International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

A Survey on the Various Security Methods Imposed on Cloud

Deeksha K R[1], Sudheer Shetty[2]

[1]M.Tech, Computer Science and Engg., Sahyadri College of Engineering and Management, Mangaluru, India
[2]Dept. Computer Science and Engg., Sahyadri College of Engineering and Management, Mangaluru, India

Abstract: ***Cloud computing makes use of computing resources that is hardware or software that are shared as services over the internet.In recent years, cloud computing has grown up rapidly because of the useful services provided by cloud. Data outsourcing in cloud is becoming more useful because of the storage services provided by the cloud computing. Thesize of the storage is increasing day by day. The outsourced datawill get stored in different data centres present in all over the world. Protection of the outsourced sensitive data in cloud is major security challenge in cloud. Storing a large amount of confidential information on the cloud will help for the sniffers to miss use the data. Thus the security to be considered as one of the top issues while considering Cloud Computing. This survey paper aims to analyse various data storage security methods.***

Keywords: Availability, Cloud Computing, confidentiality, Data outsourcing, Data Security, Sensitive data

1. Introduction

Cloud computing is a distributed computing where the services can be accessed throughout theworld. Due to the services provided by CSP (Cloud Service Provider) most of the people are moving towards cloud computing. It provides features like auto scaling, pay as you go, elasticityetc. It provides services like Saas Paas, Iaas. One of the main advantages of cloud computing is that it gives applications and storage spaces as services over the Internet for low cost. The users can access their data at any time and from anywhere. It does not require high end machine to access the application since it is hosted on cloud. It provides the concept of virtual machine where the user can use the multiple operating systems in single system. Whenever using virtual machine whatever the storage spaces we are using is the space of the cloud service provider.

2. Data Security Issues In Cloud Computing

Data Security is one of the major issues in cloud computing. Because of the storage facility offered by cloud, most of theorganisations started to store their important files oncloud whichdoes not guarantee about the security. What ever the data storing in the cloud will be in complete control of the CSP which is in remote place. There may be hackers inside the CSP or in the channel where the data get transferred.Security goals include Availability, Integrityand Confidentiality of data. Following are the security issues in cloud service providers, which have been listed and are related to file storage.

2.1Security of data in transit

Cloud Computing is completely based on networking where the data can be sent and received from the server. During these transmission data can be tracked in the channel. Files can be hacked at any time. So files should be secured in the channel where the data get transmitted.

2.2 Security of data at rest

Cloud stores the huge amount of data of different users it may be company, hospital or any other confidential data. It may be more important for the users. In all known cloud services, data are encrypted and stored in the cloud servers. Encrypted file is called cipher data which will not be in original format. When the user wants to retrieve the original file, encrypted file need to be decrypted by using the key. When the data is encrypted at cloudserver, there are chances where cloud provider will have either key after encryption where they can decrypt and retrieve the original data or before encrypting they will be having original data. If internal hackers are present they may miss use it.

2.3 Authenticated User

There are huge amount of files of different users in cloud. Whenever thefile gets stored in cloud, theuser has to be differentiated by their files. Users are authenticated so that they will not get access to the other users files.

3. Related Works

In past there have been lot of work has been done on cloud data security different techniques were used to provide security to cloud data but there are some disadvantages of such systems. Existing methods include data encryption before storing data and user authentication for storing or retrieval of data after that building secure channels for data transmission over the cloud.

Jing-Jang Hwang et al. [5], has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. The methodexplains that all the responsibility is given to Cloud service provider from storing to retrieval of data. The maindisadvantage of this method is, Data owner has complete trust on CSP where there may be an internal hacker in CSP.

Junzuo et al. [6], proposed an Attribute Based Encryption (ABE) and verifiable data decryption method. Retrieving of data is based on the user requested attribute on the encrypted data.it takes more time to search as well as morestorage space.

Spoorthy V et al.[2], discussed the Implicit storage security mechanisms use the scheme of data partitioning to store data in online. The data is simply partitioned and stored directly. The data can be divided and stored on different servers on the network. Only user will know the location of the data. To

retrieve data back user has to know the where the data is residing. This method does not guarantee about the availability of the data. These authors also discussed a Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) is a mechanism used to dynamically store data in cloud. It uses a protocol using the data reading protocol algorithm to check the data integrity. This mechanism uses homomorphism tokens, blocking erasure, and unblocking factors. It also used to check the data security provided by the service providers. This method does not guarantee about the confidentiality of the data.

Fatemi Moghaddam et al. in [7], discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment. Two separate cloud servers are required. One for data and other for key and Encryption and decryption takes place at client side,Mainitaining two separate servers for data security in cloud, which creates a more storage.

Hemalatha N, Jenis A, Cecil Donald A, Arockiam L[3],discussed Blowfish is a fast, compact and simple block size of 64 bits encryption algorithm with variable key length from 32 to 448 bits. This algorithm is suitable when the key constant. Blowfish encryption has some classes of weak keys.

Jyotirmoy Das [4], discussed RSA (stands for Rivest, Shamir Adleman) is public-key cryptography and is widely used for secure data transmission. In RSA, one of the key can be shared with everyone and another key must be kept private. Anyone can use the public key to encrypt a message; the decryption of message does not take excessive time to get the original text. Slow compared to other encryption methods.

Cong Wang and Kui Ren [8] proposed Toward Publicly Auditable Secure Cloud Data Storage Services which is the concept of TPA.Due to large amount of data stored in cloud It is difficult and expensive for those data owners to check for the data correctness.A trusted auditing organization works in the between to provide secure storage to the cloud users. But suppose data owner or TPA itself is a hacker. In this case the auditing result should identify the data correctness and has to identify which entity (Owner, TPA or cloud server) is responsible for the problem. So the problem is how to work when all entities are malicious.

Attendees et al [1], proposed public audit ability in provable data control replica for ensuring possession of records on untrusted storage in which RSA based homomorphism tag are used. With the help of this technique public audit ability concept is achieved. It suffers from security problems.

Al-Riyami and Patterson [9] proposes the method Certificateless Public Key Cryptography (CL-PKC).CL-PKC is based on bilinear pairings.In comparison with other standard encryption schemes CL-PKC requires high computational cost.

4. Conclusion and Future Work

Cloud computing is involving day by day in todays world. Thenumber of users isincreasing. Sothere is a need to provide security to the data which is stored on the cloud. Many approaches have been suggested over the decade for achieving security in the cloud. The survey consists of various existing data storage security techniques and its problem. We can go for double encryption method to give more security at client and server side that is end to end security as a futurework. The method which also achieve data confidentiality, integrity and availability of data.

References

[1] Q. Wang, C.Wang, K. Ren,W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,”IEEE Trans. Parallel Distributed Syst., vol. 22, no. 5,pp. 847-859, May 2011.
[2] Sporty V, Mamatha M, Santhosh Kumar B, “ A Survey on Data Storage and Security in Cloud Computing”, International Journal ofComputer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 6, pg. 306 – 313, June 2014.
[3] Hemalatha N, Jenis A, Cecil Donald A, Arockiam L, “ A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing”, International Journal of Computer Apllicaions,Vol. 96, No.16, June 2014.
[4] Jyotirmoy Das, “A Study on Modern Cryptography and their Security Issues”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 10, October 2014.
[5] Jing-Jang Hwang, Taoyuan, Taiwan, Yi-Chang Hsu, Chien-Hsing Wu, A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, in International Conference on Information Science and Applications (ICISA), pages 1-7,2011.
[6] Junzuo Lai, Deng R H, Chaowen Guan, Jian Weng, Attribute-Based Encryption With Verifiable Outsourced Decryption, in IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354, 2013.
[7] Fatemi Moghaddam F, Karimi O, Alrashdan M T, A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments, in IEEE 2nd International Conference on Cloud Networking, pages 185-189, 2013.
[8] Cong Wang and Kui Ren, Jin Li,” Toward Publicly Auditable Secure Cloud Data Storage Services Illinois Institute of Technology”, IEEENetwork July/August 2010
[9] Al-Riyami, Sattam S and Kenneth G. Paterson. "Certificateless public key cryptography." Advances in cryptology-ASIACRYPT 2003. Springer Berlin Heidelberg, 2003. 452-473