Abstract

With the growth of hacking and exploiting tools and invention of new ways of intrusion, Intrusion detection and prevention is becoming the major challenge in the world of network security. It is becoming more demanding due to increasing network traffic and data on Internet. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. So, the quest of betterment continues. Intrusion detection systems using data mining approaches make it possible to search patterns and rules in large amount of audit data. Classification-based data mining models for intrusion detection are often ineffective in dealing with dynamic changes in intrusion patterns and characteristics. Unsupervised learning methods are efficient in detecting unknown attacks in large datasets. In this paper we investigate clustering approaches for network intrusion detection. We carried out our experiments on K-means clustering algorithm and measured the performance based on detection rates and false positive rate with different cluster values. The KDD dataset which is freely available online is used for our experimentation and results are compared. Our intrusion detection system using clustering approach is able to detect different types of intrusions, while maintaining a low false positive rate.
Evaluation of K-Means Clustering for Effective Intrusion Detection and Prevention in Massive Network Traffic Data

- V. Kumar, Parallel and distributed computing for cybersecurity. IEEE Distributed Systems, 2005
Evaluation of K-Means Clustering for Effective Intrusion Detection and Prevention in Massive Network Traffic Data

281–297.
- T. Kohonen, Self-Organizing Map (Springer-Verlag, New York, 1997).
- M,Varapradsad Rao &quot;Algorithm for Clustering with Intrusion Detection Using Modified and Hashed K – Means Algorithms &quot;Published by IEEE Computer Society,2012
- Zhengjie Li&quot;Anomaly Intrusion Detection Method Based on K-Means Clustering Algorithm with Particle Swarm Optimization &quot;Springer Volume 4, Issue 2, April 2011.
- Asmaa Shaker Ashoor (Department computer science, Pune University) Prof. Sharad Gore (Head department statistic, Pune University), &quot;Importance of Intrusion Detection System (IDS)&quot;, International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518.
- Paul Barford University of Wisconsin, Nick Duffield AT&T, Amos Ron University and Joel Sommers Colgate, &quot;Network Performance Anomaly Detection and Localization&quot; Infocom 2009.

Index Terms

Computer Science

Security

Keywords

Network  Attacks  k-means Clustering  Security