RESEARCH REVIEW JOURNALS
Volume-04
Issue-04
April -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Study on Cloud Computing and Data Masking Techniques

[1]Shweta Rana, [2]P.Alagu Manoharan & [3]R. Arko Bagchi

[1]Research Scholar, Department of Computer Science & Engineering, Global Institute of technology & management (Affiliated by MDU University rohtak, HR) (India)
[2,3]Assistant professor, department of computer science & Engineering, Global Institute of technology and management (Affiliated by MDU University rohtak, HR) (India)

ARTICLE DETAILS
Article History
Published Online: 15 April 2019

Keywords
Cloud Computing, Deployment Models, Service Models, Data Security, Data Masking Techniques..

ABSTRACT
Cloud computing is a technology, that offers significantly less cost, scalable computing power and solutions to businesses on need for enlargement. Although, cloud computing is facilitating the Information technology business, re-search and advancement in this particular area remains to be positive. Cloud computing resources provided service on an as needed foundation, and also delivered by IP based connectivity, offering extremely scalable, reliable on demand services with grateful management capabilities. You will find a great deal of improvement in the cloud computing, protection of the information in the cloud is now the one of significant characteristics in the cloud computing. Cloud computing is only the sharing of the materials within an open atmosphere which results to the security risks. This paper aim is providing non identical models of data and cloud computing masking strategies for providing security.

1. Introduction

Cloud computing is a technology, that offers significantly less cost, scalable computing power and solutions to businesses on need for enlargement. Although, cloud computing is facilitating the Information technology business, re-search and advancement in this particular area remains to be positive. Cloud computing resources provided service on an as needed foundation, and also delivered by IP based connectivity, offering extremely scalable, reliable on demand services with grateful management capabilities. You will find a great deal of improvement in the cloud computing, protection of the information in the cloud is now the one of significant characteristics in the cloud computing. Cloud computing is only the sharing of the materials within an open atmosphere which results to the security risks. This paper aim is providing non identical models of data and cloud computing masking strategies for providing security.

It is totally an internet based technology in which client data is stored and supported in data center of cloud provider like Google, Amazon, and Salesforce.com etc. The resources in cloud system are translucent for the application and the client do not know the place of resource. The client can acquire your application from anywhere. The amount of resources presuming in the cloud system for the cloud system for the client is increased when their requirements are high and decreases when their requirements are less. The cloud computing can be seen as the important change of information industry and will make more influence on the development of information technology for the society.

1.1. Advantages of Cloud Computing:

1. **Reduced Cost-** Cloud technology is paid step by step saving the money of organizations.
2. **Increased storage-** Organization can store more data than on private computing systems.
3. **Highly automated-** IT personnel need not to worry about keeping software up to date.
4. **Flexibility-** Cloud computing provides much more flexibility than past computing methods.

2. Cloud computing service models:

Three types of cloud computing services models:

2.1. Software as a Service (SaaS): It is the top layer provider in which customer will ready to use applications running on the infrastructure provider. SaaS can be described as a process by which Application Service Provider (ASP) provide different software application over the internet. SaaS applications are designed for end users, deliver over the internet. It enables the customer to elimination of installing and operating the application on his own computer and also get rid of the huge load of software maintenance. With SaaS a provider licenses an application to the customer as a service on demand via subscription.

Generally the customer is only able to alter the parameters of the application that have been exposed by the provider. The customer should have knowledge about protecting data against administrative access by the provider.

The buyer should be aware of data encryption strategies that are put on to information. The buyer has to understand just how safe details, as specified in their information classification, is being managed on the whole and by configuration options. Salesforce, Zoho, workday are drawings of SaaS that are used for e-mail, billing etc.

SaaS programs operate on a SaaS provider's servers. The provider controls a chance to access the software, availability, including security, and performance. SaaS clients have no need of application or hardware to purchase, maintain, install, or alter. It acquires to apps is easy. User simply requires a connection to the internet. This cloud computing distribute one

program through the internet browser to thousands of buyers using architecture. On the buyer side it means no investment in servers or maybe software licensing as well as on the provider side only one app to keep, expenses are minimal as compared to standard hosting. Office program is the greatest instance of organizations in SaaS. Jobs regarding accounting, preparation and sales could all be performed through Software as a program. In an organization everybody who must acquire to a specific piece of software could be set up as a person, whether it's one or maybe 2 individuals or maybe every employee.

Benefits of SaaS:

1. SaaS helps to maintained software from a central location.
2. The user can sign up and quickly start using innovative business apps.
3. Software distributed in a 'one to many' model.
4. There is no setup costs with SaaS, as these are accessible with other applications

2.2. Platform as a Service (PaaS):

It is a middle layer which produces platform oriented service. In this customer has responsibility for application arrangement and to provide securing access to the application itself. PaaS is useful for situation where several developers doing a development project. Here the customer doesn't manage the essential cloud infrastructure like network, or storage, operating systems, servers, but it command over the deployed programs and perhaps configuration adjustments for the application hosting environment. Google App Engine, Load Storm would be the instances of PaaS for executing web applications over internet.

PaaS is really a integration of a development platform along with a fix stack, sent as a program on demand. It offers framework where software developers are able to develop brand new applications or even expand existing ones without the price and complexity of purchasing and controlling the hardware and software program. The buyer uses a hosting setting for the apps of theirs. Most cloud offerings, PaaS solutions are typically paid out for on the foundation of contract with clients.

Benefits of PaaS:

1. Develop application and get to market faster.
2. Integration with web services and databases via common quality
3. Reduce complexity with middleware as a service.
4. Teams in various locations can work together
5. Makes development possible for ‗non-experts‘

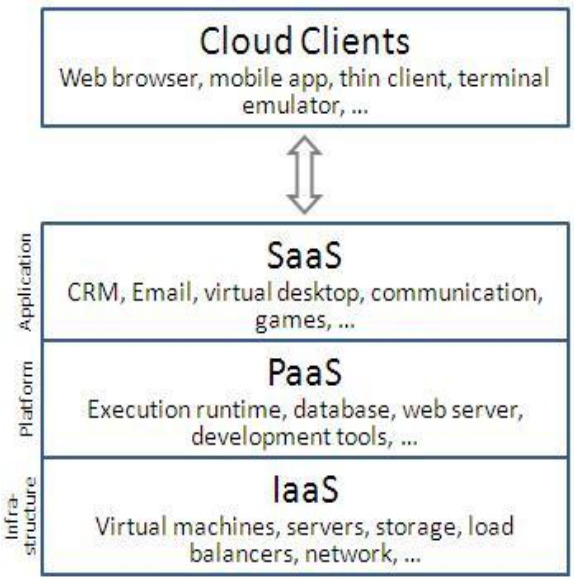
2.3. Infrastructure as a Service (IaaS)

IaaS can be utilized by enterprise customers to create cost successful and easily scalable IT solutions where the complexities and expenses of managing the elementry hardware are outsourced to the cloud provider. The user can buy the infrastructure according to the requirements as an alternative of buying the infrastructure that might not be used for months. IaaS works on a —Pay as you got model. For a startup or small business; one of the most difficult things to do is keep capital disbursement under control. In cloud you have the ability to extend as if you owned your own hardware and data center that the users pay for only what they are using. Virtualization enables IaaS providers to offer almost unlimited circumstances of servers to customers and make cost-effective use of the hosting hardware.

Benefits of IaaS:

1. Infrastructure scales on demand to hold up dynamic workloads.
2. Generally involves multiple users on a single piece of hardware.
3. Flexible and ingenious services are available on demand.
4. There is no need to invest in your own hardware.

Physical security of data centre position



3. Deployment models

Deployment models are used to define the type of accesses to the cloud i.e. how the cloud is located? Cloud can have four types of entrance: Public, private, Hybrid and community.

3.1. Public cloud:

Public cloud that is based on regular cloud computing, services might be free or provided for a pay-per-use model. The public cloud allows services and program being approachable to general public. Public cloud could be less secure since it's open to everyone. Public clouds offer service, typically over a web connection. A public cloud is resting on the web and meant to be utilized by any person with a web connection to offer a the same range of services and abilities. Public cloud customers are mainly residential customers and also attached to the public via online service provider's network. Google, Microsoft and Amazon are good examples of public cloud which offers the solutions of theirs to the general public.

Public cloud providers put a cap on the infrastructure and information necessary for its users. Organization is able to use public clouds to generate their operations remarkably much more systematic, for instance, using the storage of non sensitive content, online document collaboration and webmail.

While one of the leading bariers facing public cloud computing is protection, the cloud computing prototype offers opportunities for foundation in provisioning security solutions which keep the possibility of improving the overall security of several businesses. Organizations must entail that any selected public cloud computing remedy must be configured, deployed, and maintained to satisfy the protection of theirs along with other needs.

The public cloud provides following benefits:

1. Public cloud provides supreme scalability.
2. Cloud services like IaaS, PaaS, SaaS attend the public cloud, so it is more flexible.
3. It is Location independence means its services are accessible through internet whenever the client is required.
4. Public cloud is also cost effective because it brings together resources which are shared by all successive cloud services.

***3.2. Private cloud**:*

A personal cloud has much more protection than public clouds. It's located within an organizations inner enterprise information centre. The scalable resources and also virtual applications offered through the cloud vendor are making together that are ideal for cloud people to talk about and use. The applications of individual are significantly safer than that of the public cloud due to its specified internal vulnearbility.

The group is able to access to operate on a certain Private cloud. Firms are making up your mind the personal cloud proves less risky. The capability of Private cloud is usually to virtualize services, increases hardware use, ultimately reducing complexity and also costs.

Main materials of any companies are its energy and its information. The major limitation of individual cloud is its higher price. When collation are developed with public cloud the expense of buying equipment, software typically leads to higher costs to a company in private cloud. Nevertheless, under the personal cloud version, the cloud is just possible by an individual business providing that organization with privacy and management. A personal cloud that is in addition known as an inner Cloud busy with within the business planet along with its access is restricted usually to company personnel and business partner.

Private cloud offers following benefits:

1. Flexibility and scale will meets client demands.
2. Resource sharing surrounding by a large number of users.
3. Payment as stated by use of the services.
4. Use of technologies and internet protocol to approach cloud resources.

3.3. Hybrid Cloud:

A Hybrid Cloud is an integrated cloud services that employ both public and private cloud to do well defined features inside the same business.

It is able to in addition be defined as a number of cloud methods which are attached in manner allowing information and programs being moved very easily from a single system to another. It's a arrangement of more than one personal cloud and a minimum of one public cloud. This computing model mreges the security advantages associated with a private cloud and public cloud. Hybrid Cloud delivers much more secure command of the data and uses allowing different parties to access info over the Internet.

A hybrid cloud suggested in a single of 2 ways: a vendor has a personal cloud and then launched a partnership with a public cloud provider, or maybe a public cloud provider launched a partnership with a vendor that contributes private cloud. In hybrid cloud, a company handles several materials in home and a little out house. Generally, the hybrid approach allows a company to have advantages of the scalability and also cost effectiveness that the public cloud computing environment propound without exposing data to third party vendors.

Hybrid Cloud offers following benefits:

1. The hybrid cloud gives security as the private cloud element of the hybrid cloud model gives the security where it is needed for tactful operations and also satisfy customer needs for data handling and data storage where it is applicable.
2. Gives reinforcement for cloud-bursting.
3. The hybrid cloud gives flexibility as the availability of both secure resource and scalable cost effective public resource can give organisations with more opportunities to prospect for different operations.

4. System architecture:

The architecture of cloud computing deals with the components and subcomponents required for cloud computing. These components consist of a front end platform which consist of fat client, thin client, mobile device back end platforms which consist of servers, storage. These integrated, components make up cloud computing architecture. Security is very essential issue in cloud computing. Data masking is the job of hiding original data with random characters or data. The main aim of data masking is to protect data that is categorized as personal identifiable data or sensitive data. In data masking data may be updated in different methods involves encryption, character stuffing and character of word substitution.

The complete implementation of Data Masking at an organizational level should be tightly coupled with the Test Management, underlying Methodology and should integrated processes for the distribution of masked test data subsets

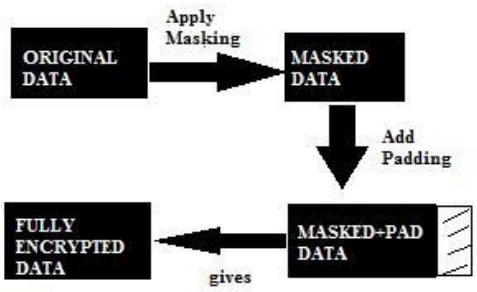
***4.1. Working of proposed System**:*

This process manifests how we encrypt the data so that the intruder does not know what the actual data is about.

In this we use Data Masking and accompanied by the padding of data is applied

4.2. Data Security In The Cloud

1) Sender Side:

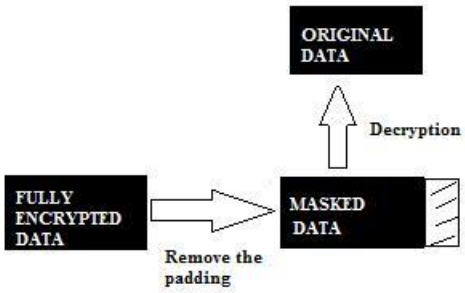


Explanation:

In the above diagram, the encryption process comes about at the socket layer of the sender side.

The diagram shows us that the mask is applied to the data so that the original data is not being review to intruder. After masking, the data is applied with the padding and hence the data is much more secure than it was before. It provides us the double encryption of the data and hence the data is more securely transferred to the receiver.

2) Receiver side:



Explanation:

At the receiver end, reverse the process of the sender is applied.

In this as shown in the diagram, the data which are encrypted double time is being decrypted double time.

At first step Padding of the data is removed and after the removal of the padding we get he masked data.

Now the masking of the data is being removed and hence the receiver gets the original data.

4.3. Need of Data Masking:

1. When copy the sensitive data outside of production environment.
2. Transferring the test data to cloud.
3. Sending data to the vendors.
4. Support off-shore development/consultant.

5. Different types of masking

5.1. Static data masking

Static data masking is used by many organizations when they create testing and is the only feasible masking method when they using outsourced developers in an individual location or an individual company. In these cases it is mandatory to duplicate the database. When doing so, it is censorious to use a static data masking tools. These tools make sure that all delicate data is masked before sending it out from the organization. Static data masking gives a basic level of data protection by creating an offline or testing database using a standard ETL procedure.

The static data base can be amended repeatedly, for example on a daily or weekly basis. This is not a security risk, but it has conclusion for a various tests and development issues.

5.2. Dynamic data masking:

Dynamic Data Masking (DDM) is a policy for managing or restricting unauthorized access to data, where data streams from a database or production environment are transformed or masked as they are requested. Dynamic data masking gives result for the cases where particulars are working close to the production environment, but should not have access to the original data. For example, contractors and staffers are trying to troubleshoot or up to date a production database. It is important that they do not have access to delicate information such as individual health data, credit card numbers, etc. —with DDM, the information is twisted or otherwise updated, so that these technicians are working with harmless data as they manipulate a database.

5.3 Data Masking and the cloud

In recent years, organizations progress their new applications in the cloud. The cloud solution now allows organization to use IaaS, PaaS, SaaS. There are many models of creating test data and moving it to the cloud. Data masking enhances the part of these processes in SDLC as the development environments.

6. Data masking techniques

6.1. Substitution

Substitution technique is regarded as the effective technique of using data masking and ready to sustain the bona fide appearance of the information records. This method includes of arbitrarily replacing the items in a column of information with info which seems similar but is totally not associated with the actual specifics. For instance, the surnames inside a customer database can be purify by changing the real final names with surnames drawn from the largish random list. Substitution data is often hard to find in big length - however a data masking program should include datasets of regularly needed items. For instance, to cleanse surnames by substitution, a summary of random last names should be publicly available. Then to sterilize telephone one figure, a summary of phone numbers should be publicly available. The exchange method have to be used for most of the fields in DB system like phone numbers, zip codes, credit card numbers along with other card type numbers like Social Security numbers.

6.2. Shuffling

Shuffling is connected to substitution except that the substitution information is produced from the column itself. In easy terms the information is randomly shuffled together with the column. Shuffling is advantageous for small amounts of information. An additional evaluation is definitely the algorithm utilized to shuffle the data. If the shuffling strategy could be solved, then the information can be quickly —unshuffled. For

instance, if the shuffle algorithm quickly ran on the table swapping the column information between each number of 2 rows it wouldn't take work that is much from an interested party to return items to their unshuffled state. Shuffling is scarcely beneficial when used on tiny quantities of information. For instance, if we have just five rows in a table it perhaps won't be much too hard to determine that of the shuffled data truly is owned by which row. On another hand, when a column of numeric data is shuffled, the amount and typical of the column still exercise to exactly the same amount. It's occasionally useful.

6.3. Encryption:

Encryption is among the toughest methods to resolve the details masking problem. The Encryption technique algorithmically misunderstands the data. This typically doesn't leave the information looking realistic and may sometimes make the information larger. Encryption also can demolish the formatting and also feel and look of the information. Encrypted data scarcely looks meaningful; in fact, it typically is like binary data. This regularly causes character set issues when manipulating encrypted varchar fields. Certain kinds of encryption inflict constraints on the information format also. It means that the fields have to be elongated with a good padding character which should next be stripped off at decryption time.

7. Conclusion

Normally many organization needs combination of dynamic and static database masking. In this paper we study about the cloud services models, deployment models and security in cloud by using data masking techniques.

Storage of data on the cloud clerify the way we manage the storage of data and access the data from the cloud. In this paper it is also declared about the various cryptography algorithms which help us to encrypting the data at sender side and then transferring it to the receiver side.

This paper also surveys the need of data masking in present information. Data masking will enable us to manage the following:

a) Expand protection against data theft.
b) Carry out 'need to access'.
c) Gives realistic data for testing, development and data sharing.
d) Gives a heightened sense of security to clients, employee and supplier.

References

1. Research on Cloud Data Storage Technology and Its Architecture Implementation Kun Liua, Long-jiang Donga
2. An Advanced Survey on Cloud Computing and State-of-the-art Research Issues
3. Cloud Computing Security Issues And Challenges Pranita P. Khairnar, Electronics Department, Amrutvahini College of Engineering, Sangamner Prof. V.S. Ubale Asst. Prof. Electronics Department, Amrutvahini College of Engineering, Sangamner
4. Various Issues & Challenges of Load Balancing Over Cloud: A Survey Palak Shrivastava1 Sudheer Kumar Arya2
5. Dr. Priyanka Tripathi3 Research Scholar National Institute Of Technical Teachers Training & Research Bhopal, India shrivastava,Associate Professor National Institute Of Technical Teachers Training & Research Bhopal, India
6. International Journal of Advanced Research in Computer Science and Software Engineering
7. Identity – Based Secure and Flexible Data Sharing in Cloud Based Smart Grid R. Ruhina Student, (SE), Department of
8. Computer Science and Engineering, JNTUA College of Engineering, Anantapuramu, Andhra Pradesh, India
9. 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
10. 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
11. Data Masking: What You Need to Know What You Really Need To Know Before You Begin A Net 2000 Ltd.
12. White Paper.
13. Swot Analysis of Mobile Cloud ComputingA.M.S.Zunaitha Sulthana*, L.Clara Mary*, A.SangeethaDepartment of computer science, MIET Institution, Trichy
14. A Survey on Recent Trends, Process and Development in Data Masking for TestingRavikumar G K1 ,Manjunath T N2, Ravindra S Hegadi3,Umesh I M4 [11] Data Sanitization Techniques*A Net 2000 Ltd. White Paper*

