Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
ISSN : 2395-7069 GIF: 2.7273, CIF: 4.964, Volume 05, No. 03, July-September, 2019, pp. 232-236

DATA MASKING WITH SECURITY METHODS ON CLOUD COMPUTING

Nidhi Maharishi*

ABSTRACT

Cloud computing is a technique with Information Technology infrastructure as distributed computing and virtualization. Cloud computing provides low cost, scalable computation capacity and services to organization on demand for expansion. Cloud computing with many beneficial features also handling the difficulty of protecting the security of data outsourced by cloud users. This paper objective is provide different models of cloud computing and emphasize on data protecting and security ways.

***KEYWORDS**: Cloud Computing, Service Models, Data Security, Data Masking Techniques.*

Introduction

A new IT infrastructure is a cloud computing which work as computing resources are provides different computing tasks and utility to computer users in the pay-as-you-go manner. Cloud computing provide shared processing resources on demand bases with its model for enabling ubiquitous, to access shared pool configurable resources. Cloud computing offers by integrating techniques like as Service oriented Architecture (SOA), virtualization, distributing computing and delivered measured services to cloud users anytime anywhere where internet is available and enable to access illusionary unlimited computing resources.

Cloud computing has classified by two ways by the offered types of servicesand by the cloud computing location.

Service Models of Cloud Computing

Cloud computing work with these models

- Software as a Service (saas)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

With these models to provide services cloud computing involves public cloud computing, private cloud computing, hybrid cloud computing and community cloud computing.

- **By the location has classified** in 1 public cloud: where the computing infrastructure hosted by the cloud vendor. 2 In private cloud: where the computing infrastructure assigned to specific organization and not shared to another organization. 3 In hybrid cloud where the private and public clouds work together. 4 Community cloud involves sharing of infrastructure in between organization of the same community.
    - **Authentication in Cloud Computing:** To access cloud computing services as a user is predefined that the person is authenticated or identified. Which means the user is already authorize for that service on server system through the application user interface on client side and permitted to accessing the stored information in the cloud. The different types of cloud public and private are using various modes for authentication with RSA. RSA cryptosystem allowed different ways for authentication like two factor authentication, knowledge based authentication and adaptive authentication. AWS (amazon web services)

* Faculty, Department of Computer Science, Kanoria PG Mahila Mahavidyalaya, Jaipur, Rajasthan, India.

is determined on the confidentiality of information when data transfer between the web server and the browser to connect with the virtual private cloud.In this context different authentication schemes are implemented, such as multifactor authentication, access management, AWS identity.

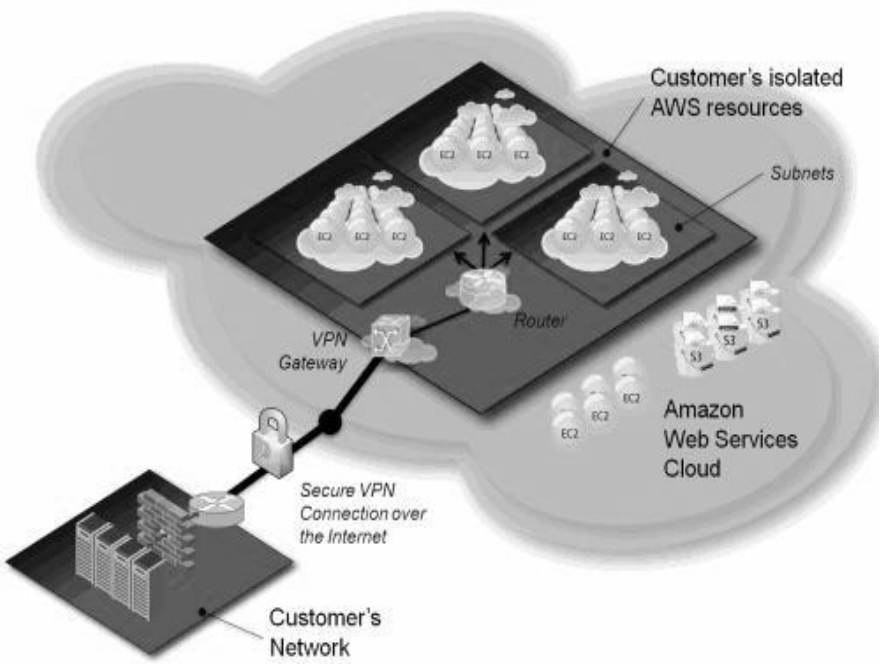


Figure: 1 In this figure multifactor authentication procedure from AWS. There is also a technique for authentication that is providing users to access through one time password in order to authenticate themselves to multiple services [3]. With this technique the users are prone to honeypot and dictionary attacks. The most famous IT companies are using this technique like Google, Microsoft, and Facebook.

This authentication method is used by AWS to protect the data in the cloud. Features of multifactor authentication mechanism are that enables identity or authenticate management and access management. Through Single password authentication is used from Facebook to enable data security in the cloud. Benefits of this type of authentication mechanism are that enables security from honeypot attacks and dictionary attacks.

- **Confidentiality in Cloud Computing:** Confidentiality is the most important security mechanism for users' data protection in the cloud. It adapts encryption of the plaintext convert in cipher text before the data is stored in the cloud. This technique protects the users' data and even cloud service providers cannot modify or read the content that is stored in this way in the cloud.

This type of protection is provided by Dell data protection and encryption, where users' data is protected when it is stored on the external drive or media. Encryption could be done either using software or hardware. Great benefit of this kind of protection is that users don't need to bother with the enforce policies of Dell data protection and encryption. Dell also uses Transparent File Encryption to control the users that are accessing the data. To make secure large scale data and provide efficient computing resources to potentially large scale applications, to handle large number of users presented in the system. It is challenging to efficiently and securely distribute the key(s) to authorize users which are requires to owner to stay online providing the key distribution to access encrypted data and decrypt by using decryption key service providing the key distribution service. Other issues that can be apply cryptography on system designthis technique based on data access control.

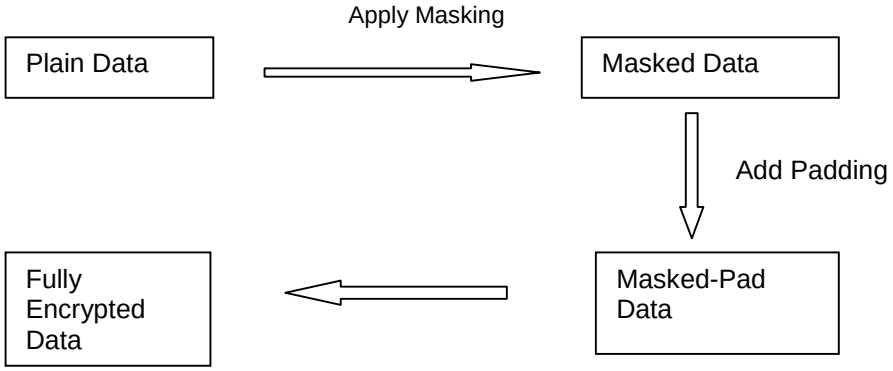
Here, we can conclude in this section that confidentiality is very important aspect for protecting the data in the cloud and different vendors offer different security techniques for ensuring the confidentiality with that we can compare here the methods of handling the cloud data in secure ways with

the handling the challenges to providing satisfying security assurance for the following folds of confidentiality are: data security versus usability, system scalability and dynamics, transmitted by cloud servers. Per example, DELL offers hardware and software based encryption, as well as transparent file encryption. The benefits of this kind of encryption techniques are that they are easy to implement and intervention of the user is not needed. Cryptography is using encryption techniques on personal computers and this method for encryption in the cloud gives advantage of the users for accessing the data. Online Tec

- **Data Protection in the Cloud:** Protection of data in the cloud is best accomplished when we have a mixture of encryption, data loss prevention techniques, integrity protection, authentication and authorization techniques. When vendors and enterprises use cryptographic algorithms, it is very important these algorithms to be well known as identified by NIST. It is also useful to have re-evaluation on an annual basis of the algorithms and keys that are utilized in order to be assured about the strength of the protection.

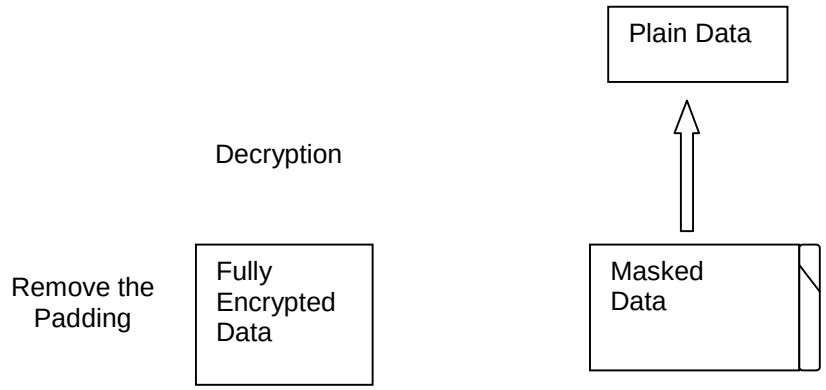
It is also very important organizations or corporations that are using cloud technology to understand the security controls that are related to the data in the cloud multi-tenant environment. Hardware Security Modules or HSMs are recommended to store the keys.

Sender Side



Explanation: in this diagram the encryption process takes place on plain text and masked the data after processing which not reflect the original data to invader. After the masking of data with the padding the data is more secure than before. Through that data is more securely transferred to the receiver and it gives us the double encryption.

Receiver Side



Explanation: At the receiver side, the reverse process happens of the sender. As shown in the above diagram the encrypted masked data is being decrypted doubly. As first the padding is removed after that removal of the padding we get the masked data. Yet the masking is removed from the data and then receiver obtains the original data.

Requirement of Data Masking

- When sensitive data is copy outside of product environment.
- Sending the test to cloud.
- Moving data to vendors.
- Leverage for moving development/consultant.

Different Types of Masking

- **Static Data Masking:** This data masking is used by most organization when they create testing and this is the only possible masking method which using outsourced developers at a separate location or a company. At these cases it is necessary to duplicate the database. When doing it, it is critical to use a static data masking tools. These tools have sure that all important data is masked before sending it out from the organization. Static data masking provides a core level of data protection by creating offline and testing database using a standard ETL procedure.
- **Dynamic Data Masking:** Dynamic data masking is a strategy to control over the unauthorized access of data, where data streams is transferred from a database or production environment or which have masked they are requested. Dynamic data masking is provides benefit for the cases where individuals working are close to production environment which could not have access the original data. For example, the staffers or contractors may be trying to troubleshoot or update the data base then they can access duplicate data base.

Data Masking and the Cloud

In current times, enterprises are develop their self new applications in the cloud. The cloud solution are allows organizations to access IaaS, PaaS, SaaS. There are many models of generating test and varies it to the cloud. In SDLC process data masking becomes the part of it with the development environment.

Data Masking Techniques

- **Substitution:** This technique is the most effective method to applying data masking and efficient to preserve the authentic face of the data records. This substitution technique dwells of randomly replacing the contents of a column of data with information that looks similar but is completely unrelated to the real details. For example, the surnames name in the customer database can be sanitized by replacing the real last names with surnames haggard from a largish random list. Substitution data can sometimes be very hard to find in large length - however any data masking software should contain datasets of commonly required items.
- **Shuffling:** Shuffling is similar to get substitution in running process except that the substitution data is arrived from the column itself. In simple ways the data is randomly shuffled with the column. It is effective for small amounts of data.
- **Encryption:** Encryption is one of the most effective methods to solve the data masking problem. The encryption technique algorithmically composes the data. This usually does not prove the data looking realistic and can many times make the data larger. Encryption also deletes the formatting of the data. Encrypted data least looks meaningful; in fact, it usually shows as binary data. Encryption sometimes has to character set issues when modifying encrypted varchar fields. Certain types of encryption obligate constraints on the data format. That means the data fields must be extended with a appropriate padding character which must be stripped down at decryption time.

Conclusion

The main goal of this work was to analyze and evaluate the security methods and data masking techniques for data protection in the cloud computing. For that purpose we analyzed and evaluated the most important security methods for data protection that are already accepted from the cloud computing service providers like amazon, google, etc. We classified them in three sections according to the security mechanisms that they provide: authentication, confidentiality and protection methods. Generally most of the organization needs combination of dynamic and static database masking. In this paper we have discussed about the cloud services models and security methods in cloud by using data masking techniques. Storage of data on the cloud describes with themultifactor authentication procedure from AWS that defines the way how to manage the storage of database at cloud and authenticate access the data from the cloud.

References

- A Survey on Recent Trends, Process and Development in Data Masking for Testing Ravikumar G K1 ,Manjunath T N2, Ravindra S Hegadi3,Umesh I M4
- Amazon aws,http://aws.amazon.com
- C. I. Fan and S. Y. Huang, "Controllable privacy preserving search based on symmetric predicate encryption in cloud storage", Future Generation Computer Systems, 29(7), **(2013)**, 1716-1724.
- D. W. Chadwick and K. Fatema, "A privacy preserving authorization system for the cloud", Journal of Computer and System Sciences, 78(5), **(2012)**, 1359-1373.
- Data Masking: What You Need to Know What You Really Need To Know Before You Begin A Net 2000 Ltd. White Paper.
- Data Sanitization TechniquesA Net 2000 Ltd. White Paper.
- DATA SECURITY IN THE CLOUD :Mr. Jiten Prithiani MCA Final year Student ,V.E.S. Institute of Technology, Mumbai, India jiten.prithiani@ves.ac.in,Mrs. Dhanamma Jagli, Department of MCA, V.E.S.Institute of Technology ,Mumbai, India
- Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing Ravikumar G K, Dr. B. Justus Rabi,Dr MGR University, Chennai, Tamil Nadu, INDIA
- Federalinformation security management act, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
- G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, 30(5), **(2011)**, 320-331.
- Google app engine,http://code.google.com/appengine
- L. Badger, T. Grance, R. Patt-Corner and J. Voas, "Cloud computing synopsis and recommendations (draft), nist special publication 800-146", Recommendations of the National Institute of Standards and Technology, Tech. Rep. **(2011)**.
- T. Acar, M. Belenkiy and A. Küpçü, "Single password authentication", Computer Networks, 57(13), **(2013)**, 2597-2614.
- The invisible things lab's blog, http://theinvisiblethings. blogspot.com/ 2006/06/ introducing- blue-pill.html
- U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, "Cloud based secure and privacy enhanced authentication & authorization protocol", Procedia Computer Science, 22, **(2013)**, 680-688.

❍❍❍