Accepted Manuscript

Attribute based encryption in cloud computing: A survey, gap analysis, and future directions

P. Praveen Kumar, P. Syam Kumar, P.J.A. Alphonse

PII: S1084-8045(18)30054-7

DOI: 10.1016/j.jnca.2018.02.009

Reference: YJNCA 2068

To appear in: *Journal of Network and Computer Applications*

Received Date: 26 June 2017

Revised Date: 13 December 2017

Accepted Date: 17 February 2018

Please cite this article as: Kumar, P.P., Kumar, P.S., Alphonse, P.J.A., Attribute based encryption in cloud computing: A survey, gap analysis, and future directions, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.02.009.

Attribute Based Encryption in Cloud Computing: A Survey, Gap Analysis, and Future Directions

P.Praveen Kumar[a,*], P.Syam Kumar[b], P.J.A.Alphonse[a]

[a]*Department of Computer Applications, National Institute of Technology, Tiruchirappalli, India*
[b]*Institute for Development and Research in Banking Technology, Hyderabad, India*

Abstract

Cloud computing facilitates to store and access the data remotely over the internet. However, storing the data in the untrusted cloud server leads the privacy and access control issues in the cloud. The traditional encryption schemes such as symmetric and asymmetric schemes are not suitable to provide the access control due to lack of flexibility and fine-grained access control. One of the prominent cryptographic technique to provide privacy and fine-grained access control in cloud computing is Attribute Based Encryption. In this paper, we comprehensively survey the various existing key policy and ciphertext policy attribute based encryption schemes based on access structure, and multi-authority schemes. Moreover, this review explores more on ciphertext policy attribute based encryption in different aspects such as hidden policy, proxy re-encryption, revocation mechanism, and hierarchical attribute based encryption. Further, this paper compares different ABE schemes based on the features, security, and efficiency. This paper also identifies the suitability of attribute based encryption for practical applications. Finally, this paper analyse the different ABE schemes to find out the research gap and challenges that needs to be investigated further on the Attribute Based Encryption.

Keywords: Cloud computing, Attribute based encryption, Key policy, Ciphertext policy, Fine-grained access control, Revocation mechanism.

1. Introduction

Cloud environment [1-3] provides the new dimension of utilizing information technology resources in the business. The cloud delivers the resources based on the on-demand and pay by use model i.e. whenever we need the additional resources based on the request, the service will be allotted and charged. The cloud delivers the variety of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) to cloud users as shown in Fig. 1. SaaS provides the application to the user such as webmail, program interface, and web browser. PaaS provides the programming languages, libraries, services, and tools, etc. IaaS provides the infrastructure, such as storage, networks, and other processing and computing resources. There are various deployment models such as private, public, community, and hybrid cloud. Private cloud is owned by a single organization, whereas the public cloud is shared by multiple consumers. Community cloud means the same kind of community consumers can join and use this service. Hybrid cloud is the combination of any two above-said deployment models of the cloud. Based on the user need and requirement, the user may choose specific services and deployment model.

* Corresponding author
Email addresses: tvp.praveen@gmail.com (P.Praveen Kumar), psyamkumar@idrbt.ac.in (P.Syam Kumar), alphonse@nitt.edu (P.J.A.Alphonse)