Abstract

Remote User authentication protocol is used for verifying the legitimacy of a remote user over insecure network environments. Recently, many secure ID based remote user authentication scheme using smart card have been proposed in the literature. In 2012, Ratan-Sanjay [1] proposed secure ID based remote user authentication scheme using smart card and claimed that their scheme can avoid all types of security flaws and feasible in terms of computation and storage cost. But we have pointed out that their scheme is insecure against user impersonation attack, server masquerading attack, off-line password guessing attack, off-line identity guessing attack, session key recovery attack and smart card stolen attack. So, their scheme can not be used for practical implementation in terms of security. Further, their scheme takes more computation and communication cost than the proposed scheme. To overcome these weakness, we have proposed an efficient secure ID based remote user authentication scheme using smart card based on cryptographic one way hash function. The proposed scheme resists all possible attacks and provides better computation and communication cost than Ratan-Sanjay’s [1] scheme published earlier.

References

Cryptanalysis and an Efficient Secure ID-based Remote User Authentication using Smart Card

Cryptanalysis and an Efficient Secure ID-based Remote User Authentication using Smart Card

Index Terms

Computer Science

Security

Keywords

Attack  Authentication  Password  Secure ID  Smart Card