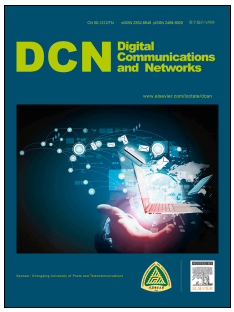
# Accepted Manuscript




An improved and secure multi-server authentication scheme based on biometrics and smartcard

Ashish Kumar, Hari Om

PII: S2352-8648(17)30035-4

DOI: 10.1016/j.dcan.2017.09.004

Reference: DCAN 104

To appear in: *Digital Communications and Networks*

Received Date: 24 January 2017

Accepted Date: 8 September 2017

Please cite this article as: A. Kumar, H. Om, An improved and secure multi-server authentication scheme based on biometrics and smartcard, *Digital Communications and Networks* (2017), doi: 10.1016/j.dcan.2017.09.004.

# An Improved and Secure Multi-Server Authentication Scheme based on Biometrics and Smartcard

Ashish Kumar[1], Hari Om[1]
[1]Department of Computer Science & Engineering
Indian Institute of Technology (ISM), Dhanbad, Jharkhand-826004
samrata@live.com, hariom4india@gmail.com

## ABSTRACT

With the advancement in internet technologies, number of servers has been increased remarkably to bring more services for end users. These services are provided over the public channels, which are insecure and susceptible to interception, modification, and deletion. In order to provide security, authentication of registered entities is performed and then a session key is established between them to communicate securely. The conventional schemes allow a user to access services only after getting registered with each desired server in a multiserver system independently. For this purpose, one needs to keep multiple smartcards and memorize various identities and passwords for getting the services from multiple servers. This has led to adoption of multiserver authentication in which a user accesses services of multiple servers after registering himself at only one central authority. Recently Kumar and Om have discussed a scheme for multiserver environment using smartcard. Since the user memorable passwords are of low entropy, it is possible for an attacker to guess it. This paper uses biometric information of user to enhance the security of Kumar and Om's scheme. Moreover, we carry out rigorous security analysis (informal as well as formal) in this paper to prove the security of the proposed scheme against all known attacks. We also simulate our scheme using automated tool, ProVerif, to prove its secrecy and authentication properties. A comparative study of the proposed scheme with the existing related schemes shows it effectiveness.

**Keywords:** Smartcard; Password; Security; Authentication; Multi-server; Biometric; ProVerif.

## 1 INTRODUCTION

Online applications and internet technologies are becoming popular day-by-day that has led to increase in number of service providing servers to handle various requirements of users. These servers provide services to authorized users through public channels. An attacker can monitor a public channel to intercept and/or modify the messages transmitted between a server and a user that may endanger the privacy and security of the system. So, some authentication mechanism is needed to make communication secure over a public channel. There have been numerous authentication schemes based on smartcard in literature. In the schemes [1-13], a user needs to register with each server for getting the services in a multiserver environment, requiring thus multiple smartcards and also various identities and passwords, which is quite frustrating. This issue has been addressed by incorporating a central authority, and one needs to register only with it to access the services in a multiserver system. A user can login to any server using only one smartcard along with one identity and password. Juang [14] presented an authentication scheme for multiserver domain that did not store the user's password in a password verification table. However, Chang and Lee [15] reported that the scheme presented by Juang was less efficient due to using the public key cryptography and they overcame this problem in their scheme. Chang and Kuo [16] discussed a scheme that included the access control features while retaining all features