ABSTRACT

The use of smart cards began in the 1980s and since then the use of its technology was increasing. However, there are problems with smart card security such as smart card forging, smart card user impersonating, user's identity theft, and the use of smart card extracted data for breaking the scheme, etc. To overcome the problem of smart cards, dynamic identity based authentication scheme is introduced.

Lee et al [6] claims their proposed scheme was secured against user impersonation attack and server spoong. However, Li et al [7] claims that Lee's scheme still has vulnerabilities against some attacks such as improper authentication, forgery attack and server spoofing attack. Li et al [7] propose an improvement to overcome Lee's scheme vulnerability and claims that his scheme is secured against replay attack, forgery attack, server spoofing & registration center spoofing attack, and stolen smart card attack. Wang et al [9] claims that Li's scheme is vulnerable against offline password guessing attack, denial of service attack. Wang proposes a new scheme which is secured against offline password guessing attack, stolen verifier attack, user impersonation attack, server masquerading attack, replay attack, parallel session attack, and denial of service attack. However, Zhai et al [11] claims that Wang's scheme still has vulnerability to offline password guessing attack.

This research proposes a new scheme to strengthen Wang's scheme against offline password guessing attack. The proposed scheme uses a random number u for securing the user's password and a timestamp for creating the dynamic value of user's identity. The proposed scheme has been proven that it is stronger than Wang's scheme against offline password guessing attack. The probability of success in guessing the user's password drops twice of Wan's scheme. The proposed scheme also has been proven as strong as Wang's scheme against user impersonation attack.

Keywords: dynamic identity based authentication; offline password guessing attack.