ABSTRACT

Now-a-days, in this world cyber-attacks are becoming more and more and no limit for it. There is also another emerging topic in this world i.e., Virtualized infrastructure in Cloud Computing for cyber attackers. To attack on Virtualized infrastructure in Cloud Computing used VENOM (Virtualized Environment Neglected Operations Manipulation), Heartbleed, Shellshock, and Distributed Denial of Service (DDoS). Virtualized infrastructure consists of virtual machines (VMs) that rely upon the software defined multi-instance resources of the hosting hardware. To detect these advanced attacks, used many approaches in the literature i.e., malware detection, security analytics, etc. This study discussed about an novel approach called Big Data based Security Analytics (BDSA).

BDSA approach consists of three steps in that the first step is to collect the network logs and application logs from the guest Virtual Machine and stored in Hadoop Distributed File System (HDFS). Second step is to find the attack features through correlation regression and MapReduce Parser. Final step is to detect the attack by two types of Machine Learning methods those are logistic regression and belief propagation. This approach has an advantage of the distributed processing of HDFS and real-time ability of MapReduce model in Spark to address the velocity and volume challenges in security analytics. This process overcomes the cyber attacks on virtual machine's i.e., software code and data. The applications of this approach are Distributed Grep, Count of URL Access Frequency. Our BDSA approach incurs less performance over-head in attack detection through monitoring the guest VM's behaviour.

Keywords: Virtualized infrastructure, malware detection, security analytics, logistic regression, belief propagation.

ACKNOWLEDGEMENT

I am extremely thankful to our beloved Chairman and Founder **Dr. M. MohanBabu**, Padmasri awardee **and Prof. T. GopalaRao**, Special Officer of SreeVidyanikethan Educational Institutions who took keen interest and encouraged me in every effort throughout this B.Tech Program.

I owe my gratitude to **Dr. P. C. Krishnamachary**, Principal, Sree Vidyanikethan Engineering College for permitting me to use the facilities available to accomplish the Seminar course successfully.

I express my heartfelt thanks to **Dr. K. Ramani**, Professor and Head, Department of Information Technology, for her kind attention and valuable guidance to me throughout the Seminar course.

I am extremely thankful to our Seminar Supervisor **Dr. K. Khaja Baseer** Associate Professor of IT department who took keen interest and encouraged me in every effort throughout the Seminar course.

I am thankful to our Seminar Coordinator **Ms. V. Jyothsna,** Assistant Professor of IT for her valuable support and guidance throughout the Seminar course.

I am also thankful for all the teaching and non-teaching staff of Information Technology Department for their cooperation.

J Vineela Reddy
(14121A1231)

i

i