

Data Security Techniques on Cloud

Shilpa. Chippalakatti¹, C.H. Renu Madhavi²

¹ECE Department, Sambhram Institute of Technology, Bangalore, India

²EIE Department, RV College of Engineering, Bangalore, India

Abstract:

The healthcare industry is producing huge amount of clinical data, storing of this data with a reduced cost is huge challenging job. Cloud based computing is the popular health care IT infrastructures where we are storing the clinical and administrative designated information system in someone else's premises and pay the rent and power to access it from any place. But the problem with this type of storage is whether the data will be safe. So before the data outsourcing the data supplier has to make sure that the data is secure and will be able to make transactions in such a way that it should not be visible to the intruders or if it is visible also it should not be in the understandable format. In this paper, we are trying to discuss the various methods used for securing the data on the clouds and we are also trying to discuss different techniques or algorithm used to do so.

Keywords: Cloud computing, Cryptography, Data Security, Techniques

1.Introduction

Cloud environment uses hardware resources and software entities for providing services in the internet. With cloud computing, one can use application as well as access required files from any location in the world, having access to internet. A well know and good illustration is Gmail for providing cloud services. The data in the cloud is stored in the virtual server like a data in pc is stored in the hard disc. An example of the cloud file storage provider is the Dropbox.

It offers wide services to the users, Infrastructure as a Service-IaaS , Platform as a Service-PaaS, Software as a Service-SaaS. There is a huge quantum of data exchange inbetween the end user and cloud provider's data centers in any type of cloud application services used over the internet. So protecting this data from the malicious or third party users is the major concern about all service providers. According to International Data corporation(IDC) in 2011, security was ranked as a major challenge by whopping 74.6% of enterprise customers.

This paper address the above issue by providing a survey on different techniques or algorithm used to secure data on the cloud.

2. Literature Review

The authors et.al [1] intend to protect the data from third party access that stored in the cloud by providing a simple and secure data encryption and decryption algorithms like AES algorithm for data encryption and RSA algorithm for the key encryption and store the key in some other location.

Seema, prakash and Ishita [2] stated that cloud is a next generation technology which is based on the internet and which provides quality services to the users with less cost. The customers who are placing the data on the cloud should be sure that it is safe and and transaction are all secure. So they proposed two methods data security with effect from Kerberos and SLAs with cloud proof.

The authors have proposed protection of privacy and security of data are the prime issues of cloud network. Different techniques in maintaining confidentiality of data, maintaining integrity of data, providing privacy of data with ease of accessibility of data has been discussed. Maintaining Integrity of data in the cloud can be done using RAID- strategies, Digital Signature. Data confidentiality by Distributive storage, Homomorphic encryption, Hybrid Techniques, Encrypted search and database ,data concealing, deletion confirmation. Availability of data is achieved by a Storage Reliable agreement and a Reliable Hard-Drive. Privacy of Data is prone to the following attack like Abuse of Service, Attacks Aversion, Identity Management [3].

In this paper the author's major stress is on the multi-tenancy security issues. He also discussed different type of attack which happens on the data which is saved in cloud [4].

This paper briefs various data protection methods with loopholes in it. It also focuses on the security at each level like SaaS, Paas and Iaas as well as data-in-rest and data-in-transmit. This paper also highlights different encryption algorithm such as Hash function, Stream cipher, Block cipher [5].

Jitesh, Piyush [6] gave an insight of storing the mobile data on the cloud and how to protect that data from the malicious user. The various methods of data encryption techniques for mobile data are Multi-clouds Databases, Multicast Key Management , Homomorphic Encryption , Data Partitioning Technique ,Cipher Cloud, Data Trust Third Party and Elliptical Curve Cryptography.

3. Cloud Architecture

Cloud architecture is different technologies are combined together to form a cloud. In IT environment it abstract, pool and share scalable resources across the network. It can also be defined as all the components and capabilities are connected together to provide online platform to run application.

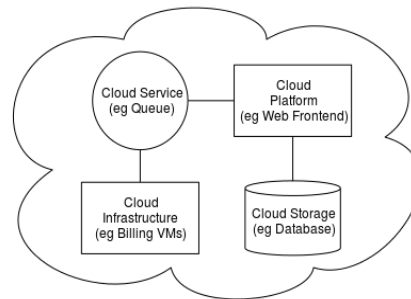


Fig 1. General Cloud Architecture

High bandwidth, uninterrupted access to application, on-demand agile network, fast movement of data and network security are the major concerns for cloud.

3.1 Cloud Services

The services provided by the cloud are

3.1.1 Infrastructure as a Service (IaaS)

IaaS is a cloud based model where the service providers lease or rent the infrastructure on the cloud. The user can run any application on this platform without maintenance and operating cost. The service providers are responsible for the maintenance of the cloud like security, firewalls and storage. The companies which are offering IaaS are Amazon EC2, Google cloud platform, Microsoft azure etc.

3.1.2. Platform as a Service (PaaS)

PaaS works on IaaS. The cloud vendors provides the infrastructure components like middleware and operating systems which is required to develop and test application. The PaaS provides a cloud users to store the data, development tool and business analytics application on the cloud. The companies which are offering PaaS are AWS, OpenShift, Oracle cloud, SAP and Microsoft Azure.

3.1.3. Software as a Service (SaaS)

SaaS is special which incorporates both IaaS and PaaS. The cloud providers delivers the complete software. Most common SaaS are Microsoft office 360, Google G Suite, Oracle CRM, SAP and Business by Design.

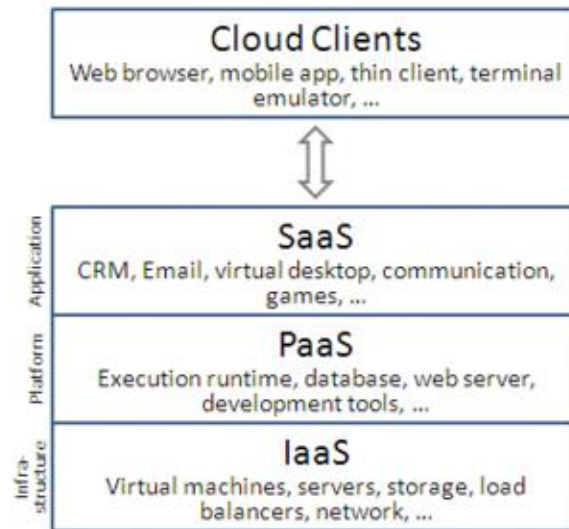


Fig 2. Cloud Computing Service Model

3.2. Deployment Models

The Three Deployment Models are described below

3.2.1. Public Model: This infrastructure is available to the general public. Public cloud is structure in which the resources are available to all the users.

3.2.2. Private Model: This type of infrastructure is available only to one company who wants to keep there data hidden. The data/resources in the private cloud will not be available for all the cloud users.

3.2.3. Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This type of infrastructure is used by the companies when some of the resources should be hidden and some resources are available to all the users of the cloud.

4. Data Security Techniques

The various techniques used to protect the data from malicious attack, whether the data is in transmission stage, rest state or in the processing stage are

4.1 Authentication /Identity

Cryptography is used for communication systems and for Authenticating the users. The various methods like one time password, security token, finger print are used for user Authentication.

4.2. Data Encryption

If we are storing the confidential information on the cloud, data encryption techniques is used. As it is more secure than age old firewall and password which the hackers can bypass for accessing data. After encryption data will be converted into the cipher text and without the encryption key it cannot be converted into the plain text. As the data now becomes dormant to the hacker. This process called data encryption technique where without the secret key the data for the hacker becomes derogatory. The encryption techniques used are DES algorithm, AES algorithm, Hash function, RSA algorithm etc, if still more security is needed for the data then we can encrypt the secret key also using a RSA algorithm and keep the key in other server and not in cloud.

4.3. Information Availability (SLA)

The major problem in the cloud based computing is to know whether the data or resources are available or not. Service Level agreement(SLA) is a trust bond which is created between the consumer and the service providers which will provide the information whether the data/resources is available or not. The alternate way to have access is to have a backup plan for critical information and local resources. It provides information to the user regarding the resources inspite of their unavailability.

4.4. Solution for Malware-injection attack

The solution for the above attack is by creating the number of the client virtual machines and to store them in central station. This is done using FAT-File Allocation Table which tells us which application is running and it has a virtual operating system. The scheduling and managing is done via Hypervisor. Integrity checking is done based on the IDT -Interrupt Descriptor Table.

4.5. HADOOP

The processing of large set of data in a distributed computing environment is done using the free and Java based programming called Hadoop. Master/Slave structure is used here. Using this we can process large set of data. As it uses the distributed file system, data can be transferred rapidly which allows the normal operation of the system even if there is failure of some nodes. Hadoop provides many advantages like scalability, economical, flexible, fault tolerance etc and it is used by many international sectors to handle their big data.

5. Conclusion

The paper reviewed cloud architecture and various data security techniques used in cloud environment. The cloud architecture reveals deployment, models of cloud and data security techniques discusses the various techniques used to secure the data on cloud. Based on the security requirement, various encryption algorithms can be used in alone or

in combination to improve the security of user data at cloud storage. Above paper provides the overview of cloud and how to protect the data when it is at rest, transmitting, processing or if it is big data.

References

- [1] Fakhruddin Noori, Abdul Ghafar “Omerkhel”: A Review on Data Security in Cloud Computing In: International Journal of Engineering Research & Technology (IJERT) <http://www.ijert.org> ISSN: 2278-0181 IJERTV10IS030208 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : www.ijert.org Vol. 10 Issue 03, March-2021
- [2] Bayan A. Alenizi¹ , Mamoona Humayun² , NZ Jhanjhi³: Security and Privacy Issues in Cloud Computing in: International Conference on Recent Trends in Computing (ICRTCE-2021) Journal of Physics: Conference Series 1979 (2021) 012038 IOP Publishing doi:10.1088/1742-6596/1979/1/012038
- [3] Mishra, S., S.K. Sharma, and M.A. Alowaidi, Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing, 2020: p. 1-12. 2.
- [4] Mishra, Sambit Kumar, Sonali Mishra, Ahmed Alsayat, N. Z. Jhanjhi, Mamoona Humayun, Kshira Sagar Sahoo, and Ashish Kr Luhach. "Energy-Aware Task Allocation for Multi-Cloud Networks." IEEE Access (2020).
- [5] Chatterjee, Moitrayee, Prerit Datta, Faranak Abri, Akbar Siami Namin, and Keith S. Jones. "Abuse of the Cloud as an Attack Platform." In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1091-1092. IEEE, 2020.
- [6] Arjun, U. and S. Vinay. A short review on data security and privacy issues in cloud computing. in 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC). 2016. IEEE.
- [7] Sun, X. Critical security issues in cloud computing: a survey. in 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), 2018. IEEE.
- [8] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831- 1838.
- [9] Shuai, H., & Jianchuan, X. (2011, 15-17 Sept. 2011). Ensuring data storage security through a novel third party auditor scheme in cloud computing. Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference
- [10] Parsi Kalpana & Sudha Singaraju (2012).Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology(IJRCCT), vol 1, Issue 4.
- [11] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced data security model for cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on.
- [12] Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013). Privacy preserving cloud data access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE.
- [13] D.Sakthipriya¹ R.priya² , S.kalaivani³: Security issues in Cloud Computing In: Journal of Analysis and Computation (JAC) (An International Peer Reviewed Journal), www.ijaonline.com, ISSN 0973-2861 International Conference on Emerging Trends in IOT & Machine Learning, 2018
- [14] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143- 152, 2010. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0. R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11.
- [15] Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computer world. Retrieved May 02, 2014

- [16] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. Retrieved May 02, 2014
- [17] Kartit Z. et al.: Applying Encryption Algorithm for Data Security in Cloud Storage. In: Sabir E., Medromi H., Sadik M. (eds) Advances in Ubiquitous Networking. UNet 2015. Lecture Notes in Electrical Engineering, vol 366. Springer, Singapore (2016)
- [18] Ms. Seema Kumari¹, Mr. Prakash Pathak², Ms. Ishita Madan³: Techniques for Securing the Data in Cloud Computing In: International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 05 | May -2017
- [19] YunchuanSun,¹ JunshengZhang,² YongpingXiong,³ andGuangyuZhu⁴: Data Security and Privacy in Cloud Computing In: International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages <http://dx.doi.org/10.1155/2014/190903>
- [20] Varsha, Amit Wadhwa, Swati Gupta: Study of Security Issues in Cloud Computing. In: International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, pp. 230-234, June- 2015.
- [21] Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills: Data Security in Cloud Computing. In: Fifth International Conference On Future Generation Communication Technology, FGCT 2016
- [22] Jitesh S. Zade, Piyush Ingole: Data Security Techniques in Cloud Environment: A Review. In: 3rd National Conference of Innovative Research Trends in Computer Science Engineering & Technology 2014.
- [23] Gururaj Ramachandra^{†,‡}, Mohsin Iftikhar^{†,*}, Farrukh Aslam Khan: A Comprehensive Survey on Security in Cloud Computing. In: The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017)
- [24] Rongzhi Wang: Research on data security technology based on cloud storage. In: 13th Global Congress on Manufacturing and Management, GCMM 2016
- [25] M.Ramya M.Sc.,M.Phil.,¹, P.Sonali², N.Naga Dharshini³: SECURITY WITH BIG DATA IN CLOUD COMPUTING. In: Journal of Analysis and Computation (JAC) (An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861 International Conference on Emerging Trends in IOT & Machine Learning, 2018
- [26] Garima Gupta¹, P.R.Laxmi² and Shubhanjali Sharma³: A Survey on Cloud Security Issues and Techniques. An, Y.Z., Zaaba, Z.F., Samsudin, N.F.: Reviews on security issues and challenges in cloud computing. In: IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing (2016)
- [27] An, Y.Z., Zaaba, Z.F., Samsudin, N.F.: Reviews on security issues and challenges in cloud computing. In: IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing (2016).
- [28] Leena Khanna, AnantJaiswal, —Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Theml, IJARCSSE 2013.