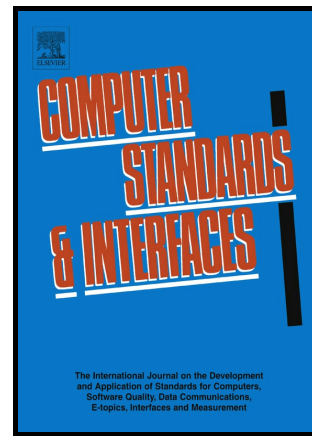


Author's Accepted Manuscript

A Secure and Privacy-Preserving Mobile Wallet
with Outsourced Verification in Cloud Computing

Zhen Qin, Jianfei Sun, Abubaker Wahaballa,
Wentao Zheng, Hu Xiong, Zhiguang Qin



www.elsevier.com

PII: S0920-5489(16)30190-8
DOI: <http://dx.doi.org/10.1016/j.csi.2016.11.012>
Reference: CSI3174

To appear in: *Computer Standards & Interfaces*

Received date: 14 March 2016
Revised date: 3 November 2016
Accepted date: 25 November 2016

Cite this article as: Zhen Qin, Jianfei Sun, Abubaker Wahaballa, Wentao Zheng, Hu Xiong and Zhiguang Qin, A Secure and Privacy-Preserving Mobile Wallet with Outsourced Verification in Cloud Computing, *Computer Standards & Interfaces*, <http://dx.doi.org/10.1016/j.csi.2016.11.012>

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

A Secure and Privacy-Preserving Mobile Wallet with Outsourced Verification in Cloud Computing

Zhen Qin^a, Jianfei Sun^a, Abubaker Wahaballa^a, Wentao Zheng^a, Hu Xiong^{b,*},
Zhiguang Qin^a

^aUniversity of Electronic Science and Technology of China, Chengdu, China, 610051

^bState Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China

Abstract

Mobile wallet, also known as mobile payment, is becoming one of the most frequently used approach to provide payment services under financial regulation via mobile device and may redefine our lifestyle with the rapid popularity of mobile Internet. In this paper, we address the security of the mobile wallet by providing a detailed threat analysis and identifying some unique design requirements in terms of security and privacy protection for mobile wallet. We then provide a novel approach to secure the mobile wallet and protect the privacy of the mobile user by incorporating the digital signature and pseudo-identity techniques. In view of several advantages of cloud computing, the computation task on the client side, which is usually featured with limited computation resources, is outsourced to the untrusted cloud server securely. The performance of our approach is evaluated via both theoretic analysis and experimental simulations. Also, the security analysis demonstrate that our approach can achieve desirable security properties of mobile wallet.

Keywords: Mobile wallet, Digital Signature, Secure Computation Outsourcing, Cloud Computing.

*Corresponding author

Email address: xionghu.uestc@gmail.com (Hu Xiong)

متن کامل مقاله

دریافت فوری ←

ISIArticles

مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات