Security of information is of utmost importance to any organization or individual, which depend on computer system or internet for business transaction or source of information or research. Many viruses are able to recognize certain anti-virus software, and respond differently to such software than to programs designed for other purposes. Some viruses go after the databases stored by anti-virus products. Some viruses simply go after anti-virus products, trying to erase them. Immune systems also face this daunting control challenge. On the one hand, there is need to minimize damage from pathogens, without wasting energy and resources, but on the other must avoid initiating or perpetuating autoimmune responses.

Several preventive measures including identification and authentication, logic access control, audit trails, digital signature and firewalls have been developed for the purpose of information security on system. As a result of inadequacies of these measures intrusion detection was introduced to complement these techniques and hence guarantee full protection of computing resources. Detection system is the process of identifying and detecting unauthorized access or
abnormal incursions, actions and events in the system, which provides information for timely counter measures.

This paper presents a systematic approach to intrusion detection using machine learning techniques to purging in order to avoid autoimmunity on network. Machine learning is an automatic process of extracting hidden or interesting knowledge from data in order to generate its own rule based on the given set of data. In this paper rough set theory will be used as a mathematical tool to deal with imprecise and insufficient knowledge, finding hidden patterns in data and reduce dataset [12]. Appraisal of the shortcomings of the current intrusion detection systems (IDS) will be pointed out and the international knowledge discovery and data mining tools (KDD99) are used for benchmarking intrusion detection used, with the designing of rough-set model.

References


Index Terms
Computer Science Security

Keywords
Autoimmunity, Purging, Intrusion detection, Rough Set Theory