Provably secure dynamic id based anonymous two factor authenticated key exchange protocol with extended security

Abstract:

Authenticated Key Exchange (AKE) protocol allows a user and a server to authenticate each other and generate a session key for the subsequent communications. With the rapid development of low-power and highly efficient networks like pervasive and mobile computing network in recent years, many efficient AKE protocols have been proposed to achieve user privacy and authentication in the communications.

Existing system:

With the rapid development of low-power and highly efficient networks, mobile users can pay bills, buy goods online, and carry out electronic transactions by subscribing to various remote services. Though mobile computing devices are highly portable, they are usually unprotected and easy to be stolen or get lost. Unless precautions are taken, an unauthorized person may gain access to the information stored on them. The lack of authentication and privacy may cause even more severe results like personal data loss, disclosure of non-public data, or charge of abused usage against the device owner.

Disadvantages:

1. Data security is not provided and there is a chance for data attacks.
2. Performance efficiency has to be improved.

Proposed system:

In this paper, we proposed an Anonymous Two-Factor AKE scheme which preserves security against various attacks including de-synchronization attack, lost-smart-card attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or intractability, adaptively password change, no centralized password storage, and no long-term public key. Furthermore, our protocol maintain high efficiency in terms of storage requirement, communication cost as well as computational complexity Additional, the proposed scheme is provably secure in our extended security model of AKE. Therefore, the proposed scheme is suitable for deployment in various low-power networks, in particular, the pervasive and mobile computing networks.

Advantages:

1. Provides security in terms of data guessing attacks.
2. Imporves efficiency in terms of storage requirement and communication cost.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –III
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.

- Database : MySQL 5.0
- Database Connectivity : JDBC