A Survey: A Framework to Secure Cloud Data Server Information Using Data Obfuscation

[1]Juli Chaudhari,[2]JayeshMevada, [3]Krunal Suthar
[1]M.Tech Student,[2]Assistant Professor, [3]Assistant Professor
[1]Department of Computer Engineering, MEC,Basna. India.
[2]Department of Computer Engineering, MEC ,Basna. India.
[3]Department of Computer Engineering, SPCE,Visnagar. India.

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.Cloud storage is efficient for data storage. Users' data are sent to the cloud is to be stored in the public cloud environment. Data stored in the cloud storage might Combined with other users' data. This will lead to the data protection issue in cloud storage. If the confidentiality of clouddata is broken, then it will cause loss of data to the industry. 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 haveefficient 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.

In this paper we survey the current literature on data obfuscation and review current practices as well as applications. We analyse the different obfuscation techniques in relation to protection of software secrets,intellectual property and data. Surprisingly, the same techniques reverse engineers are used.

Index Terms - cloud storage, obfuscation,data protection, confidentiality, de-obfuscation.

I. INTRODUCTION

In today's IT industry, the more sophisticated data storage is cloud storage. but the enterprises are still waiting to use cloud computing, because of the data security problem of cloud computing is not solved completely. Cloud Storage provides a virtual space to store bulk data. But the data owners have no control over their data. The cloud provider has full control on the user's data. This makes the user's mind to think about the data security in the cloud.
Ensuring confidentiality of user's data in cloud storage is the main research problem around the cloud computing. Cloud storage providers store users critical data; it needs to be secured. Designed approach for encryption and hiding data to perform security mechanism. Using Technique of Encryption with Obfuscation, achieve high security level on data transmitting in cloud environment. Obfuscation is look for, only to resist attacking during small time. Cloud types include public, private (both external and internal), hybrid, and shared community types. With each type, you need to consider where data and functionality will be maintained.
This paper uses encryption and obfuscation techniques in an integrated manner to protect the data from the attackers (insiders and outsiders).obfuscation has been found to be the cheapest and easiest solution to this Problem. Encryption and obfuscation could be done from user's side.
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.
Section 2 illustrates Survey on various obfuscation techniques to secure cloud data server information. Section 3 contains overall comparison among all these approaches followed by conclusion in Section 4. Last section contains the list of references used.

II. SURVEY ON VARIOUS OBFUSCATION TECHNIQUE TO SECURE CLOUD DATA SERVER INFORMATION

Authors of [1], define the several technique 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 obsecurity.This paper present a strength of Obfuscation technique using set of metircs.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.

Authors of [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 notcompromised.Proposed model also focus on query on encrypted and obfuscated data.The performance is also increase where only encryption technique used for confidentiality.

Authors of [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.

III. 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 used with the benefits that researcher gets as well as 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 shown ?**	**Experimental setup?**
[1]	√	√	X	√	√	x	X	X	√	X	√
[2]	√	√	x	x	√	√	x	X	√	X	X
[3]	√	√	√	√	√	√	√	X	√	√	X
[4]	√	√	√	√	√	√	√	x	√	√	√
[5]	√	√	√	√	√	√	x	√	√	x	X

IV. CONCLUSION

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

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 VitalyShamatikov ,**"Obfuscated Database and Group Privacy**" ,The University of Texas at Austin{arvind,shmat}@cs.utexas.edu,2013.
[3]Christian Collberg,ClarkThomborson,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] AtiqurRehman,M.Hussain SZABIST Islamabad Pakistan,"**Efficient Cloud Data Confidentiality for DaaS**," International Journal of Advanced Science and Technology Vol.35,october,2011.

[6]PriyankRajvanshi, Varun Singh Nagar, PriyankaChawla ,**"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 AlexandePastsyak**,"Evaluation of Data Anonymization Tools"**The Fourth International conference on Advances in Database,Knoweldge, and DataApplication ,DBKDA 2012.
[8]S N Dhage, B BMeshram**," Cloud Computing Environment"**International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET,Mumbai, India.
[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]ShilpashreeSrinivasamurthy and David Q. Liu **"Survey on Cloud Computing Security"**Department of Computer Science,Indiana University – Purdue University FortWayne,Fort Wayne, IN 46805,2010.
[12]Cloud computing for e-governance. White paper, IIIT-Hyderabad, January
2010. Available online (13 pages).
[13]VidyanandChoudhary. Software as a service**: Implications for investment in software developmen**t. In HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, page 209a, Washington, DC, USA,2007. IEEE Computer Society.
[14]AriniBalakrishnan, 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, andobfuscation - tools for software protection.In IEEE Transactions on Software Engineering, volume 28, pages 735–746, August 2002.