Abstract

In real time applications, more number of servers and data centers are needed for fast processing in the required time and to provide high level of security in communication due to rapid growth of data. Password Authenticated Key Exchange (PAKE) protocol is used to verify the authentication of the communicating parties and then secret key is generated based on their passwords. Mostly in single server environment the users share a password with a trusted
single server. If the single server is compromised, then the environment is prone to many attacks such as online dictionary attacks, server spoofing attack and stolen verification attacks. The proposed system is built based on ElGamal encryption scheme and Diffie-Hellman Key Exchange algorithm in the two-server password based authentication and key exchange protocol. Discrete logarithm in \( f^*p \) is used in ElGamal encryption to provide additional security. Discrete logarithm problem would render the ElGamal cryptosystem, secure against the man in the middle attack and other cryptographic attacks. The proposed scheme is provided with additional security and also its resistance against attacks.

References

- Bhavana A, Alekhya V, Deepak K, and Sreenivas V, "Password Authentication"

Index Terms

Computer Science
Security

Keywords
Password Authenticated Key Exchange  Two-server  Diffie-hellman Key Exchange.