Accepted Manuscript

Provably secure authenticated key agreement scheme for distributed mobile cloud computing services

Vanga Odelu, Ashok Kumar Das, Saru Kumari, Xinyi Huang, Mohammad Wazid

PII: S0167-739X(16)30306-5
DOI: http://dx.doi.org/10.1016/j.future.2016.09.009
Reference: FUTURE 3159

To appear in: *Future Generation Computer Systems*

Received date: 29 May 2016
Revised date: 12 August 2016
Accepted date: 15 September 2016

Please cite this article as: V. Odelu, A.K. Das, S. Kumari, X. Huang, M. Wazid, Provably secure authenticated key agreement scheme for distributed mobile cloud computing services, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.09.009

Provably secure authenticated key agreement scheme for distributed mobile cloud computing services

Vanga Odelu [a,b], Ashok Kumar Das [c], Saru Kumari [d], Xinyi Huang [e], Mohammad Wazid [f]

[a] *Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*
[b] *Department of Computer Science and Engineering, Indian Institute of Information Technology, Chittoor, Sri City 517 588, Andhra Pradesh, India*
E-mail: odelu.vanga@gmail.com, odelu.vanga@iiits.in
[c] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[d] *Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India*
E-mail: saryusiirohi@gmail.com
[e] *Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian, China and the State Key Laboratory of Cryptology, Beijing, China*
E-mail: xyhuang81@gmail.com
[f] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
E-mail: mohammad.wazid@research.iiit.ac.in, wazidkec2005@gmail.com

Abstract

With the rapid development of mobile cloud computing, the security becomes a crucial part of communication systems in a distributed mobile cloud computing environment. Recently, in 2015, Tsai and Lo proposed a privacy-aware authentication scheme for distributed mobile cloud computing services. In this paper, we first analyze the Tsai-Lo's scheme and show that their scheme is vulnerable to server impersonation attack, and thus, their scheme fails to achieve the secure mutual authentication. In addition, we also show that Tsai-Lo's scheme does not provide the session-key security (SK-security) and strong user credentials' privacy when ephemeral secret are unexpectedly revealed to the adversary. In order to withstand these security pitfalls found in Tsai-Lo's scheme, we propose a provably secure authentication scheme for distributed mobile cloud computing services. Through the rigorous security analysis, we show that our scheme achieves SK-security and strong credentials' privacy and prevents all well-known attacks including the impersonation attack and ephemeral secrets leakage attack. Furthermore, we simulate our scheme for the formal security analysis using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, and show that our scheme is secure against passive and active attacks including the replay and man-in-the-middle attacks. More security functionalities along with reduced computational costs for the mobile users makes our scheme more appropriate for the practical applications as compared to Tsai-Lo's scheme and other related schemes. Finally, to demonstrate the practicality of the scheme, we evaluate the proposed scheme using the broadly-accepted NS-2 network simulator.

Keywords: Cloud computing, SK-security, credentials privacy, mutual authentication, user untraceability, AVISPA, NS2 simulation.

1. Introduction

In recent couple of decades, the use of mobile devices, such as smart phones and laptops, is rapidly increasing due to the portability and availability of mobile devices. ABI Research forecasts that by the end of 2015 more than 240 million mobile business users will utilize cloud services driving nearly $5 billion in revenues [1, 2, 3, 4, 5, 6, 7]. Thus, the user mobility is a highly desirable feature in the distributed computer networks and telecommunication systems. In mobile cloud computing, the mobile users can access computation results, resources, applications, and services that are stored, implemented, and deployed in cloud comput-