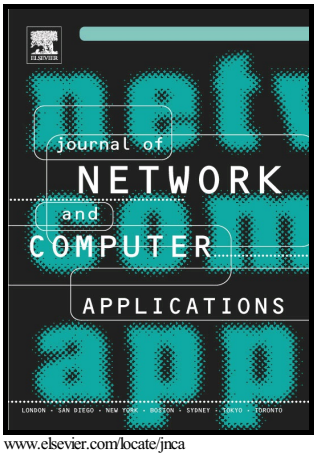
Author's Accepted Manuscript

Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution

Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki, Arcangelo Castiglione



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30392-2
DOI: https://doi.org/10.1016/j.jnca.2017.11.012
Reference: YJNCA2015

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

Received date: 19 May 2017
Revised date: 3 November 2017
Accepted date: 28 November 2017

Cite this article as: Lu Zhou, Quanlong Wang, Xin Sun, Piotr Kulicki and Arcangelo Castiglione, Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution, *Journal of Network and Computer Applications,* https://doi.org/10.1016/j.jnca.2017.11.012

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 galley proof before it is published in its final citable 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.

ACCEPTED MANUSCRIPT

Quantum Technique for Access Control in Cloud Computing II: Encryption and Key Distribution

Lu Zhou[a], Quanlong Wang[b], Xin Sun[c], Piotr Kulicki[d], Arcangelo Castiglione[e]

[a] *University of Aizu, Japan*
[b] *University of Oxford, UK*
[c] *Sun Yat-sen University, China*
[d] *The John Paul II Catholic University of Lublin, Poland*
[e] *University of Salerno, Italy*

Abstract

This is the second paper of the series of papers dealing with access control problems in cloud computing by adopting quantum techniques. In this paper we study the application of quantum encryption and quantum key distribution in the access control problem. We formalize our encryption scheme and protocol for key distribution in the setting of categorical quantum mechanics (CQM). The graphical language of CQM is used in this paper. The quantum scheme/protocol we propose possesses several advantages over existing schemes/protocols proposed in the state of the art for the same purpose. They are informationally secure and implementable by the current technology.

Keywords: quantum encryption, quantum key distribution, categorical quantum mechanics, access control

1. Introduction

This is the second paper of the series of papers dealing with access control problems in cloud computing by adopting quantum technique [30]. A simple model for the access control problem in cloud computing is shown in Fig. 1. Such a model has three components: *data owner*, *cloud* and *data user*. The

[☆] The names of the authors are ordered anti-alphabetically. Xin Sun is also affiliated with the John Paul II Catholic University of Lublin.

Email address: xin.sun.logic@gmail.com (Xin Sun)

Accepted manuscript

Download English Version:

https://daneshyari.com/en/article/6884879

Download Persian Version:

https://daneshyari.com/article/6884879

Daneshyari.com