**Introduction**

JHoneypot, a Java-based network deception tool with a web-based monitoring interface and a rule-based intrusion detection engine. JHoneypot is based on the Honeyd program by Niels Provo’s, but features important enhancements. First, since JHoneypot is written in Java, it can potentially run on various platforms, windows or UNIX, workstations or handheld devices. Second, JHoneypot has a rule-based intrusion detection engine, whose design is guided by the analysis of real world attack data. The attack data was collected by opening up our J-Honeypot to solicit possible attacks. Third, JHoneypot includes a web based monitoring tool that is easily accessible and can help network administrators better understand network traffic and possible attacks.

A Honey-pot is a program, machine or system, which is used for network security. The basic idea is to deceive the attackers by making the honey-pot seem like a legitimate system. It traps attacks, records intrusion information about tools and activities of a hacking process, and prevents attacks outbound the compromised system. We propose a system, which is used for identifying the blackhats’in a network and recording their activities like when they break in and what are their motives. This is done by Data control, Data capture and Data Duplication mechanisms using a honey-pot developed in JAVA. We implement these mechanisms to control the intruders and capture their activities without them knowing that they are being under control. This helps in collecting the information about the attacks and the areas of attacks and to make the network security stronger.