Abstract

Intrusion detection plays a vital role in maintaining the stability of any network. The major requirements for any intrusion detection system are speed, accuracy and less memory. Though various intrusion detection methods are available, they excel at some points while lack in the others. This paper presents a comprehensive survey of the technologies that are used for detecting intrusions. It analyzes the pros and cons of each technology and the literature works that utilizes these technologies. Challenges faced by the current IDS and the requirements for IDS in the current network scenario are discussed in detail. A detailed study on the datasets that can be used for effective building of an IDS is discussed. The research framework is proposed and a discussion of the various technologies that can be used for improving the efficiency of the IDS is provided.

References

- S. Sonawane, Sh. Pardeshi, G. Pradad, A Survey on Intrusion Detection Techniques (Department of Information Technology, Technocrats Institute of Technology, Bhopal, India, April 2012.)
- N. Jacob, C. Brodley, Offloading IDS Computation to the GPU (Computer Science Department, Tufts University, Medford, 2006).
- Tsang CH, Kwong S. Multi-agent intrusion detection system in industrial network using

Index Terms

Computer Science Networks
Keywords
Intrusion detection system; KDD CUP 99; SSENet; Evolutionary algorithms; Graph Database; Big Data