**Cloud Cyber Attacks against Social Networks**

**ABSTRACT :**

The clients cannot depend on cloud’s security infrastructure in public cloud computing environments. They may need to monitor and protect their virtual existence by implementing their own intrusion detection capabilities along with other security technologies within the cloud fabric. Cloud Cyber Attacks against Social Networks targets security of the infrastructure level for a public cloud by providing Cloud Cyber Attacks against Social Networks targets security that is highly elastic, portable and fully controlled by the cloud consumer.

**Existing System :**

Now a days network security measurements face new challenges in the cloud that is virtual machine intrusion attacks and malicious user activities, so we have need for increasing the user level trust’s in clouds. Currently, cloud providers enforce data encryption for the storage containers, virtual firewalls and access control lists. However, cloud consumers need to develop secure and customizable solutions to comply with their application requirements. The current security mechanisms from the cloud providers are not intended to enforce this level of constraints so additional measurements are required.

**Proposed System:**

we propose the Detection of Intruder System against Social Networks, which is a network and signature based IDS for the cloud model. In particular, Cloud Cyber Attacks against Social Networks is an on-demand, portable, controllable by the cloud consumer and available through the pay-per-use cost model. Cloud Cyber Attacks against Social Networks mainly targeting the IaaS level of the cloud. However, other levels of the cloud can be monitored such as the SaaS level. The major contribution for this work is a scalable and customizable cloud-based service that provides cloud consumers with IDS capabilities regardless of the cloud model. Cloud Cyber Attacks against Social Networks administrators have the abilities to monitor and react to attacks on multiple VMs residing within a consumer’s Virtual Private Cloud (VPC), and to identify specific attacking scenarios based on their application needs. Moreover, the system can adapt its performance to the traffic load by activating the on-demand elasticity feature. For example, the number of the available IDS Core components can change based on the amount of traffic targeting the protected business application.

**Advantages:**

Cloud Cyber Attacks detection components can be scaled to protect virtual machines residing in different cloud regions. These features are designed with the consideration of the cloud environment.

**IMPLEMENTATION :**

**Main Modules :**

1. User Module **:**

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

1. Intruder detections in the cloud :

Cloud Cyber Attacks against Social Networks, which is assists cloud consumers with securing their virtual machines by deploying an intrusion detection system in public clouds. It protects them against attacks initiated from any external source over the internet in addition to those originating from inside the cloud. Here, cloud consumers implement the applications they want to protect in the form of Virtual Machine Instances within a secure virtual network. Concurrently, cloud cyber attacks components can be placed in the same to guard these valuable assets.

1. The Cyber attack Alert System :

This also helpful for detecting the intruder detection.The Alert Management component is used as a GUI tool to view the generated alerts and correlate them. It allows the security administrator to extract events and relate them to predefined attacking situations.

1. Information change :

The information change for at the logout time so if any hackers stolen your username and password definitely he want to knowing last time of given subject changes this is very helpful for detecting the intruders.

# System Configuration :

# H/W System Configuration :

# Processor - Pentium –III

Speed - 1.1 Ghz

RAM - 256 MB(min)

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

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, Java, Jsp
* Scripts : JavaScript.
* Server side Script : Java Server Pages.
* Database : Mysql 5.0
* Database Connectivity : JDBC.