Abstract

As the dependence of daily life is increasing on Internet technology, the attacks on the systems, servers are also rapidly increasing. The motives of attacks are to steal the confidential data from the systems or making the system unavailable to the authorised users. An effective approach is required to detect the intrusions to provide the defence to the Networks. First we applied the feature selection to reduce the dimensions of NSL-KDD data set. By feature reduction and machine learning approach we able to build Intrusion detection model to find attacks on system and improve the intrusion detection using the captured data. The intrusion detection accuracy of learning algorithms is also performed on the data set, without the level 21 attacks which is most easy to identify attacks, using learning algorithms and the success rate of proposed model is calculated over the attacks which are hard to detect.

References

- "Nsl-kdd data set for network-based intrusion detection systems. Available on:
Improving the Intrusion Detection using Discriminative Machine Learning Approach and Improve the Time Complexity by Data Mining Feature Selection Methods

- Jiawei Han and Micheline kamber: Data Mining Concepts and Techniques, Publisher Elsevier, 2001, pp. 67-69,296-301.
- Lior Rokach and Oded Maimon, "DECISION TREES", Department of Industrial Engineering, Tel-Aviv University, pp. 181

Index Terms

Computer Science

Artificial Intelligence
Keywords

Feature Selection  Weka  NSL-KDD data set  Accuracy  Intrusion detection  Machine learning