International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 11: November 2015, pp 3-4. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey on Data Security Using Identity Based Encryption in Cloud Computing

Sowmya R, Dr.P Ezhilarasu, Satheesh Kumar D, Manoj Prabhakar J

***Abstract*—** In this paper, we discuss about the various data security techniques used to secure the data in cloud computing. Many papers are taken for survey. Its advantages and disadvantages are discussed.

***Keywords*—** Identity-based encryption (IBE), revocation, outsourcing, cloud computing

I. INTRODUCTION

Cloud computing is a model that enable omnipresent network access to a shared pool of configurable computing resources[1].Cloud computing and storage solution provide capabilities to users for store and process their data in third party data centers[2]. To make the data confidential, an algorithm and secret key are used for the data to be encrypted. After encryption process the data gets converted into cipher text. To decrypt the cipher text, similar algorithm is used to obtain the original data. Identity-Based Encryption (IBE) is an alternative to public key encryption. It simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities such as unique name, email address, IP address as public keys. Hence sender using IBE does not need to look up public key and certificate, but directly encrypts message with receiver's identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. Revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques.

Cloud computing offers three important service [1] as shown in the figure 1. Those are

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service(IaaS)

Cloud computing is an enhancement of desktop computing. The main limitation in cloud computing is its security as compared to desktop computing. In normal network we can provide security using any one method .Ex [3].Hence there is a need for enhancing the security in cloud computing. Because the third party also involved in providing cloud computing services. There are three types in cloud

Those are
Private cloud
Public cloud
Community cloud

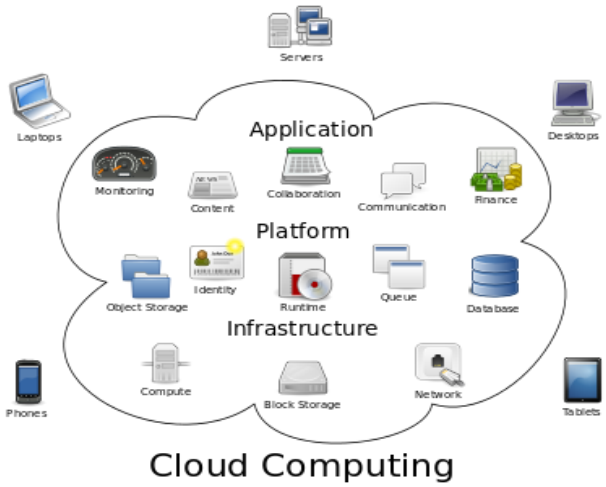

Fig.1.Cloud computing services [1]

In case of public cloud the security level is low as compared to the private cloud.

II. VARIOUS SECURITY METHODS

The various security methods are given in the table 1.

Table.1.Analysis of security methods

S. NO	Title	Description
1.	Privacy Preserving Access Control with Authentication For Securing Data in Clouds [4].	This method have privacy preserving Authenticated access control scheme for securing data in clouds. The cloud verifies the authenticity of the user without knowing the user's identity before storing information.
2.	Toward Secure and Dependable Storage Services in Cloud Computing [5].	This method allows users to audit the cloud storage with very lightweight communication and computation cost and achieves fast data error localization. It secures dynamic operations on outsourced data, including block modification, deletion, and append.
3.	Fuzzy Keyword Search over Encrypted Data In	This technique maintains the keyword privacy. Based on keyword similarity semantics it matches the exact files or

Sowmya R, PG scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: priyamka.nk@gmail.com)
Dr.P Ezhilarasu, Associate Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: prof.p.ezhilarasu@gmail.com)
Satheesh Kumar D, Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: dsatheeshme@gmail.com)
Manoj Prabhakar J, PG scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: ash.cupid24@gmail.com)

	Cloud Computing [6].	closely related matching files when user searches the inputs.
4.	Cryptographic Cloud Storage [7].	This method provide a high level, several architectures that combine recent and non-standard cryptographic primitives to achieve a secured cloud storage service on top of a public cloud infrastructure.
5.	Identity-Based Cryptography for Cloud Security[8].	This method a novel Hierarchical Architecture for Cloud Computing (HACC),Identity-Based Encryption (IBE) and Identity-Based Signature (IBS) to allow the users with a platform of limited Performance to outsource their computational tasks to more powerful servers.
6.	A fully homomorphic encryption scheme [9].	This technique fully homomorphic encryption scheme, solving a central open problem in cryptography.
7.	Token-Based Cloud Computing [10].	This method focus on the applications where the latency of the computation should be minimized by using trusted hardware token with Secure Function Evaluation (SFE)
8.	Trust Cloud: A Framework for Accountability and Trust in Cloud Computing [11].	This paper discusses key challenges in achieving a trusted cloud through the use of detective controls, and presents the Trust Cloud framework, which addresses accountability in cloud computing via technical and policy based approaches.
9.	Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing [12].	This method tackles the hidden area in cloud computing, by a new secure provenance scheme based on the bilinear pairing techniques.
10.	Adding Attributes to Role-Based Access Control [13].	In this technique attribute-based access control (ABAC) suggests that attributes and rules could either replace RBAC or make it more simple and flexible.

III. CONCLUSION

In this paper, we studied about various data security method to prevent the malicious attackers. Toward Secure and Dependable Storage Services in Cloud Computing technique provide opportune to users when the data is moved into the cloud .Amazon Simple Storage Service (S3),

and Amazon Elastic Compute Cloud (EC2) are internet-based online services that provide huge amounts of storage space ,resources and make the responsibility of data maintenance at the same time.

REFERENCES

[1] https://en.wikipedia.org/wiki/cloud computing.

[2] Haghighat M.,zonouz,s.,and Abdel-Mottaleb,M, “CloudID: Trustworthy cloud-based and cross-Enterprise Biometric identification” Expert Systems with Applications, Vol. 42, No. 21, pp.7905-7916,2015.

[3] Rohit G Bal, Dr P Ezhilarasu, “An efficient safe and secured video steganography using Shadow Derivation”, International Journal of innovative Research in computer and communication Engineering, Vol.2, March 2014.

[4] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak,” Privacy Preserving Access Control with Authentication for Securing Data in Clouds” 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 556-563,2012

[5] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, vol.5, no. 2, pp. 220-232, Second 2012, doi:10.1109/TSC.2011.24

[6] T.Balamuralikrishna, C. Anuradha, N.Raghavendrasai1,” Fuzzy keyword search over encrypted data in cloud computing” Asian Journal Of Computer Science And Information Technology, Vol.1,No.3,pp.86-88,2011.

[7] Seny Kamara, Kristin Lauter,”Cryptographic Cloud Storage”. Financial Cryptography and Data Security, Volume 6054 of the series Lecture Notes in Computer Science pp 136-149,2010.

[8] Hongwei Li, Yuanshun Dai, Bo Yang: Identity-Based Cryptography for Cloud Security. IACR Cryptology ePrint Archive 2011: 169 (2011)

[9] Craig Gentry. "A Fully Homomorphic Encryption Scheme (Ph.D. thesis)", 2009.

[10] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy,”Token-Based Cloud Computing”. Trust and Trustworthy ComputingVolume 6101 of the series Lecture Notes in Computer Science pp 417-429, 2010.

[11] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, "TrustCloud - A Framework for Accountability and Trust in Cloud Computing", IEEE 2nd Cloud Forum for Practitioners (IEEE ICFP 2011), IEEE Computer Society, Washington DC, USA, 7-8 July 2011.

[12] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin Sherman Shen - Secure provenance: the essential of bread and butter of data forensics in cloud computingProceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10) pp. 282--292, New York, NY, USA,2010

[13] Richard Kuhn, Edward J. Coyne, Timothy R. Weil, “Adding Attributes to Role-Based Access Control” , IEEE Computer, vol. 43, no. 6 ,2010 , pp. 79 – 81.