International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **7**, July **2010**

 ISSN 1349-4198
pp. 3239–3245

AN EFFICIENT INTERNET ON-LINE TRANSACTION MECHANISM

Chin-Chen Chang[1,2] and Shih-Chang Chang[1]

[1]Department of Computer Science and Information Engineering
National Chung Cheng University
160 San-Hsing, Ming-Hsiung, Chiayi 621, Taiwan
{ ccc; csc96p }@cs.ccu.edu.tw

[2]Department of Information Engineering and Computer Science
Feng Chia University
100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan

Received January 2009; revised May 2009

Abstract. *Even with the popularity of on-line transactions, security remains customers' main concern in deciding whether to make an on-line transaction or not. In 2005, Tzeng et al. proposed a secure on-line software transaction scheme. However, we find that their scheme has the deadlock problem and is inefficient. We propose an efficient novel on-line transaction method that can solve the deadlock problem. The security of the novel method is based on several cryptographic techniques, including the secure one-way hash function and RSA cryptosystems. Our method also has lower computational cost than that of Tzeng et al.*
Keywords: On-line transaction, One-way hash function, RSA cryptosystems, Authentication

1. **Introduction.** With the rapid development of computer technologies, more and more financial transactions, called e-commerce, are completed on the Internet. Commercial "goods" sold through the Internet can either be physical or nonphysical. Physical goods may be sent to customers through certain traditional approaches, resulting in extra costs such as inventory cost and packaging costs. Nonphysical goods, like software, can be sent through the Internet and are easier to deliver than physical goods. Software is one example of nonphysical goods. If software is purchased through on-line transaction, costs related to packaging, distribution and middlemen will be reduced.

The software data is sent through the Internet to the certain place. So we describe the characteristics of the Internet to show that product, like software, can be received by the customers. Then, we show the characteristics as following:

(1) Publicity: One that uses application programs, there is no need to know his identity. Each user can send his data or receive any information through the Internet.
(2) Anonymity: While sending or receiving data, we can get the user's IP address. But we are unable to obtain other personal information about the user.
(3) Diversity: Because the Internet is public, anyone can develop or do anything in any form, e.g. doc, txt, etc. Therefore, we can receive any kinds of the information in the Internet.
(4) Non-geographical limitation: Internet users come from all over the world. Everyone can communicate with others come from other country at anytime.
(5) Digital environment: Information transferred through the Internet is digital data. Hence, it is easy to copy or obtain data and information.