# A Novel Verification Protocol to Restrict Unconstitutional Access of Information From Smart Card

Ajay Kumar Sahu, Raj Kumar Goel Institute of Technology and Management, India
Ashish Kumar, ITS Engineering College, India

## ABSTRACT

The services of the internet play an essential part in the daily life of the users. So, safety and confidentiality of the information are to be maintained to preserve user conviction in various services offered by network. The two-factor-based password verification techniques are used between remote server and legitimate users for verification over insecure channel. Several protocols have been suggested previously claiming their simplicity, privacy, safety, and robustness. The authors proved that their enhanced protocols are vulnerable to different attacks on the network and permit only authenticated users to update their password preserving traceability and identity. Analysis shows that no scheme has fulfilled all the security requirements and achieved entire goals. Therefore, in this article, a scheme has been presented to overcome these issues in the previous schemes to resist illegal access leading to misuse and achieve all the security requirements and goals. The safety analysis of the presented scheme has confirmed its performance in terms of reliability and safety.

## KEYWORDS

Hash Function, Identity, Information Retrieval, Key Agreement, Mutual Authentication, Password, Security, Smart Card

## INTRODUCTION

As time grows day by day, dependency of user in various technology increases which constituted a challenge regarding validity of the remote user. There are various types of attacks possible in the network which causes significant financial loss. Therefore, there is a requirement of some techniques to validate the legitimate users to an unsafe media such as Internet. The most commonly used technique is two factor based password verification. This protocol is susceptible to numerous attacks caused by human intellectual capacity of scheming and memorizing typical passwords.

Chip card based technique can be efficiently implemented in various password-based verification protocols (Lamport, 1991), (Gamal, 1985), (Kocher & Jaffe, 1999), (Messerges, Dabbish, & Sloan, 2002), (Chang C. C & Wu T. C, 1993), (Hwang M. S & Lee, 2000), (Kumar & Gupta, 2011), (Xiong & Niu, 2014) and (Kumari & Khan, 2013) easily. These have several applications like financial

DOI: 10.4018/IJDCF.2021010104

transactions, identity approval and accessing of remote services. To improve their feasibility, cards are confined in to limited size and cost. Various protocols has been reported (Tang, Hwang, & Lee, 2002), (Chang & Chang, 2005) and (Srivastva & Sharma, 2012) in which user may update password without interacting with the server, however user's identity must be same in every login attempt. Moreover, the schemes based on variable identity (Das, Saxena, & Gulati, 2004), (Wang, Liu, Xiao, & Dan, 2009), (Chang and Chang, 2009), (Madhusudhan & Mittal, 2012), (Chang, Tai & Chang, 2013), (Khan et al., 2014), (Devgan & Awasthi, 2016), (Chaudhary et al., 2015), (Wang et al., 2015), (Kharu et al., 2018), (Lu et al., 2016) and (Jung, Lee & Kim, 2016) are less prone to attacks and promising.

Literature review of the various schemes shows that till date most of the presented schemes are unsafe to different attacks like pose attack, online password guessing attack, chip card misplaced attack, repetition attack and man in middle attack. Many of the above schemes need a lot of storage cost and computational cost which decreases the performance of the scheme. Various schemes are fail to achieve all the security parameters and goals; therefore a need arises to develop a protocol that fulfils the entire above criterion. Therefore, in this paper, the authors proposed a scheme as A Novel Verification Protocol to Restrict Unconstitutional Access of Information from Smart Card.

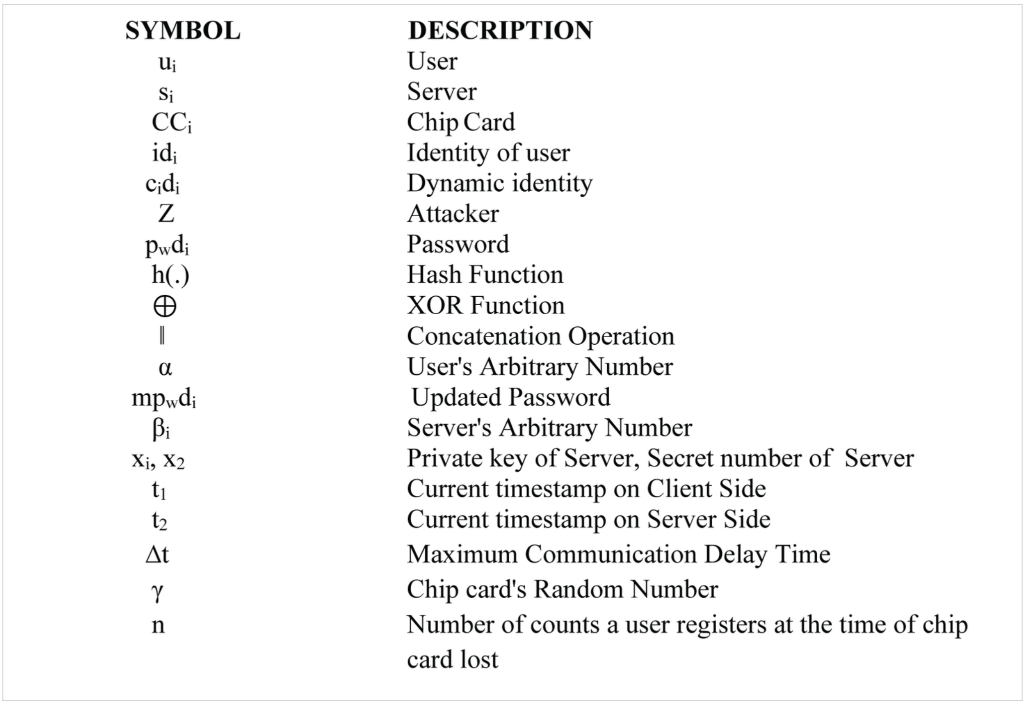
## NOTATIONS AND DESCRIPTION

The following symbols/notations are preferred in this paper as described in Table 1.

### Scheme Design

Initially, user enters his personal information to the terminal and sends towards the server for registration. Then user obtains chip card delivered by the server with security parameters. The

**Table 1. Symbols/Notations**



| SYMBOL | DESCRIPTION |
|---|---|
| $u_i$ | User |
| $s_i$ | Server |
| $CC_i$ | Chip Card |
| $id_i$ | Identity of user |
| $c_id_i$ | Dynamic identity |
| Z | Attacker |
| $p_wd_i$ | Password |
| h(.) | Hash Function |
| $\oplus$ | XOR Function |
| $\|$ | Concatenation Operation |
| $\alpha$ | User's Arbitrary Number |
| $mp_wd_i$ | Updated Password |
| $\beta_i$ | Server's Arbitrary Number |
| $x_i$, $x_2$ | Private key of Server, Secret number of Server |
| $t_1$ | Current timestamp on Client Side |
| $t_2$ | Current timestamp on Server Side |
| $\Delta t$ | Maximum Communication Delay Time |
| $\gamma$ | Chip card's Random Number |
| n | Number of counts a user registers at the time of chip card lost |