



Network security enhancement using OTP implementation with J-Pake: An Implementation

¹Payal Rani, Research Scholar, Department of CSA, CDLU Sirsa

²Monika Bansal, Assistant Professor, Deptt. Of CSA ,CDLU ,Sirsa

ABSTRACT: 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 canter sites 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.



© IJRPS International Journal for Research Publication & Seminar

[1] INTRODUCTION

NETWORK SECURITY THREATS

Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant with in order to attack from full range of threat agents, from hackers to nation-states. system must be capable to restrict damage & recovery from occurrence of attacks.

TYPES OF ATTACK

Five types of attacks are as follow:

1. **Passive Attack**
2. **Active Attack**
3. **Distributed Attack**
4. **Insider Attack**
5. **Close in Attack**

Passive Attack

A **passive attack** generally checks data which has been not converted traffic & would checks for sensitive information & clear-text passwords which could be used with in different types of attacks.

Active Attack

In **active attack** attacker generally attempts to crack or breakdown into secured systems. This could be performed through worms/viruses/stealth/Trojan horses.

Distributed Attack

A **distributed attack** would require opposition introduced code, such as back-door program or Trojan horse attacks, to trusted component or software which are later be distributed to several other client companies & users.

Insider Attack

An **insider attack** includes somebody from inside, such as discontented operative, attacking on network that generate Insider harmful attacks may be spiteful or not spiteful. Malicious insiders intentionally steal, eavesdrop or damage confidential or valuable data;

Note :For Complete paper/article
please contact us info@jrps.in

Please don't forget to mention reference number ,
volume number, issue number, name of the
authors and title of the paper