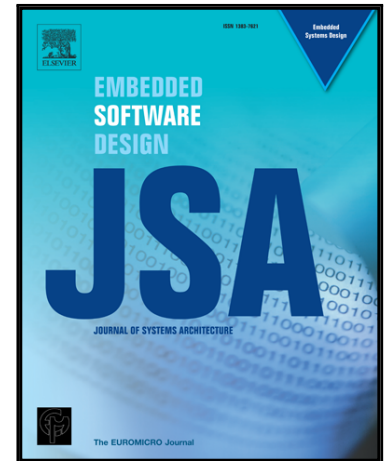


Accepted Manuscript

Access Control Based Privacy Preserving Secure Data Sharing with Hidden Access Policies in Cloud

S. Sabitha, M.S. Rajasree

PII: S1383-7621(17)30133-9
DOI: [10.1016/j.sysarc.2017.03.002](https://doi.org/10.1016/j.sysarc.2017.03.002)
Reference: SYSARC 1424



To appear in: *Journal of Systems Architecture*

Received date: 22 February 2016
Accepted date: 3 March 2017

Please cite this article as: S. Sabitha, M.S. Rajasree, Access Control Based Privacy Preserving Secure Data Sharing with Hidden Access Policies in Cloud, *Journal of Systems Architecture* (2017), doi: [10.1016/j.sysarc.2017.03.002](https://doi.org/10.1016/j.sysarc.2017.03.002)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Access Control Based Privacy Preserving Secure Data Sharing with Hidden Access Policies in Cloud

Sabitha S¹

sabitha@cet.ac.in
Research Scholar, University of Kerala
College of Engineering Trivandrum

Rajasree M S

rajasree.ms@iiitm.ac.in
IIITMK, Trivandrum

Abstract

Attribute-based encryption is a promising solution to the access control based data sharing in the cloud. In this scheme, access policies are being sent in plaintext form which discloses the user privacy and data privacy. Once the ciphertext has been shared among the set of authorized users they would be able to decrypt the ciphertext. Whenever the authorized users are acting as malicious users, they may alter the data and further encrypt and outsource the modified data. It may adversely affect the data owner. In the existing attribute-based encryption scheme, data owner's authenticity cannot be verified. In order to resolve these problems, we are proposing a novel idea to anonymize the access policy and a signature scheme to verify the authenticity of data as well as that of the data owner. Anonymized access policy never discloses the privacy. The signature scheme is able to detect the insider attack on attribute-based encryption scheme. The proposed system is secure against indistinguishable chosen-ciphertext attack. It is a provably secure and existentially unforgeable access control based data sharing method in the public cloud.

Keywords: Attribute-Based Encryption, Access Policy, Data

*Corresponding author: Sabitha S, ssabithasureshkumar@gmail.com

Download English Version:

<https://daneshyari.com/en/article/4956232>

Download Persian Version:

<https://daneshyari.com/article/4956232>

[Daneshyari.com](https://daneshyari.com)