**HoneyCloud A Honeypot Network Approach for Enhanced Security to the Cloud**

**ABSTARCT**

Abstract- With the rapid increase in the number of users, there is a rise in issues related to hardware failure, web hosting, space and memory allocation of data, which is directly or indirectly leading to the loss of data. With the objective of providing services that are reliable, fast and low in cost, we turn to cloud-computing practices. With a tremendous development in this technology, there is ever increasing chance of its security being compromised by malicious users. A way to divert malicious traffic away from systems is by using Honeypot. It is a colossal strategy that has shown signs of improvement in security of systems. Keeping in mind the various legal issues one may face while deploying Honeypot on third-party cloud vendor servers, the concept of Honeypot is implemented in a file-sharing application which is deployed on cloud server. This paper discusses the detection attacks in a cloud-based environment as well as the use of Honeypot for its security, thereby proposing a new technique to do the same.

**EXISTING SYSTEM**

Cloud computing is a technique to store, share and access data anytime and anywhere with a device that is connected to a network, preferably the internet. Cloud computing consists of an expandable storage space with no physical storage space which is accessible from anywhere in the world using any device, by connecting it to the internet. It contains large number of computing devices connected through a real-time communication (the internet) and has a common data storage area. The term “the cloud” is used as a metaphor for the Internet, based on the fact that a cloud like shape was used to indicate network telephone schematics, and later the Internet as an abstraction of underlying infrastructure it represents.

**Disadvantage**

1. Less Security
2. Unable manage traffic

**PROPOSED SYSTEM:**

In this project we are developing Honeypot server to detect and prevent attacks. Honeypot is an additional server which sit between user and cloud server and whenever any user send request then Honeypot will intercept that request and authenticate user and his request and if user authenticated then it allow user to access cloud server and if user is not authenticated and send request with fake password then Honeypot will monitor all his activity and serve him fake responses and the attacker with think he successfully attack server and keep sending malicious activities and Honeypot will record all his activity and later admin will block such IP address or instruct server from serving such IP Address.

In propose work designing Honeypot server which accept user request to upload, download and share file. While sharing file users will gave sharing permission and password to genuine users and then shared users can give password to download file. If any malicious user try to download file with fake password then Honeypot server will serve him blank page.

In propose paper if we serve blank page to attacker then he will easily understand that Honeypot serving him empty response then he will stop doing further activity and Honeypot cannot extract more information him and to avoid this problem in extension work instead of serving empty response Honeypot serve fake file which assure attacker that server has successfully hijack and he continue sending malicious activity which help Honeypot extract more information from him.

**Advantage**

1. Provide more security to the data
2. Handle traffic efficiently

**SYSTEM REQUIREMENT:**

**HARDWARE REQUIREMENTS:**

* **Processor - Intel i3(min)**
* Speed - 1.1 GHz
* RAM - 4GB (min)
* Hard Disk - 500 GB

**SOFTWARE REQUIREMENTS:**

* Operating System - Windows10(min)
* Programming Language - Python(3.7.0)