A storage area network (SAN) is a high-speed and widely used special-purpose network that interconnects different kinds of storage devices with associated data servers on behalf of a larger network of users. SAN security is a specialized field dealing with issues related to the storage industry, it follows the same established principles found in all modern IT security. Therefore, it requires a continuous process of evaluating SAN environment's current state of security against the constant changes brought about by innovations in technology and an increase in awareness concerning security issues. This paper is all about intrusion detection in storage area network, and more important, how to detect and prevent suspicious activity of an unauthorized user by maintaining an audit record. This paper proposes an approach to detect an intrusion attack by clustering (k-mean) (to identify groups of similar behaved object, i.e. malicious and non-malicious activity), classification technique (to classify all data into particular class categories).
A Clustering based Intrusion Detection System for Storage Area Network

Index Terms

- Computer Science
- Network Security
Keywords
SAN observer  IDS manager  host agent module  SAN observer module  manager module