**CS794-CS892 Final Year Project Synopsis**

|  |  |
| --- | --- |
| **Group Members** | Sagar Shaw (134), Manish Kumar Gupta (125) |
| **Project Mentor** | Prof. Sanjay Chakraborty |
| **Project Title** | Malware Detection In Cloud Architecture |

**Objective**

To develop a malware detection technique and implement it into cloud architecture.

**Scope**

To develop a malware detector technique that works on two phase to detect malicious files, and apply it into cloud architecture.

**Plan**

Cloud computing is becoming an increasingly popular paradigm due to new services and increased media attention. This increase in popularity has lead to concern over the security of the cloud, especially from threats such as malware. Antivirus software is one of the most widely used tools for detecting and stopping malicious and unwanted files. However, the long term effect of traditional host based antivirus is questionable and fails to detect many modern threats. The first is that antivirus software fails to detect a significant percentage of malware in the wild. Moreover, there is a significant vulnerability window between when a threat first appears and when antivirus vendors generate a signature or modify their software to detect the threat. This means that end systems with the latest antivirus software and signatures can still be vulnerable for long periods of time. The second important trend is that the increasing complexity of antivirus software and services has indirectly resulted in vulnerabilities that can and are being exploited by malware. That is, malware is actually using vulnerabilities in antivirus software as means to infect systems.

Malware detection techniques are basically anomaly based and Signature based. Our aim is to develop a malware detector technique that works on two phase to detect malicious files. In First phase, we have a list of behaviour of a valid program and that checked with the programs. If match then it declare a valid program if not then it goes to the second phase. In Second phase, we observe the behaviour of the program when it execute. And determine whether it is a malicious program or not. This malware detector technique is deploy into cloud architecture with the help of cloud deployment models and free open source computer software Eucalyptus.

**References**

*Website: www.ijacsa.thesai.org*

*Topic: Malware Detection in Cloud Computing*

*Journal: International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014*