Chapter 6

CONCLUSION AND FUTURE SCOPE
Chapter 6
CONCLUSION AND FUTURE SCOPE

Enhancing Kerberos system where authentication is based on combined ‘asymmetric’ and ‘symmetric’ key cryptography, and authorization is based on the ‘context-aware access control mechanism’ has been achieved.

We have designed and successfully implemented an innovative function of using the device key in the authentication phase and eliminated dependency on the user password completely. Authentication requests use symmetric encryption based on a device key, and the response is based on public key cryptography, which shortens the message size and reduces computational overheads compared to PKINIT. We could complete the implementation with all design aspects and a given comparative analysis between PKLK, PKINIT, and Kerberos, which proves that the PKLK has lesser communication overheads and needs fewer computations as compared to PKINIT. We have simulated context based authorization and enhanced Kerberos functionality to accept context-aware data in the authorization phase and have performed a dynamic validation on the KDC server.

To avail complete benefits, organizations would need to take some burden on cost to produce customized GPS devices where a device key can be safely stored and this device can encrypt information (context data and timestamp) as and when required for authentication and authorization. The organization also needs to invest on servers or vendors to maintain public key
infrastructures, maintain a LDAP database, and a dynamic context database. Organizations also need to invest in training people to put right processes and control operational risk to ensure that KDC’s authentication infrastructure is not compromised.

The system can be further improved by working on three major components individually. On client component a secure A-GPS service can be built that can run on Android based smartphones. Server Module can be enhanced so as to trace location across a login session and the Application Server can be enhanced to create or modify FTP and HTTP software, which can read SGT and the user session key and the encrypted GPS parameters for the third phase of Kerberos. Group Authentication can be supported in Kerberos to minimize the load on the system.