**Pattern Malware Detection in the Context of Cloud Computing**

Sagar Shaw (Roll no-134) Manish Kr. Gupta (Roll no-125)

Under the guidance of Prof. Sanjay Chakraborty

Department of Computer Science & Technology, Institute of Engineering & Management,

Salt Lake Electronic Complex, Kolkata-700091, India

**Synopsis: -** 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. Malware detection techniques are basically anomaly based and Signature based. In anomaly-based detection, the inverse of this knowledge comes from the learning phase. So theoretically, anomaly-based detection knows what is anomalous behavior based on its knowledge of what is normal. Since anomalous behavior subsumes malicious behavior, some sense of maliciousness is captured by anomaly based detection. If the malware detector employs a signature-based method, its knowledge of what is malicious comes from its repository, which is usually updated/maintained manually by people who were able to identify the malicious behavior and express it in a form amenable for the signature repository, and ultimately for a machine to read. The other input that the malware detector must take as input is the program under inspection. Once the malware detector has the knowledge of what is considered malicious behavior (normal behavior) and the program under inspection, it can employ its detection technique to decide if the program is malicious or benign. Although Intrusion Detection Systems (IDS) and malware detectors are sometimes used synonymously, a malware detector is usually only a component of complete IDS. 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 behavior 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 behavior of the program when it execute. And determine whether it is a malicious program or not.

Under Supervision of:

Prof. Sanjay Chakraborty.

Department of CSE, Institute of Engineering & Management