© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Network security enhancement using OTP implementation with J-Pake: A Review

[1]Payal Rani, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor, Deptt. Of CSA ,CDLU ,Sirsa

Abstract: Battle between ethical or white hat Security hackers and malicious or black hat Security hackers is a long war, which has no end. While ethical Security hacker help to understand companies' their System security needs, malicious Security hackers intrudes illegally and harm network for their personal benefits. objective Enhancement of Password Authentication system is to prevent Security hacker's Attack make remote servers more secure.It is necessary to keep password safe and secure. There may be a chance to hack password by outside onlookers to access data provided by user. So, it is necessary to follow techniques to preserve password from onlookers to hack it. Several techniques are used here for password authentication. Public Key Info systems is one of technique used under public key infrastructure in which public keys are used to create to avoid password hacking. Limitation of this system is that user has to check validity of key each and every time in password system. It consumes more time for execution. Then, another system called Password only protocols or Password Authenticated Key Exchange or PAKE which does use public key system for password authentication. So, it is easy for users to use this system for real world applications.

1. Introduction to Cloud Computing

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new innovative, technical and pricing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology.

Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security concerns. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users and providers.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security.