Volume: 6 Issue: I Month of publication: January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1289

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Issues Related to Data Security and Privacy in Cloud Computing

Ashish A. Patokar[1], Dr. V. M. Patil[2]
[1]Assistant Professor Dept. of Computer Science & IT, Shri Shivaji College, Akola
[2]Head & Associate Professor Dept. of Computer Science & IT, Shri Shivaji College, Akola

Abstract: Nowadays cloud computing is rapidly expanding technology in the instant word. Data security and privacy issues are most important in the growing technology in cloud computing in business, industry and academics. Various types of the cloud service providers are available in the market such as Microsoft, Google, Amazon, Go Grid, Enomaly etc. Customers use this application in establishing application in cloud surrounding and access them from anywhere. Huge data are store on the cloud and the authorized users can access this data with support of various service providers. Data security and privacy issues are applicable both hardware and software building in cloud. The data store in the cloud storage must be protected by using various cryptographic algorithms such as AES, DES, 3DES and RSA.

This paper focus on the data security and privacy issues such as data integrity, data privacy, data availability, data location access control in the cloud computing and the solution to the data security.

Keywords: Security issues, Cloud computing, AES, 3DES.

I. INTRODUCTION

Cloud computing is a emerging internet occupying computing system and implement easy and personalized utility to the customer for accessing the data on different cloud applications. The authorized users store their data on the data severs and also access this data from the server when require to the users. Cloud server providers (CSPs) maintain the data/information security and establish a mindset to corruption of the sensitive precise data without the former knowledge of the customer. There are various security algorithms are used for encryption and decryption of the data. With the help of these algorithms, users encrypt the data formerly storing in the cloud storage server [1]. The encryption process makes the data unreadable for the illegal/unapproved users and gives the strong data security. Cloud computing is associated with the different types of cloud services such as information as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2].

II. LITERATURE REVIEW

R. Velumadhava Rao et.al discussed the data security issues such as locality, integrity, access, confidentiality, breaches, segregation and data center operation and give the security solution for data by using encryption algorithm [1]. MeghnaUnnikrishnan et.al discussed security mechanism and comparative study of various algorithms and found an efficient algorithm to make the data secure using the homomorphic encryption and MD file algorithm for protecting the data [2]. Deepika Verma et.al proposed security algorithms for better security performance and by using this security algorithm the data files such as audio, text, video and images are properly stored on cloud [3] .V. Venkatesa Kumar et.al give the data security issue solution and security attacks occur in the cloud and ensure cloud more secured [4]. Vijendra Rajendra Augustine et.al discussed the cryptographic mechanism such as RSA, AES and DES for data security in cloud [5]. Uma Naik et.al introduces security issues and security purpose RSA algorithm and dual security algorithm for cloud computing [6].R. Pushplatha et.al discussed security issues, cloud services and various symmetric sand asymmetric algorithms to give better security for cloud [7]. Poonam M. Pardeshi et.al. Proposed secured and efficient AES base system and the system supports public auditing for use of TPA and privacy preserving and does not leakage of data to TPA during verification process [8]. K. R. Monisha discussed AES and RSA security techniques for data security and privacy issues in cloud storage for protecting the data in cloud system [9]. Mervat Bamiah et.al discussed the cloud security challenges and the clouds adopt services in industries [10]. S. Arul Oli et.al discussed about the security techniques for minimizing time, data size and services while data uploading into the cloud storage [11].Cong Wang et.al discussed about the secured cloud storage system by supporting privacy preserving public auditing [12].

III. DATA SECURITY AND PRIVACY ISSUES IN THE CLOUD COMPUTING

There are various data security and privacy issues for cloud computing are as follows-

A. Data privacy

There is no guarantee to keep the secret data to be preserved unauthorized users can access the data in the cloud, for these privacy policies and procedures are provided for the safety of data on cloud [1, 2, 4, 5].

B. Data integrity

At the equal time, several users and cloud suppliers access and repair the data so integrity preserved perfectly to avoid data loss [1, 2, 4, 5].

C. Data availability

Users can store daa on particular servers located in various clouds. Data availability develops into a dominant appropriate issues as the possibility of unmatchable arrangement becomes tough [1, 2, 5].

D. Data confidentiality

Clod users store their data or information on private server and content like audio, video, data files etc. stored among multi cloud suppliers. Although the data is stored in the private servers, confidentiality of that data is necessary provision [1, 2, 5].

E. Data location

In cloud data is located over the different regions and search the location of data is challenging. During the data are dragged to distinct geographic locations and the laws guided. Users appreciate their data location is declared by the cloud service provider [1, 5, 6].

F. Segregation

The important feature of cloud computing is multi enterprise and grant the permission to store data on cloud servers by multi users. By accepting any function, data can be trusted. Extremely it is required to store data independently from the surviving users' data. And these data segregation can recognize using the data validation and insecure storage stage [1].

G. Access control

Access control points out the data security rules. Access control mechanism perform by using various security algorithms such as encryption techniques and key management are used for the data stored and shared on the cloud and only authorized users can access this data. The security is given to the data to avoid data hack from unauthorized users. Encryption techniques are used by the users to avoid security attacks [1,2].

H. Data Loss

When the users store and share data on cloud the chances of the data loss occurs. To avoid data loss gives the permission to the authorized users and protect the data from the unauthorized users and use the encryption techniques for the data loss [4].

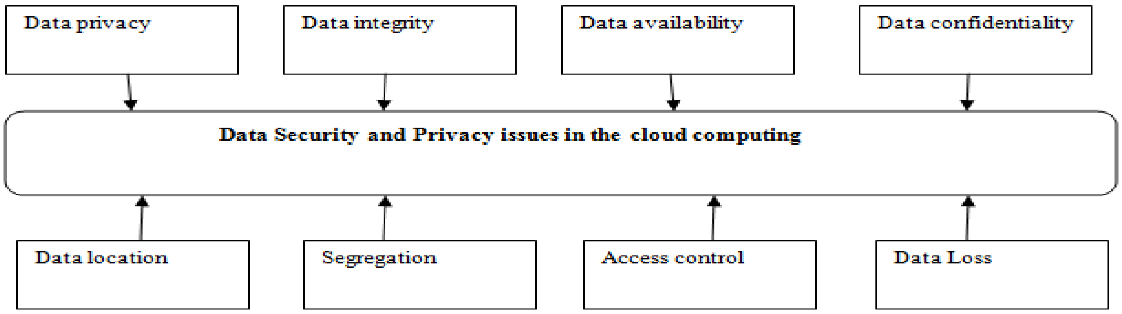

Figure: -Data Security and Privacy issues

IV. PROBLEM STATEMENT

Data Security in the most important issues in cloud data storage. Users can store their data or information in the cloud but sometimes the data may be loss or corrupted due the third party intruder. While storing and retrieving the data from the cloud security is the important issues to avoid the unauthorized users does not access these data. To overcome such types of problems occur in cloud storage introduce encryption algorithms such as AES and 3DES for better security and performance.

V. DATA SECURITY SOLUTIONS

Data security is given by using various cryptographic algorithms. Data store and shared on the cloud servers users first encrypt the data and only the authorized users can access this data. For better security to data, data integrity, access control, Segregation, data encryption, data availability security issues are used to improve the security of data over cloud servers. To avoid data from unauthorized users, use the encryption techniques that makes the data unreadable and only the authorized users can read by using the management system. Firstly to identify the data is properly stored on backup and contents do not change during the uploading process. Software as a Service model is used to segrate data from various users. AES and 3DES algorithms are used for encryption of the data. 3DES symmetric key algorithms also are used for strong security for the data and only the authorized users can access this data by using key management system.

VI. CONCLUSION

In this paper different data security issues such as data availability, privacy, integrity, access control, data loss, segregation and security solutions are provided using the encryption techniques for better security for the secured data access from the cloud. For secure data access in cloud, encryption algorithms such as AES and 3DES used for storing and sharing data from cloud. Also provides the key for the authorized users for retrieving the data from the cloud and unauthorized users can not access these data.

REFERENCES

[1] R. Velumadhava, K. Selvamani, “Data Security Challenges and Its Solution in cloud Computing”, International Conference on Intelligent Computing, Communication and Convergence (ICCC-2015), pp 204-209.

[2] MeghnaUnnikrishnan, LipiArun, “Comparative study of cloud computing data security methods”, International journal of computer application (0975-8887),2014, pp 13-18.

[3] DeepikaVerma,KaranMahajan, “ To Enhance Data Security In Cloud Computing Using Combination of Encryption Algorithm”, International journal of advance in science and technology (IJAST) , Vol.2,issue 4, December 2014, ISSN 2348-5426 pp 41-44.

[4] V. Venkatesa Kumar, M. Nithya, “Improving Security Issues And Security Attacks In Cloud Computing”, International journal of advance research in computer and communication engineering, ISSN (online):2278-1021, Vol 3, issue 10, October 2014, pp 8148-8151.

[5] VijendraRajendra Augustine, Prabhakar L. Ramteke, “Data storage Security In Cloud Environment With Encryption And Cryptographic Techniques”, International journal of application or Innovation in Engineering and management (IJAIEM), ISSN 2319-4847,vol 3, issue 3, March 2014, pp 209-213.applicable in Multi-Cloud Environmebt”, International journal of Advanced Research in computer and communication engineering, vol. 5, issue 3, March 2016, pp 460-463.

[6] Uma Naik, V. C. Kotak, ”Security Issues With Implementation of RSA and Proposed Dual Security Algorithm For Cloud Computing”, IOSR Journal of electinics and communication pp 362-375.

[7] R. Pushplatha, “Cloud Computing And Security Issues”, international journal of engineering and computer science, ISSN:2319-7242, vol 3, issue 5, May 2014, pp 5764-5768.

[8] PoonamPardeshi, Deep0ali R. Borade, “Improving Data Integrity for Storage Security in Cloud Computing”, IJCSNS International journal of computer Science and network security, Vol. 15, No. 7, July 2015, pp 61-67.

[9] K. R. Monisha, “Secure Cloud ComputingUsing AES and RSA Algorithms”, Proceedings of 20th IRF International conference, ISBN:978-93-84209-01-8, 1 March 2015, pp 12-17.

[10] MervetBamiah, SarfarazBrohi, SuriayatiChuprat, Muhammad Nawaz Brohi, “Cloud Implementation Security Challenges”, Proceeding of 20125 international of mcloud computing technologies, application and management © 2012 IEEE, pp 174-178.

[11] S. Arul Oli, L. Arockiam, “ Confidentiality Technique for Enhancing Data Security Using Encryption and Obfuscation in Public Cloud Storage”, Inyternational Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2016, pp 431-435

[12] Cong-Wang S. M. Chow, Qian Wang, KuiRen, Wenjing Lou, “ Privacy Preserving Public Auditing for Secure Cloud Storage”, IEEE Transactions On Computer, Vol. 62, No.. 2, Feb. 2013