Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Data Security in Cloud Computing Using Combined Approach

Venshila SanthaKumar[1]
Post-Graduate Student,
Department of CSE,
Karunya University,India

Jeno Lovesum [2]
Assistant professor,
Department of CSE,
Karunya University, India

***Abstract* - Cloud computing plays the vital role in the IT sectors emerging trends. It has the resources like availability of data, low cost and many other uses. But the security is the major issue in cloud. Specialized procedures and the different techniques are compressed to form as the frame work for providing the security in this paper. The goal of this paper is to provide the security of data from the starting of the process to till the end. By using three cryptographic parameters, SSL encryption technique, MAC for integrity and by the user authentication the security is provided for the data in cloud.**

Keywords: Cloud computing, Security, integrity.

I. INTRODUCTION

It is used to describe a variety of different computing concepts that involves a large number of computers, which is connected through a real time communication network. It offers the huge space for the data storage. Cloud computing refers to the computation of different resources and delivers the computed resource across the internet. Instead of keeping data on own hard drive or updating the application needs in our own, can be done across the internet also. At remote locations it allows the individuals and business to use the hardware and software, which is managed by the third parties.

1.1 Characteristics:

On demand self service: For each service provider email, applications, network or server service can be provided without human interaction.

Broad network access: Is available over the network and it can be accessed through the standard mechanisms**.**

Resource pooling: To serve the multiple consumers the resources are pooled together.

Other characteristics such as rapid elasticity and measured service are also available.

1.2 Types of cloud:

Private cloud: Used for single organization. It can be internally or externally hosted.

Public cloud: Provisioned for open use for the public by a particular organization who also host the service.

Community cloud: Shared by several organizations. Typically externally hosted.

Hybrid cloud: It is the components of two or more cloud. Goal of the hybrid cloud is to minimize the change. It takes the advantages in cost effectiveness and scalability.

Google, amazon, and IBM are using the cloud computing.

II. RELATED WORKS

II.1 Proofs of Retrievability: Theory and Implementation

Bowers KD, Juels A, Oprea A, used the methodology like Adversarial model, keygen algorithm, challenge algorithm, respond algorithm, extract algorithm. It has the advantages such as storage overhead and proof costs, tolerates higher error rates, secure in a stronger adversarial setting.

II.2 A High-Availability and Integrity Layer for Cloud Storage

Bowers KD, Juels A, Oprea A. methodologies discussed by them are redistribute algorithm, challenge response algorithm. High compact ability, robust against an active mobile adversary are the advantages.

II.3 Computationally Private Information Retrieval with Poly logarithmic Communication

Cachin C, Micali S, Stadler M. mentioned about the database algorithm D and user algorithms. It clearly states the improved computational complexity.

II.4 Private Information Retrieval

Chor B, Gilboa N, computational theorem for two server scheme, Collision-resistant cryptographic hash functions were used by them. It reduce the communication complexity of schemes in which the user's queries.

II.5 Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility

Dikaiakos MD, depicts with soa architechture and some crypto concepts. It highlights about cost sharing and reduction, interoperability, increased autonomy, privacy.

II.6 Revisiting the Computational Practicality of Private Information Retrieval

Gertner Y, Ishai used the methodology such as single-server PIR scheme, trivial PIR solution and multi-server PIR schemes. It provides the realistic computation power and network bandwidth.

II.7 PORs: Proofs of Retrievability for Large Files

Juels A, Burton J, Kaliski S. described their concepts with the symmetric key cryptography, saas, sentinel-based POR scheme, Reed-Solomon code. It has the advantages like quality-of-service guarantees, security guarantees of our protocol.

II.8 Towards Analyzing Data Security Risks in Cloud Computing Environments

Encryption trust mechanism, trusted transitive encryption are used by Julisch K, Hall M.. it helps in Security risk analysis.

II.9 Cryptographic Cloud Storage

Kamara S, Lauter , symmetric encryption and digital signatures, symmetric searchable encryption (SSE), Attribute-based Encryption are used by them. Data retention and destruction, security, availability are available in this.

II.10 Replication is not needed: single database, computationally private information retrieval

Kusilevitz E, Ostrovsky described their concepts with oblivious transfer protocol. Here they concluded that replication of data is not necessary in order of retrieving.

II.11Compact Proofs of Retrievability

Hovav Shacham and Brent Waters used the techniques like cryptographic, combinatorial, and coding-theoretical techniques, and storage algorithm to implement their concepts. Public verifiability, Extractability are the parameters, and it has the advantages as, the attacker cannot query the random oracle, validating the integrity of blocks. And it fails redundantly to encode the file.

II.12 Data security metrics based on the above section are compared in the below table.

Methodology	Cost	Asymmetric effect	Error rate	Reliability	Code redundancy	Integrity	Processing time for cpu	Locality	Response time
Adversarial model, keygen algorithm, challenge algorithm, respond algorithm, extract algorithm.			√						
Redistribute algorithm, challenge response algorithm					√				
Database algorithm D and user algorithms.							√		
soa architecture				√					
Single-server PIR scheme, trivial PIR solution and multi-server PIR schemes						√			√
Symmetric key cryptography, saas, Reed-Solomon code.	√								

Encryption trust mechanism.								√	
Symmetric encryption and digital signatures							√		

III. CONCLUSION

The comparison of base paper with literature survey of several papers, it is concluded that, protection of data, integrity check and authentication are done in this paper with best possible industry mechanisms.

REFERENCES

[1] Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive. Report 2008/175; 2008a.

[2] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print Archive. Report 2008/489, 2008b.

[3] Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication, LNCS Springer Verlag, Advances in Cryptol- ogy- EUROCRYPT'99, 1592, p. 402–414, 1999.

[4] Chor B, Gilboa N, Naor M. Private information retrieval by keywords. Report 98-03. Theory of Cryptography Library, 1998.

[5] Dikaiakos MD, Katsaros D, Pallis G, Vakali A,Mehra P. Cloud computing. IEEE Internet Computing 2009;12(5):10–3.

[6] Gertner Y, Ishai Y, Kushilevitz E. Protecting data privacy in private information retrieval schemes,In Proceedings of the 30th annual ACM symposium on theory of computing, ACM, p.151–160,1998.

[7] Juels A, Burton J, Kaliski S. PORs: proofs of retrievability for large files. Proceedings of CCS'07,p.584–597,2007.

[8] Julisch K, Hall M. Security and control in the cloud. Information Security Journal: A Global Perspective 2010;19(6):299–309.

[9] Kamara S, Lauter K. Cryptographic cloud storage. Lecture Notes in Computer Science 2010;6054:136–49.

[10] Kusilevitz E, Ostrovsky R. Replication is not needed: single database, computationally private information retrieval, In Proceedings of the 38th annual symposium on foundations of computer science, IEEE, p. 364–373, 1997.

[11] Shacham H, Waters B. Compact Proofs of Retrievability, Proceedings of Asiacrypt '08, 5350, p. 90–107, 2008.