Abstract

Use of smart card makes remote user verification and key agreement easy, elastic to making a secure scattered system environment. It is very important to provide user privacy protection in authentication phase. In this paper, we are describing the performance comparison of Juang approach for multiple server authentication and key agreement schemes with user protection in network security with our proposed approach. First we are describing the juang approach then overview of our approach with comparison. All the areas those can be improved by us are also defined. Our approach is works for single server as well as multi sever environment. According to our analysis the juang approach is open to the element, leak-of-verifier attack and session key discovery attack and smart card loss attack. We are saving data into the server table in form of digital identity, smart card is removed by us, and so the new approach is safe from smart card loss attack.

Index Terms

Computer Science

Information Sciences

Keywords

User verification, session key, comparison, key size, smart card, network security