storage, Obfuscation, Data protection, Confidentiality, De-Obfuscation.

1.INTRODUCTION

Cloud Computing and Obfuscation are the two emerging trends now a days in the world of information technology and computing. "Cloud computing refers to the web-based computing, providing users or devices with shared pool of resources, information or software on demand and pay per-use basis". It allows end user and small companies to make use of various computational resources like storage, software and processing capabilities provided by other companies such as Amazon or Microsoft.

Cloud Services provided by the clouds are broadly divided into three categories:Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Infrastructure as a service (IaaS): In the IaaS model computers are offered as physical or asvirtual machines, and other resources.

Platform as a service (PaaS): In the PaaS model, cloud providers offers acomputing platformincluding operating system, programming language execution environment, database, and webserver. Without buying and managing hardware andsoftware on a cloudplatform.

Software as a service (SaaS): In the SaaS model, cloud providers install andoperate applicationsoftware in the cloud and cloud users access the software from cloud clients.

"Data Obfuscation (DO) is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials. This form of encryption results in unintelligible or confusing data.**"** Data Obfuscation tasks include Storage & Encoding)split variables,convert static data to procedure & change encoding,change variable(, Aggregation)merge scalar variable & split,fold,merge arrays(, Ordering)reorder instance variables,reorder methods,reorder arrays (.

Data Obfuscation process……

- **Storage:** Used to choose unnatural storage class for dynamic & static data .
- **Encoding:**Encoding used to choose unnatural encoding for common data type.
- **Aggregation:** The main work of reverse engineering is to restore the program data structure.so, important for

Obfuscation is try to hide this data structure.

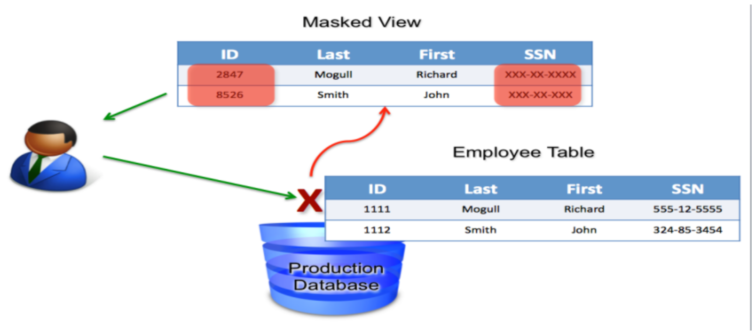
- **Ordering:**Randomizing the order in which computation are perform is useful obfuscation.

2. Background Theory

Data Obfuscation is also known as data scrambling and privacy preservation , that changing the data structure appearing in the source code. Data Obfuscation is to make attacking complicated enough to repel attacker ,rather than formally proving the strength of algoritham.

2.1 DATA OBFUSCATION:

Data Obfuscation in cloud computing is the designed approach of hiding data to perform security mechanism. The data obfuscation is a form of data masking where data is purposely scrambled to prevent unauthorized access to sensitive materials. Using data obfuscation we secure the cloud users data in the cloud storage and provide maximum security to user data in the cloud data.


Masked View
ID Last First SSN
2847 Mogull Richard XXX-XX-XXXX
8526 Smith John XXX-XX-XXX
Employee Table
ID Last First SSN
1111 Mogull Richard 555-12-5555
1112 Smith John 324-85-3454
Production Database

3. Related Work

Authorat [1] define the several techniques for technical protection software secrets. They argue that automatic code obfuscation is currently the most viable method for preventing reverse engineering .they describe large number of such transformation, classify them, and evaluate them with respect to their quality of an obfuscating transformation.

Authors of [2], present a survey of software protection based on the concept of security by obscurity. This paper present strength of Obfuscation technique using set of metrics. It describes three metrics: Potency (to what degree is human reader confused) , Resilience(how well are automatic deobfuscation attack resisted) and Cost(how many extra resource Used during runtime).

Authors of [3], use encryption and obfuscation as two different techniques to protect the data in the cloud storage confidentiality. Here, based on the type of data, encryption and obfuscation can be applied. so author use the three algorithm:
1. Used to find out type of data.
2. used for obfuscation (for numeric data type).
3. used for encryption (for numeric or alphanumeric data type).
The integration of both techniques should provide maximum security to user’s data in the cloud data.

Author [4]Here, the author make proposed model to maintain confidentiality of data , which stored in cloud database like DaaS .This model define ,user can encrypt or Obfuscate the data using any algorithm before it sending to server for storage. Here, confidentiality of data can not compromised. Proposed model also focus on query on encrypted and obfuscated data. The performance is also increase where only encryption technique used for confidentiality.

Author [5], define the new concept of privacy as group privacy against “mass harvesting” queries. It ensures that users of the obfuscated database can retrieve individual records or small subsets of records by identifying them exact. finally, it carried out in the random oracle model. Whether privacy-via-obfuscation can be achieved.

COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique usedwith the benefits that researcher gets the limitations found in schemes.

Criteria Group →	**Encryption/ Obfuscation oriented measures**								Others		
Individual Criteria → Providers ↓	**Cloud Storage**	**Data/Software Protection**	**Confidentiality**	**Encryption**	**Obfuscation**	**DaaS Security**	**Time Consuming**	**Group Privacy**	**Database Privacy**	**Algo/Flowchart Show**	**Experimental Setup?**
[1]	√	√	X	√	√	X	X	X	√	X	√
[2]	√	√	X	X	√	√	X	X	√	X	X
[3]	√	√	√	√	√	√	√	X	√	√	X
[4]	√	√	√	√	√	√	√	X	√	√	√
[5]	√	√	√	√	√	√	X	√	√	X	X

Table 1. Comparison study

4. Our contribution

Various researchers have worked to achieve better shown in figure 4.

4.1 Flow Chart

The proposed system flowchart based on Verification and Right management are the two of the main goals to be achieved in Security Data storage model for Cloud Computing. Both the operations in our model are achieved as mentioned beneath.

4.1.1 Uploading File on Cloud

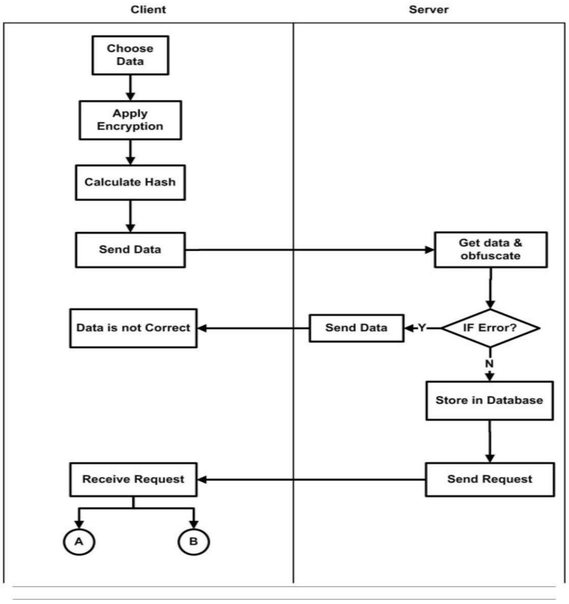


Fig. 2.Uploading file in cloud process

In Fig 2 shown we propose a process for Upload data on Cloud. So,client choose data for storage.Then client apply encryption and calculate hash value and send the data to the server.In other side,server get the data and obfuscate that data.If the data is correct then server store the data in the database and send the reply to the client.

(a)Verification Process

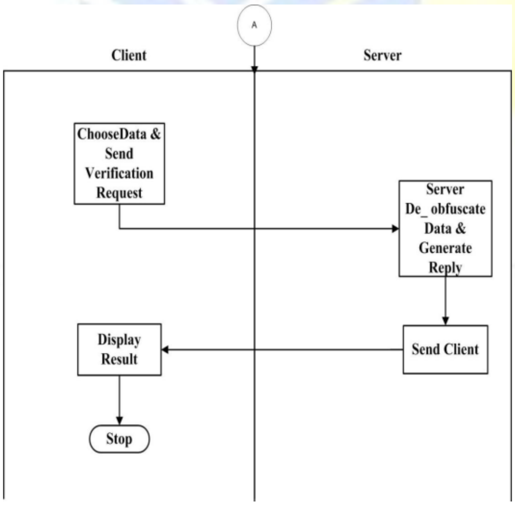

A
Client
Server
ChooseData & Send Verification Request
Server De_ obfuscate Data & Generate Reply
Display Result
Send Client
Stop

Fig. 3.Verification process.

In this process ,client chooses data and send verification request to the server.so,server de-obfuscate the client data and send reply to the client. After this, client compare the own hash code with coming reply and display the result.If the hash code is not match then there is something changes done at server side.

(b)Right Management Process

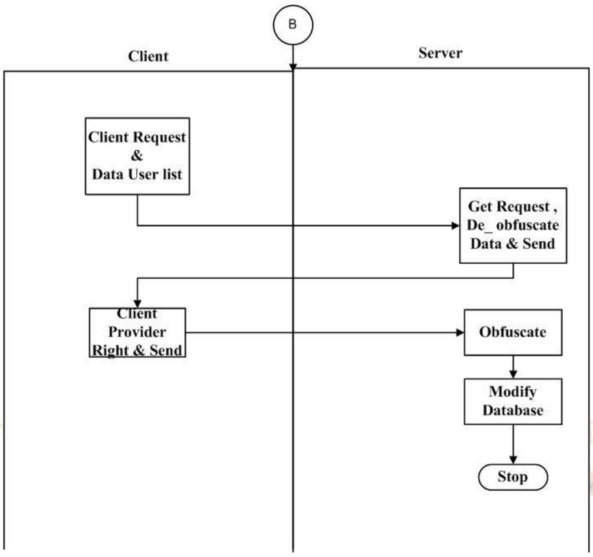

B
Client
Server
Client Request & Data User list
Get Request , De_ obfuscate Data & Send
Client Provider Right & Send
Obfuscate
Modify Database
Stop

Fig. 4.Right Management process.

In this process, Client request for data and user list .Then server De-obfuscate that data and send to the client. After that client send the rights and send to the server. The server again obfuscate that data and modify the database accordingly.

5.CONCLUSIONS

This paper explores the necessity of obfuscation with encryption in present information age. woh yduts ewObfuscation, along with encryption ot krowemarf desoporp ew oS .gnitupmoc duolc ni desu siachieve encryption,obfuscation,overhead,performance,speed/accuracy and privacy/integrity. The proposed model presented an approach to protecting users' confidential data in Cloud computing from Cloud service providers in the Cloud environment. The literature surveyed produces-Though data obfuscation we can conclude that the we required the model which will provides following outcomes. dohtem lacissalc yduts fo esac a sA of data obfuscation of obfuscation .

Data Confidentiality and Data verification facility for user.

We Increase trust of user on Service providers.

This system becomes more secure using obfuscation.

Data obfuscation enhances security of user's data.

Combined both the techniques solve existing issue of both Client & service provider.

We have proposed an idea for Upload Encrypted data on cloud and how to verify data and also provide right management to this uploaded data in server. We have tried to explore new ways using combine two methods,is encryption and obfuscation which achieve high security at server side in Cloud computing in short time. The obtained results optimal performance of each combination of algorithms.The proposed idea is yet to be implemented and tested under simulator or real-time environment before its adaptation or recognition, which is the forthcoming plan of action for us.

6. REFERENCES

[1] Dr.L.Arockiam and S.Monikandan ,"Efficient Cloud Storage Confidentiality to Ensure Data Security"2014 International conference on Computer communication and Information(2014 IEEE) ,jan.03-05,2014,coimbatore,India.

[2] Arvind Narayanan and Vitaly Shamatikov , "Obfuscated Database and Group Privacy", The University of Texas at Austin{arvind,shmat}@cs.utexas.edu,2013.

[3] Christian Collberg,Clark Thomborson,Douglas Low," 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"2012

[4] Muhammad Hataba and Ahmed EI-Mahdy, "Cloud Protection by Obfuscation : Techniques and Metrics,"2012 IEEE Seventh International conference on P2P,Parallel,Grid,Cloud and Internet Computing,

[5] Atiq ur Rehman,M.Hussain SZABIST Islamabad Pakistan,"Efficient Cloud Data Confidentiality for DaaS," International Journal of Advanced Science and Technology Vol.35,october,2011.

[6] Priyank Rajvanshi, Varun Singh Nagar, Priyanka Chawla , "Data Protection in Cloud Computing" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013.

[7] Sergey Vinogradov and Alexande Pastsyak,"Evaluation of Data Anonymization Tools" The Fourth International conference on Advances in Database,Knoweldge, and Data Application ,DBKDA 2012.

[8] S N Dhage, B B Meshram," Cloud Computing Environment" International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET,Mumbai, Insdia.

[9] Why Add Data Masking to Your Best Practices for Securing Sensitive Data, Dataguise Inc., Whitepaper, 2009. www.dataguise.com <retrieved: October, 2011>

[10] Data Solutions for Data Privacy, Direct Computer Resources Inc., Whitepaper, June 2010. www.datavantage.com <retrieved: October, 2011>

[11] Shilpashree Srinivasamurthy and David Q. Liu "Survey on Cloud Computing Security" Department of Computer Science,Indiana University – Purdue University Fort Wayne,Fort Wayne, IN 46805,2010.

[12] Cloud computing for e-governance. White paper, IIIT-Hyderabad, January 2010.Available online (13 pages).

[13] Vidyanand Choudhary. Software as a service: Implications for investment in software development. In HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, page 209a, Washington, DC, USA, 2007. IEEE Computer Society.

[14] Arini Balakrishnan, Chloe Schulze CS701 Construction of Compilers, Instructor: Charles Fischer, Computer Sciences Department, "Code Obfuscation Literature Survey," University of Wisconsin, Madison, December 19th, 2005

[15] Google app engine. http://code.google.com/appengine/.

[16] Christian S. Collberg and Clark Thombor-son. Watermarking, tamper-proofing, and obfuscation - tools for software protection.In IEEE Transactions on Software Engineering, volume 28, pages 735–746, August 2002.