INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A STUDY ON SECURITY & PRIVACY IN "PUBLIC CLOUDS WHILE ADOPTING CLOUD SERVICES"

Murali Krishna[1], Govardhan[2]
[1]murali.bedarakota@g mail.com
[2] govardhan_cse@jntuh.ac.in

Author Correspondence: Hyderabad, + 919291539783, murali.bedarakota@gmail.com

Abstract
Cloud Computing provides fastest way of computing than traditional client server model. Now days, many software companies are offering cloud services to various customers. There is lot of benefits for both cloud service providers and customers such as reduced capital cost, Improve Accessibility, Globalizing the workforce etc., at the same time most of the customers are willing to use cloud services. This creates a serious problem towards customers for the security of the important business data as the data is stored in the cloud owns by unknown provider. This may lead to losing privacy of the customer's business details. In this paper we discuss possible security and privacy threats when considering the adoption of cloud services and some possible solutions to them.

Keywords: Cloud, Security, Privacy, security and privacy threats.

1. Introduction

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on our own hard drive or updating applications for our needs, we use a service over the Internet, at another location, to store our information or use its applications. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications.

It has different types of service models such as Software as a service, Platform as a service Infrastructure as a service with different types of deployment models such private cloud , public cloud ,community cloud, hybrid cloud . Cloud service providers offer different types of clouds based on customer requirement. Most of the small and medium sized companies are adopting the cloud services in recent trends.

2. Security Problems

When an Entrepreneur stores the data in one of the cloud service provider he needs to access the information of his own interest which is located geographically at remote location, it involves various security and privacy problems.

2.1 Trust in Cloud Vendors

When using the cloud services user should be aware of the data that is stored to the cloud leaves the control to the cloud service provider. The main problem arises here is required trust between cloud provider and customer.

2.2 Accessing Data through Internet

Cloud Computing means Internet Computing. Data, Applications anything related to cloud must be accessed only through the internet. This may create a big problem towards data security.
It leaves the Hackers to steal the information easily from Internet .They may manipulate the data for their benefit in different businesses such as Retail markets, Banking, Government websites etc.,
Cloud data is accessed from anywhere on the internet if a data gap occurs via hacking or careless username or password security, the data can be compromised.

2.3 Confidentiality and Integrity

The customer must store the information in the cloud only through the network , as the service provider may be located somewhere from the customer's location and at the same time cloud provider should also send the results back to the customer through the internet which is far away from storage. This leads to hack the data very easily. The hacker who has the details of username and password can easily alter the data it leads to the lack of integrity of the data. Hacker can also download the data which leads to the loss of confidentiality of the data. The attackers learn the application logic and use this logic in other applications which may lead to high yielding benefits to the attacker. In the same way attacker can easily steal the application logic many times till the customer has agreement .Malicious actions can be done on the name of customer identity.

3. Privacy Problems

Privacy is even more important when it comes to cloud storage. Cloud Vendors may not maintains trust towards customers. Some service providers may sell the data to the organizations who has the urgent need of it. Many of the vendors don't care about the privacy of customer data as the costs will increase if they use the high level security tools. Some service providers may scan the documents with out the legal permission from the customer violating Privacy of the customer data.

4. Possible Solutions:

4.1 Integrity

Storing of the applications in two or more public clouds gets the clarity of the results of application. The customer when using one cloud may be in doubt that the result provided by cloud provider is correct. Now the customer can compare the results from two or more clouds to confirm the business between the cloud provider and customer is trust worthy. It also provides the integrity of the results of the application. It does not provide confidentiality.

4.2 Data Leakage

In recent studies Google documents has a flaw of accessing their data by anyone who even doesn't shared with them. To reduce this data leakage the application logic and data storage must be tightly integrated as many of the software as a service business applications are implementing. The data should not be directly accessible by the application. Complex authentication mechanisms can be used to protect the data. Application logic and data should be stored in two different clouds.

4.3 Confidentiality

The data and processing logic should be hidden to the service request and also to the cloud provider.
The logic of the application should be spitted and evenly distributed in different clouds. By this way cloud vendor can know only some information about the application .Cloud vendor cannot gain full knowledge about

the application. This reduces the risk of violation of confidentiality. Usage of more number of clouds provides greater chances to confidentiality.

4.4 Encryption

The data should be safeguarded while it is processing, for this purpose the user should use the encryption techniques. There are different types of Homomorphism encryptions used such as Fully-homomorphic encryption (FHE), somewhat homomorphism encryption (SHE), searchable encryption, structured encryption, functional encryption. In this technique the operation are performed on the cipher text and the results are generated in encrypted form. In this case the user only can encrypt and decrypt the data. The cloud vendor has no chance to operate on the plain text .cloud vendor loses the ability to see the data. The complete process is going to happen through the network, as the use of homomorphic encryptions the attackers can not be able to hack the data.

4.5 Data Splitting

The application data is of two types structured and unstructured. Data can be splitted by considering three factors such as

a) Volume-- How much data will be stored?

b) Velocity-- What is the rate at which your data will grow? Is it an internal app that isn't generating a lot of data? An external app that customers will be uploading images and videos into?

c) Variety – What type of data will you store? Relational, images, key-value pairs, social graphs?

There are basically three types of splitting. They are vertical splitting, horizontal splitting, Hybrid splitting.

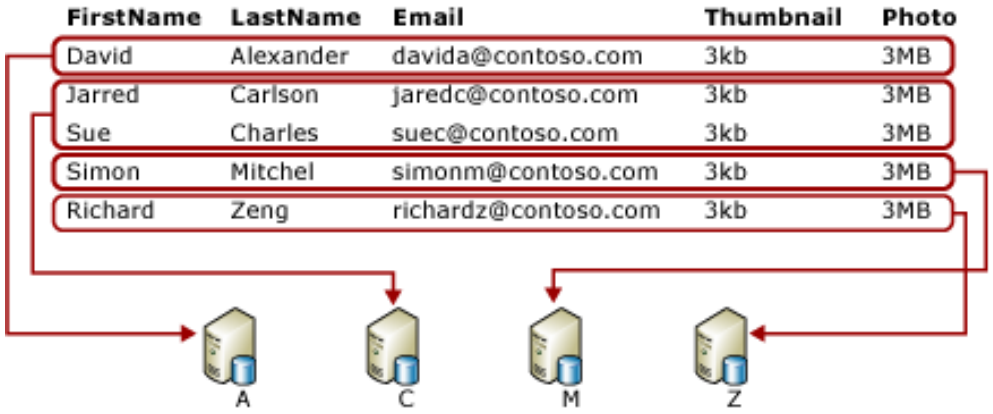
Vertical splitting

The Structured data is stored in one cloud and unstructured data is stored in another cloud. For example when we consider a table of data whose columns has First name, Last name, Email, Thumbnail, Photo.

All the First three columns are stored in one cloud and last two columns of data are stored in other cloud, this technique is vertical splitting.

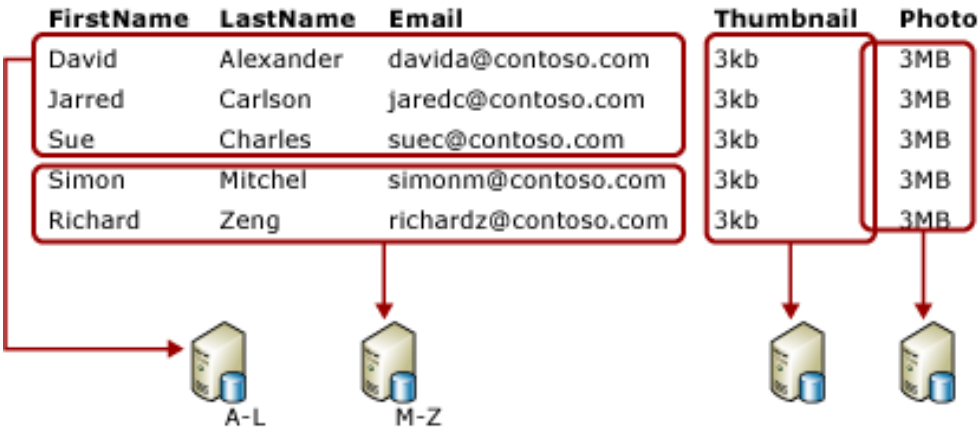
Horizontal splitting

Horizontal portioning is like splitting up a table by rows: one set of rows stored into one cloud, and some set of rows goes into a different cloud. There is no restriction of using limited number of clouds.



Hybrid splitting

The combination of vertical and horizontal splitting defines hybrid splitting.



5. Conclusion

In this paper, we discussed various security problems and privacy problems while adopting cloud services by making use of extra clouds.

6. REFERENCES

[1] Tom Dykstra, Mike Wasson and Rick Anderson 2014 Data Partitioning Strategies (Building Real-World Cloud Apps with Azure).

[2] J. Somorovsky, C. Meyer, T. Tran, M. Sbeiti, J. Schwenk and C. Wietfeld, &ldquo,SeC2: Secure Mobile Solution for Distributed Public Cloud Storages,&rdquo, Proc. Second Int',l Conf. Cloud Computing and Services Science.

[3] Arvind Arasu, Ken Eguro, Raghav Kaushik, and Ravi Ramamurthy- Querying Encrypted Data