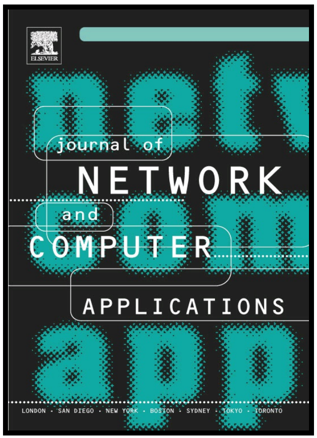
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud

Daniel Ricardo dos Santos, Roberto Marinho, Gustavo Roecker Schmitt, Carla Merkle Westphall, Carlos Becker Westphall

PII: S1084-8045(16)30171-0
DOI: http://dx.doi.org/10.1016/j.jnca.2016.08.013
Reference: YJNCA1695

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

Received date: 13 April 2016
Revised date: 11 July 2016
Accepted date: 12 August 2016

A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud

Daniel Ricardo dos Santos[a,*], Roberto Marinho[a], Gustavo Roecker Schmitt[a], Carla Merkle Westphall[a], Carlos Becker Westphall[a]

[a]*Networks and Management Laboratory*
Department of Informatics and Statistics
Federal University of Santa Catarina
88040-970 - Florianópolis - SC - Brazil

Abstract

Cloud computing is advantageous for customers and service providers. However, it has specific security requirements that are not captured by traditional access control models, e.g., secure information sharing in dynamic and collaborative environments. Risk-based access control models try to overcome these limitations, but while there are well-known enforcement mechanisms for traditional access control, this is not the case for risk-based policies. In this paper, we motivate the use of risk-based access control in the cloud and present a framework for enforcing risk-based policies that is based on an extension of XACML. We also instantiate this framework using a new ontology-based risk assessment approach, as well as other models from related work, and present experimental results of the implementation of our work.

Keywords: access control, cloud computing, risk

1. Introduction

Cloud computing enables the delivery of computational resources and services through the Internet, providing easy access, elasticity and resource sharing [1]. The cloud model is widely adopted because of its economical and performance advantages for customers and service providers. However, the growing number of users and available resources, as well as the diversity of supported applications, emphasize the security challenges of this model [2].

Access control is crucial to ensure the correct enforcement of security policies on the cloud. There are well-known solutions to enforce policies based on traditional access control models, such as the eXtensible Access Control Markup Language (XACML) [3]. Nonetheless, the emergence of new requirements in access control, derived from current information security needs and the needs

[*] Corresponding author
Email address: danielrs@inf.ufsc.br (Daniel Ricardo dos Santos)