ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/97900, November 2016* ISSN (Online) : 0974-5645

Data Security is the Major Issue in Cloud Computing - A Review

G . Monika* and Y. Kalpana

Department of Computer Application, Vels University, Chennai – 600117, Tamil Nadu, India; aakinomm@gmail.com, ykalpanaravi@gmail.com

Abstract

Objectives: Cloud computing is a vast technology which is growing very fast in the IT environment. The cloud computing faces many security issues both in the service provider side and client side. **Methods/Statistical Analysis:** This paper carries forward the analysis of security issues and its solutions. There are many issues discussed earlier some are with solutions and encryption techniques. Few issues are still with unfound solutions too and researchers are trying to solve them. Cloud computing has problem with storage procedure since the data are stored in the data center far away from the source system. Many common security issues are discussed in the paper and the major security is taken as the data security. **Findings:** This paper says that data security is the major issue in the security concern because both the service provider and client are worried about the data. The data is the target for the hijackers for attacking the data center server. The data security issues are also analyzed and some solutions are discussed in this paper. **Applications/Improvements:** Further this paper could be enhanced by broadly discussing the solutions of the security issues.

Keywords: Client, Cloud Computing, Data Security, Encryption, Security, Server

1. Introduction

The cloud computing is an ongoing technology which is being improved every day. This has occupied almost several IT industries due to its cost efficiency and available for ease. "Cloud computing can be defined as a parallel and distributed computer system consisting of a collection of inter-connected resources based on Service-Level Agreements (SLA) established through negotiation between the service provider and consumers"[1]. The US National Institute of Standards and Technology (NIST) define cloud computing as "a user convenience modal, on demand network access gives the computing resources (e.g. networks, storage, applications, servers and services) that can be instantly implemented with minimal effort or service provider interference"[2]. Cloud is a way of distributed computing where largely IT enabled services are provided to customers using internet technologies. Cloud is served on demand and scaled as per the demand to the consumers. Cloud can also be known as online computing of storing and retrieving data, creating, deploying applications without their own hardware or software. Cloud computing provides many services over internet by using virtualization of data centers or data servers where responsibility is of provider[3].

This cloud computing provides computing as a service to the customers, the services are provided in many extended way to satisfy the customer. The cloud is flexible, scalable with large pool of resources. Due to its enlarged resources it is sometimes misused and hijacked by the attackers. This causes various security problems in the field of cloud computing. To tackle those problems many researches are happening to get out of the security issues. In this paper we are going to discuss about the cloud computing models, various services provided in cloud computing and numerous security issues which are discussed by researchers.

2. Cloud Computing Models

Cloud gives the user its resources through different models. These cloud computing services are provided

* *Author for correspondence*

by the service providers and hosted by cloud vendors to users. Service models in cloud

2.1 SAAS: Software as a Service

Software can be used from cloud as a service without installing them in their hardware in the providers' infrastructure. This could be done even in the mobile devices, web servers or any devices. Examples Google's Gmail, docs, BPOS (Business Productivity Online Standard suite).

2.2 PAAS: Platform as a Service

This gives the services like developing the applications in the provider's platform. The user can deploy application with the provider's tools, resources, servers and operating system.

2.3 IAAS: Infrastructure as a Service

This service is about the physical environment of cloud where it provides the storage space, networking and other needed resources. The user has the control on storage, network.

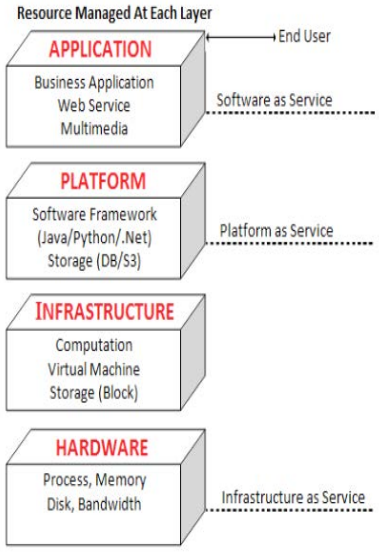

Figure 1. Layered architecture of cloud services[3].

- Application layer where applications are deployed by the users.
- Platform layer it runs the applications for the user.
- Infrastructure layer here virtualization of servers happens.
- Hardware where storage, processing and allocation is done.

3. Deployment Models in Cloud

3.1 Private Cloud

This is used by organizations to maintain and share resources within their organizations by having data centers internally or externally.

3.2 Public Cloud

This is shared by multiple customers through internet. The third party hosts the cloud for customers from different datacenters.

3.3 Community Cloud

Sharing of resources between organizations with in a community, like same company of different branches.

3.4 Hybrid Cloud

This is the combination of one or more from the above cloud models. For sensitive data uses private cloud and other data it uses public cloud.

4. Security Issues in Cloud Environment

There are many security issues faced by cloud computing. The customers uses the cloud for its on demand services, pool of resources at very cost efficient and can do computing from anywhere at any time. But the customers and the cloud providers are worried about the security issues they face. Cloud computing is a shared pool of resources where anyone can host the cloud on demand. Because of this interconnected networks a severe challenge to security of data.

Cloud computing has a drawback of numerous security issues and challenges. The network security is the biggest security problem and he refers to the Bradley layered security approach[4]. This layered approach has the basic security products like firewall, Antivirus and Intrusion detection system. Cloud security alliance top security threats of data breach, data loss and service traffic hijacking. Due to the VMs sharing same private keys by other VMs in the same server will give way to hijacking.

The attacker may get sensitive information of one client and via the others information are also at risk. This issue could be solved by encrypting all data on the database. Some of the major security issues are mentioned below:

4.1 Insecure Interface

The interface used in the cloud should be secured. A single threat in the interface may affect the user's data and data integrity. So the service provider should be aware of this and should have a secured interface in the cloud for users.

4.2 Data Theft

Due to the usage of external data server for cost effective and flexibility the data theft can happen when the data is transmitted from server to customer system by malicious attackers.

4.3 Data Loss or Leakage

The data are stored in the remote servers from the users and there may be chances of data loss from the servers. The data are transformed from the user's machine to remote servers where the data loss could occur.

4.4 Malicious Insider

The cloud service provider may be genuine to the user but the provider has employee who handles the users information may misuse them[5].

4.5 Shared Technology

Working in the cloud environment is a shared pool of resources where everything is freely available (virtualization, processing, caches etc.). Single misconfiguration will lead to compromise the entire cloud[5].

4.6 P Spoofing

The IP spoofing is network traffic the attacker make false request against the server and the server will trust the attacker as trusted user. Then the attacker determines the IP address of the user and changes the information which seems like it is from the trusted user's system.

4.7 Man in the Middle Attack

If the SSL secured socket layer is incorrectly configured then the client and server authentication will not work as expected.

4.8 DDOS

Distributed Denial of Service is still an ever ending threat in the cloud. The attacker's false request makes the server in active/denies the service when the trusted user make request.

4.9 VM-Based Malware Attacks

VM based root kits which attack both the client and server system by sending some malicious code instead of the original message from server/client. This code affects the both client and server system.

4.10 Flood Attacks

The customer uses the cloud services due to its extended size of service the initialization happens only by depending upon on the internal communication. And attacker makes false request to server. So the server gets busy and fails to work.

4.11 Loss of Control

If client is making some document under an application which is stored on cloud and if the client needs to change the cloud provider, then he can be threatened about misuse of his information already stored on the present cloud data center.

4.12 Access Control

Clients saved the data in the data center are unused for years. This can be hacked by some unauthorized access and data can also be used illegally lack of authorized rights of access control.

4.13 nsufficient Due Diligence

Organization moving to cloud must ensure that they have sufficient resources for performing exclusive due diligence before jumping into cloud and understand the risk it assumes.

These are the security issues that where faced by both the service providers and the clients. The service provider should ensure the client by keeping strong security policies. Then client should also be careful in handling the data in cloud by using proper authentication methods

and should often use the information stored long back. This will not lead to unnecessary attack from attacker or deletion of information.

The service provider should trust the client and also the client should trust the providers for storing the information in cloud. The providers also should have the access control to check the right access over the client's data. This should be integrated on the basis of Service Level Agreement (SLA)[6].

5. Why Data security a major issue in cloud computing?

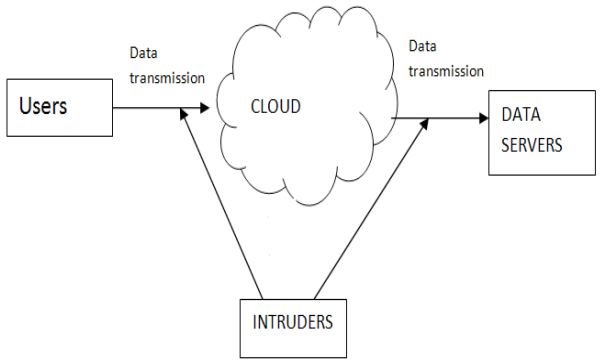

Figure 2. Data intruded by attackers while transmitting - A diagram.

The cloud offers services to clients for storing, retrieving data in the remote servers in order to reduce the cost of hardware and software. But the transmission of data from the user to the data server is the point where the intruders hijack the sensitive data of client. Figure 2 depicts data intruded by attackers while transmitting. So the client and the service providers always worry about the data security. The data protection and privacy protection are the major issues in cloud are the reason for many organization not adopting it. The data is stored in the database in data center which is far away from the user system along with thousands of other files on cloud. This may lead to high risk of Confidentiality, Integrity and Availability (CIA) of data in cloud[7].

The intruders, malicious attackers everyone who tries to intrude in the cloud computing are focusing only on the clients data. So here the data security is seemed to be an important than the other security issues. All the security issues in cloud at last ends in the data security only. So this has to be found and rectified to have trusted computing in cloud. Following are the cloud computing data security issues.

5.1 Data Privacy

Privacy is one of the issues in data security. As the information stored in the data center and are available across the countries. The private information of an individual is at risk but professionals are developing security services to solve data privacy issues. The data privacy could be maintained by using Anonymous Password Authentication (APA)[8].

Hence the data are stored in different data servers in data center the client is not aware where the data goes and the sensitive data of client is at risk and tend to be a privacy issue. The cloud service provider must ensure the privacy of user's data by having trusted security policies.

5.2 Data Availability

The data are stored in remote servers and the users' do not know the exact place of where their information is stored. The recovery of data during any accident such as hard disk crash, damage and natural calamities should be ensured by the cloud provider. The user's concern is cloud vendors are governed by local laws and user should be aware of those laws[9]. The client is unaware about the data and where it is processed so the client has no control over his/her data. So the provider must ensure the security of data through some SLA (Service Level Agreements)[10]. Data availability means framework should be capable to handle data operations even when the security break up happens. Data should be available based on the authorized users need and able to access at all time[11].

5.3 Data Confidentiality

Data are moved to remote data centers and the client have no physical access of the data. So data confidentiality is at risk and data should be kept confidential from cloud provider and other customers. A solution for this cryptography is the practice that can keep the data confidential[12]. The data encryption technique should be used before moving to data servers which ensures the data confidentiality.

5.4 Data Integrity

As data is stored in data server which is hosted by vendors to the customers, there may be lots of intrusions between

the data transmission. So there is a problem of data integrity by unauthorized access. The malicious insider or outsider could attack the information like Google docs got attacked in 2009, Amazon was also attacked recently. This could be avoided by providers' strong security measures. Many mechanisms are used to test the integrity of data, some of them are PDP (Provable Data Possession) and POR (Proof of Retrirvability) are used to test the integrity of data from the cloud.

5.5 Data Boundary

The cloud provider multiples the data copies in many data center for the availability of data for clients. Nothing goes wrong if the data is visited often by the clients, by chance if it is not used for long then it may lead to deletion, leak of information if not kept safe.

5.6 Data Loss or Leakage

Data are taken from data centers to the clients system which is transmitted from one execution mode to multiple execution mode this may cause data lose or leakage. Even data is stored far away from clients system so there may be chances of data loss or leakage.

5.7 Data Segregation

Though the encryption technique are effective, it should be ensured that encryption are tested and programmed well because using encryption and segregating the data should be done safely otherwise data loss or theft may occur.

5.8 Data Breaching

Domain of cloud will get to know about the data of all the users and lead to enormous effect on the data security.

6. Strategies and Encryption Techniques for Data Security

From the above data, security is the major issue in the cloud environment and researchers. Professional has found some strategies and encryption techniques to solve the issues. Some of them are as follows:

To secure the data from the malicious attack, the data should be encrypted by using the proper cryptography methods. Here three types of techniques explained by[13].

- Symmetric key cryptography method which is traditional method of encryption DES, AES and RC5 algorithms are used here for encryption. One key is used by both the sender and the receiver in this method[13]. The secret key can be a text or string where each letter is shifted by number of places in the alphabet.
- Asymmetric cryptography method where two private and public keys are used to prevent them from falling into wrong hands. Here RSA, Elliptic curve are used to do encryption. This is slower than the symmetric encryption it takes more processing power to encrypt and decrypt the content. Here secret key is kept confidential to hide them from the hacker so it's safe and data confidentiality, integrity could be maintained.
- The third one is Hash Function cryptography which is one way cryptography method. Output of the hash function is named as Message Digest (MD)[13]. This is safer than the other two because single alteration like adding comma also make huge difference. In this SHA1 and MD5 are used. This is often used to solve the data integrity problem.

The main thing in the security is trust between the client and the cloud service provider. This could be achieved by SLA (Service Level Agreements). The data is travelled from client end to the server end where the data could be easily hacked by third party14. Encryption technique is focusing on steganography14.

- Image Steganography: Steganography means hiding information in some other information where secret message cannot be detected easily. The image is used as information in which secret data is embedded. Then the secret data is embedded into the image by detecting the edges of the image using pixel key pattern.
- Pixel Key Pattern: This is used as a tool in image processing and computer visualization. This used multistage algorithm to detect edges of the image.

[15]Describes the techniques for the security in cloud. Some of them are:

- The raid technique which maintains the data integrity. This encrypts and encodes the original data and later distributes the fragments across multiple providers.

- Then encryption technique is used to maintain the data confidentiality. One of the encryption techniques is homomorphic encryption. Using this technique there is no need to decrypt the whole data since it is consistent.
- Hybrid technique uses the RSA, 3DES and random number generator. RSA connect through digital signature, 3DES useful for encryption of block data. This technique is good for data confidentiality and integrity.
- Cipher Retrieval Technology: The data protection is attained by encrypting the data and then putting the cipher text in to server. The retrieval of encrypted data should be done by solving the cipher text. The cipher text could be solved by using the methods like linear searching method, public key based on keyboard searching method, security index searching method and order preserving encrypted searching method.
- User Authentication: Two authentication methods. They are ID/Password and PKI (Public Key Infrastructure) authentication technology. Strong ID/Password are recommended for effective user authentication. PKI authenticates using public key cryptography. Other party is authenticated based on the certificate without sharing secret information.
- Data Concealment: Data Concealment mixes the visual fake data and real data to fix the real data's volume. It is like to hide the real data inside the fake data to keep the data confidential. This is suitable for private cloud data's are not accessible to all users. Water marking methods are used as a key for real data so that the authorized users can use it.

We discussed many encryption techniques and strategies for various data security in this paper. Though there are many security solutions even more improvement are needed to ensure full secure cloud environment.

7. Conclusion and Future Work

Cloud computing is a technology which is available in all services and on demand where the computing could be done at very low cost. Though it has a bright future its obstacles are security issues. Providers are in need to ensure the data security for clients since they are depending on service providers so that they could use the cloud in an effective way. The data security plays a vital role in client side and also in cloud provider side. The major security issue that we have discussed in this paper was data security. Most of the people use cloud to save their data due to its flexibility. So data security should be taken as a very serious issue and encryption techniques and methods are required to bring solution to this issue. In this paper selected methods and encryption techniques are explained and further improvement needed in those techniques, so various security issues and the major data security are discussed. The future work will be to enhance the security encryption techniques and strategies to get a fully secured data in cloud.

8. References

1. Kaur R, Kaur J. Cloud computing security issues and its solution: A review. 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom); 2015. p. 1198–200.
2. Kumar SRG. Security facet in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(4):964–7.
3. Grover J, Shikha S, Sharma M. Cloud computing and its security issues - A review. 2014 International Conference on Computing, Communication and Networking Technologies, ICCCNT'14; 2014. p. 1–5.
4. Moyo T, Bhogal J. Investigating security issues in cloud computing. 2014 8th International Conference on Complex, Intelligent and Software Intensive Systems; 2014. p. 141–6
5. Kaur JP, Singh S, Karn A. Analysis of security issues and management standards in cloud computing. 2nd International Conference on Computing for Sustainable Global Development (INDIACom); 2015. p. 1474–8.
6. Kaur M, Singh H. A review of cloud computing security issues. International Journal of Advances in Engineering and Technology. 2015; 8(3):397–403.
7. Narula S, Jain A, Prachi MS. Cloud computing security: Amazon web service. 2015 5th International Conference on Advanced Computing and Communication Technologies; 2015. p. 501–5.
8. Badawi EAALA, Kayed A. Survey on enhancing the data security of the cloud computing environment by using data segregation technique. IJRRAS. 2015 May; 23(2):136–43.
9. Vasanth C, Bhagawat B, Arul D, Kumar LS. Survey on data security issues in cloud environment. IJIRAE. 2015; 2(1):31–5.
10. Cyril BR, Kumar SBR. Cloud computing data security issues, challenges, architecture and methods - A survey. IRJET. 2015; 2(4):848–57.
11. Puthal D, Sahoo BPS, Mishra S, Swain S. Cloud computing features, issues and challenges: A big picture. International Conference on Computational Intelligence and Networks; 2015. p. 116–23.

12. Balasubramanian V, Mala T. A review on various data security issues in cloud computing environment and its solutions, ARPN Journal of Engineering and Applied Sciences. 2015; 10(2):883–9.
13. Suveetha K, Manju T. Ensuring confidentiality of cloud data using homomorphic encryption. Indian Journal of Science and Technology. 2016 Feb; 9(8):1–7.
14. Kaur R, Kaur J. Cloud computing security issues and its solution: A review. 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom); 2015. p. 1198–200.
15. Snehal A, Narale N. Employing security techniques in the current world of cloud computing environment: A study. International Journal of Computer Science and Mobile Computing. 2015; 4(4):796–801.