415/19/4/17

Name of scholar: Shuchi Sethi

Name of Supervisor : Dr Mansaf Alam

Department: Department of Computer Science,
Faculty of Natural Sciences, Jamia Millia Islamia,
New Delhi

Title: Cloud Security: Data Separation through Secure Virtual Partitioning in Multitenant Data Centers

Abstract

As the technological innovation and trend moves towards service based cloud environment, including for the management of sensitive information, it becomes imperative to adopt strong and adequate security measures. Meanwhile, attempts to build secure systems typically require abandoning goals of fast processing, ease of availability at low cost, since providers resort to multitenant architecture which gives rise to a new set of security issues. Certain attacks arise during different phases of data handling in cloud such as storage, processing and migration. Examples of such attacks include Covert channel attacks, Denial of service attacks etc. Covert channel attacks can be carried out at different stages using various resources and those are named based on the resource used for carrying out the attack while other category of attacks - like Denial of service - are usually carried out either by co-residing VMs(Virtual Machines), which is easily detectable or by using machines in cloud to form a Botnet. In the thesis, it is argued that multitenant systems can be made more secure by identifying attacks in the cloud architecture and enabling a mechanism for control and detection of such attacks. This premise is supported by a proposed framework for detection mechanism in the cloud, including detection of covert channel attack based anomaly which attributes its origin to multitenancy in cloud. Out of various approaches proposed in literature for mitigation and detection of covert channel attacks, only a few were

found suitable for cloud environment and certain techniques for detection which provide high accuracy are very expensive in terms of processing time and storage. Thus to achieve high accuracy proposed framework considers certain parameters which can be obtained with ease and can be used by forensics. After obtaining the features, signature builder is invoked that captures analysis of the distributions and some statistical features to obtain valid signature of the problem. Also it is found that use of context, which is missing in the literature, is introduced in the framework and accuracy improvement was seen in results. Machine learning algorithm is used to obtain pattern from the signature.

It is logical to ensure that the framework can also be processed in cloud by distributing the dataset in a balanced and efficient manner. Thus proposed framework is extended to enable processing on multiple virtual machines to preserve accuracy and allow scalability in processing. This approach offers advantages of low cost and fast processing for providing support to near real time applications requiring better security measures. To take it to a next level, the framework is then generalized to test for detection of Botnet, which is another serious threat that gains momentum when multiple machines are available for use, based on additional parameters. Thus acquiring trust in cloud by providing security mechanisms at storage, analysis, processing and post processing level will enable current state of technology to achieve new heights. As encryption techniques and intrusion detection systems need support from targeted frameworks for specific issues, research in these areas will make the security systems robust and less vulnerable to attacks from external sources as well as exploitation from within.