Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing

ABSTRACT

A virtualized infrastructure consists of virtual machines (VMs) that rely upon the software-defined multi-instance resources of the hosting hardware. The virtual machine monitor, also called hypervisor, sustains, regulates and manages the software-defined multi-instance architecture. The ability to pool different computing resources as well as enable on-demand resource scaling has led to the widespread deployment of virtualized infrastructures as an important provisioning to cloud computing services. This has made virtualized infrastructures become an attractive target for cyber attackers to launch attacks for illegal access.

EXISTING SYSTEM

Security approaches to protecting virtualized infrastructures generally include two types, namely malware detection and security analytics. Malware detection usually involves two steps, Monitoring hooks are placed at different points within the virtualized infrastructure, and then a regularly-updated attack signature database is used to determine attack presence. While this allows for a real time detection of attacks, the use of a dedicated signature database makes it vulnerable to zero-day attacks for which it has no attack signatures.

DRAWBACKS

- Cannot detect advanced attacks in virtualized infrastructures.
- Security analytics removes the need for signature database by using event correlation to detect previously undiscovered attacks, this is often not carried out in real-time and current implementations are intrinsically non scalable.

PROPOSED SYSTEM

In this paper we use a novel big data based security analytics (BDSA) approach to protecting virtualized infrastructures against advanced attacks. By making use of the network logs as well as the user application logs collected from the guest VMs which are stored in a Hadoop Distributed File System (HDFS), our BDSA approach first extracts attack features through graph-based event correlation, a Map Reduce parser based identification of potential attack paths and then ascertains attack presence through two-step machine learning, namely logistic regression and belief propagation.

ADVANTAGES

- In Proposed work we are using BDSA approach to protecting virtualized infrastructures against advanced attacks.
- Extraction of attack features is performed through graph-based event correlation and Map Reduce parser based identification of potential attack paths.

SYSTEM REQUIREMENTS

- **H/W System Configuration:-**

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

- **S/W System Configuration:-**

- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X

- Backend coding : Java
- Tool : Virtual Box
- Environment : Ubuntu
- Technology : Hadoop