ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Review Paper on Data Security Techniques Used for Cloud Computing

Dushyant[1]

Department of Computer Science Engineering, Vivekananda Global University, Jaipur, India[1]

dushyant.singh@vgu.ac.in[1]

ABSTRACT: Now a day on the internet data is shared on a large basis and transferred on a large scale through the cloud computing techniques. In cloud computing it maintain it privacy and security so it's become very big task. Cloud computing is playing very important role in this. Tenant was of cloud computing techniques is technology a technology focused on the internet where consumers offer quality services including application and other information are available. These are also available on remote servers called outsourcing data as stored third party user resources consumer always looks for services that affordable and manageable and trust able too. So for consumers this is cheaper than no privacy hardware and application for purchase storing the details. During access the data provider must ensure that the data is secure, transaction may take place and the transaction must also take place to the data providers must be protected and needed visible.

KEYWORDS: Cloud, Integrity, Confidentiality, Cloud Computing, Data Security, Techniques.

I. INTRODUCTION

Distributed computing means a significant change by the way we store data and run applications. Presently as opposed to running projects and information on an individual personal computer, everything is facilitated in the "cloud"— a shared pool of PCs and workers got to through the Web. Cloud registering gives the office to get to all the reports also, application from anyplace on the planet and permits various gathering individuals to team up from various areas[1]. One of the greatest components of distributed computing which is broadly utilized is Information stockpiling ability. A few free what's more, dependable online stockpiling administrations accessible to the clients are Microsoft SkyDrive, Apple iCloud, Google Drive, Amazon S3, Dropbox and Space. As we become acquainted with such countless preferences of distributed computing however everything has a few advantages and disadvantages both and distributed computing isn't an exemption[2]. There are a few questions in client's mind prior to moving towards cloud registering. As the utilization of distributed computing gets broad, security of the re-appropriated client information turns into a significant exploration theme. The boundaries that are mulled over for information security are Privacy, Uprightness, and Accessibility. The issue of re-appropriating information faces the accompanying snags:

i)Confidentiality: We should trust and share certain third parties; they're our personal data? Is our data still there? Over the cloud confidential? While a service provider ensures that consumer data security is a fact the data in certain countries is physically located, and is subject to local laws and guidelines. Certainly, the provider countries allowed access to consumer data countries within its laws and regulations[3].

ii)Availability: Does the data we saved in the cloud? Will be there anytime we wanted it, i.e. disponibility data. If the customer is absolutely reliant on cloud data storage, quick access to it becomes necessary.

iii)Integrity: The third party data outsourcing must ensure for the person who saved the data on the cloud any unauthorized user will not be modified or modified. There are some doubts that any customer worries about or a cloud computing company that needs to shift. We'll learn about some strategies for this paper to ensure the security of cloud computing data storage.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

II. DISCUSSION

In any case, numerous individuals actually stress that information saved money on a distant stockpiling framework could be gotten to by different customers and they will adjust it. Programmers could likewise endeavor to take the actual machines on which information is put away[4]. A representative from a cloud specialist organization could modify or demolish information utilizing their verified client name and secret key. Rather than every one of these dangers, customers are embracing distributed computing generally. Distributed storage organizations are putting away a great deal of cash to ensure that their customers' information would be protected[5]. They are attempting to restrict the chance of information burglary or debasement. We are examining a few procedures here that are assisting with getting security on distributed storage and for various customers by perusing the distinctive examination paper. In this article we take a gander at the Confided in Stage Module (TPM). TPM gives privacy and honesty in mists. Kerberos is a procedure which is utilized to confirm the clients and SLA Evidence for recovering composed serializability, and newness in mists[6].

i)Problem statement: Security and stability are two main problems in cloud computing. Customers must ensure that their cloud-based data is not exploited by other customers. There are so many techniques and algorithms available to achieve security in the cloud. Some of these methods.

ii)Encryption: The complex algorithm is used in this technique to hide the original information using the encryption key. The data is converted and then saved in remote server storage into unreadable form known as cypher text.

iii)Authentication processes: A authentication framework is used to ensure that the cloud data is accessible by the only authenticated person. The user name and password must be established.

iv)Authorization practices: To determine who can access data saved on the cloud system, a list of registered clients is being used.

A. Trusted Storage System for the Cloud:

"A Confided Away Framework "store the information just as it needs private putting away additionally and keeps up the respectability of the information. To accomplish secrecy and trustworthiness of the information, cryptographic procedures can be utilized to encode information to encode the customer's information inside the cloud, Scrambled record frameworks (EFS) is utilized[7]. In EFS client's information is scrambled with the assistance of encryption key which changed the first information into figure text which is garbled for different clients. It builds up the Respectability of the information inside the cloud[8]. Five conventions are created which guarantee that the customer's information is put away just on confided away workers, Information is replicated distinctly on confided away workers, and assurance that the information proprietors and other advantaged clients of that information access the information safely. The framework depends on confidence in registering stage innovation.

i). Encrypted File Systems:

EFS is intended to encrypt saved data (the Secure File System). Encryption techniques are not conducted at programme level at file system level. Encryption is user-friendly and transparent. For encryption utilizing cryptographic techniques; thus users do not need to handle encryption keys. The method as seen below diagram EFS encryption[9].

ii) Trusted Platform Module:

The Trusted Platform Module (TPM) is a computer microchip or a microcontroller which performs various task related to security and cryptography. This technology provides the tools to authenticate the computer platform. The tools or objects can include certificates, encryption keys, passwords, and integrity metrics of a platform. The TPM can be used in the process of remote attestation of a platform of a machine which will be discussed further later. The chip is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

installed on the motherboard of a computer. The TPM communicates with the rest of the system by using a hardware bus. The TPM implementation of that specification as a chip. The specification is provided by the Trusted Computing Group[10].

B) Ensuring Data Storage Security in Cloud Computing with effect of Kerberos:

With Kerberos Authentication Program, this technology guarantees cloud storage stability. That is, by the introduction of the Kerberos; users will have storage protection. The ticket formation and award of the ticket to each user is specified for Kerberos. This system is more focused on consumers to boost protection.

i)Kerberos operation:

Kerberos utilizes the strategy of solid encryption technique and complex ticket conceding calculation so clients can be validated on organization. In this a meeting key is utilized which permits scrambled information streams over an IP network for every client. On the off chance that a new client needs to utilize the cloud, at that point he should make a profile on the organization by giving the data. In the wake of enlisting with Kerberos, the client will get his client ID and secret word which will likewise store on the worker Information base.

- Every client should follow following strides for utilizing cloud information:
- Sign on to the framework by utilizing client ID and secret phrases.
- Client will send the solicitation for ticket conceding pass to the Validation Worker.
- Confirmation worker checks the client's accreditation in the information base; make the ticket and meeting key. Results are scrambled utilizing key obtained from client secret key.
- Client will send the solicitation cloud administration allowing pass to Ticket Conceding worker.
- TGS will send the Ticket and meeting key to the client.
- Workstation sends ticket and authenticator to cloud worker supplier.
- Worker checks ticket and authenticator coordinate, whenever confirmed, and afterward award admittance to support.

ii)Enabling Security in Cloud Storage SLAS with Cloud Proof:

"Enabling Cloud Storage SLAs security with Cloud Proof" is another Cloud Storage Security strategy. This provides a stable, Cloud-based storage infrastructure designed especially for the cloud. Cloud evidence helps consumers to detect when data confidentiality, write serialization and freshness are abused. You will also demonstrate third-party breaches

III. CONCLUSION

During this discussion, we find many strategies that ensure the protection of cloud-based data. In this paper, we explain how the use of EFS and TPM technologies guarantees secrecy and honesty and also safe for the cloud computing. In this paper also discuss about the Kerberos which provides network for the user's and also provide the authentication. Cloud Evidence SLAs improve secrecy, honesty, seriality and freshness of reading (denoted by C, I, W, F). It is very complicated and cost efficient to have client privacy and cloud data but various technologies that we addressed in this document can be used to do it.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

REFERENCES

[1] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, 2012, doi: 10.1016/j.future.2010.12.006.

[2] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Secur. Priv.*, 2009, doi: 10.1109/MSP.2009.87.

[3] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," 2012, doi: 10.1109/ICCSEE.2012.193.

[4] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data Security and Privacy in Cloud Computing," *International Journal of Distributed Sensor Networks*. 2014, doi: 10.1155/2014/190903.

[5] C. L. Philip Chen and C. Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," *Inf. Sci. (Ny).*, 2014, doi: 10.1016/j.ins.2014.01.015.

[6] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," 2010, doi: 10.1109/ISSA.2010.5588290.

[7] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny).*, 2015, doi: 10.1016/j.ins.2015.01.025.

[8] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," 2015, doi: 10.1016/j.procs.2015.04.171.

[9] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, 2013, doi: 10.1186/1869-0238-4-5.

[10] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*. 2011, doi: 10.1016/j.jnca.2010.07.006.

[11] Vishal Jain, Dr. Mayank Singh, "Ontology Based Information Retrieval in Semantic Web: A Survey", International Journal of Information Technology and Computer Science (IJITCS), Hongkong, Vol. 5, No. 10, September 2013, page no. 62-69, having ISSN No. 2074-9015, DOI: 10.5815/ijitcs.2013.10.06.

[12] Vishal Jain, Dr. Mayank Singh, "Ontology Based Pivoted Normalization using Vector – Based Approach for Information Retrieval", IEEE Co-Sponsored 7th International Conference on Advanced Computing and Communication Technologies (ICACCT), In association with INDERSCIENCE Publishers, UK, IETE and Technically Co-sponsored by Computer Society Chapter IEEE Delhi Section, held on 16th November, 2013, organized by Asia Pacific Institute of Information Technology SD India, Panipat, India.

[13] Vishal Jain, Dr. Mayank Singh, "Ontology Based Web Crawler to Search Documents in the Semantic Web", "Wilkes100 - Second International Conference on Computing Sciences", in association with International Neural Network Society and Advanced Computing Research Society, held on 15th and 16th November, 2013 organized by Lovely Professional University, Phagwara, Punjab, India and proceeding published by Elsevier Science.

[14] P. Lavanya, R. Meena, R. Vijayalakshmi, Prof. M. Sowmiya, Prof. S. Balamurugan , " A Novel Object Oriented Perspective Design for Automated BookBank Management System", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015.

[15] P.Andrew , J.Anishkumar , Prof.S.Balamurugan , S.Charanyaa, " A Survey on Strategies Developed for Mining Functional Dependencies", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015.

[16] SV Amridh Varshini, R Kaarthi, N Monica, M Sowmiya, S Balamurugan, "Entity Relationship Modeling of Automated Passport Management System", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 2, February 2015

[17] J Ganeshkumar, N Rajesh, J Elavarasan, M Sarmila, S Balamurugan, "Certain Investigations on Anonymous Authentication Mechanisms for Data Stored in Clouds", International Journal of Innovative Research in Computer and Communication Engineering, 2015