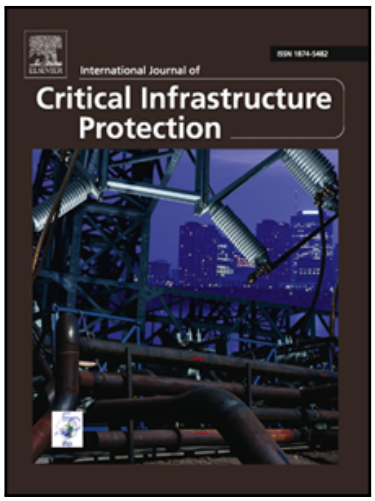

An improved authentication protocol for distributed mobile cloud computing services

Hoda Jannati, Behnam Bahrak

PII: S1874-5482(16)30002-6
DOI: 10.1016/j.ijcip.2017.10.003
Reference: IJCIP 228

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 4 January 2016
Revised date: 24 October 2017
Accepted date: 24 October 2017

Please cite this article as: Hoda Jannati, Behnam Bahrak, An improved authentication protocol for distributed mobile cloud computing services, *International Journal of Critical Infrastructure Protection* (2017), doi: 10.1016/j.ijcip.2017.10.003

An improved authentication protocol for distributed mobile cloud computing services

Hoda Jannati[a1] and Behnam Bahrak[b]

[a]*School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Farmanieh Avenue, Tehran 19538-33511, Iran*
[b]*School of Electrical and Computer Engineering, College of Engineering, University of Tehran, North Kargar Street, Tehran 14395-515, Iran*

Abstract

Cloud computing is a popular network access model for the transparent and ubiquitous sharing of services and computing resources among customers by service providers. In the critical infrastructure domain, cloud computing is used by governments for applications such as revenue collection to improve operations and achieve cost savings. Although cloud computing systems promise convenience, they threaten the privacy of users who transfer their applications to the cloud. In order to prevent illegal access, it is imperative that cloud providers implement secure authentication schemes.

Tsai and Lo have recently proposed an efficient authentication protocol based on a bilinear pairing cryptosystem for use in distributed mobile cloud computing services. They claim that the protocol provides mutual authentication and privacy to users, and also generates and exchanges session keys for each pair of communicating parties. This paper analyzes the security of the authentication protocol and demonstrates that the protocol is vulnerable to impersonation attacks and does not provide user anonymity and untraceability to users. The improved protocol presented in this paper prevents impersonation attacks and provides user anonymity and untraceability with only slight performance degradation.

[1]Corresponding author: Hoda Jannati (hodajannati@ipm.ir)