Abstract

Artificial intelligence is a technology to make the machines human compatible. Various techniques like- heuristic search (Generate and test, Hill climbing, BFS, DFS, Problem reduction, constraint satisfaction, means-ends analysis etc.), game playing, understanding, planning, NLP, Learning, commonsense, predictions and actions, and expert systems are there to make the system intelligent. This paper primarily focuses on the problem of malicious objects in the cyber space and discusses the usage of different AI techniques to overcome the mentioned problem. Every day the information stored in the computer and the information in transit faces threats due to malicious objects which further leads to a big loss. This paper discusses the possibilities to incorporate the AI techniques to analyze the data and finding and restricting the malicious objects. To make a proactive cyber defense system how the system log can be explored to find the malicious object and how the AI techniques like heuristic search can help in this process is discussed. This paper also discusses about the uncertainty of attacks and gives some views to implement AI techniques such as probability and Bayes' theorem, certainty factors and rule based system, Bayesian networks, fuzzy logic etc.

References
- Dinesh Kumar Saini &quot;Sense the Future&quot; Campus Volume 1- Issue 11, Page No14-17, February 2011.
- Jan-Erik Lane, The logic of means-end analysis , Quality and Quantity Springer Verilog, Volume 20, Number 4, Netherland, pp. 339-356, 1986.
- Dinesh Kumar Saini and Nirmal Gupta &quot;Fault Detection Effectiveness in GUI Components of Java Environment through Smoke Test&quot;., Journal of Information
Soft Computing Techniques in Cyber Defense

Technology, ISSN 0973-2896 Vol. 3, issue 3, 7-17 September 2007.
- Dinesh Kumar Saini "Testing Polymorphism in Object Oriented Systems for improving software Quality" ACM SIGSOFT Volume 34 Number 2 March 2009, ISSN: 0163-5948, USA
- Lakshmi Sunil Prakash, Dinesh Kumar Saini and Kutti N. S. "Integrating EduLearn Learning Content Management System (LCMS) with Cooperating Learning Object Repositories (LORs) in a Peer to Peer (P2P) architectural Framework" ACM SIGSOFT Volume 34 Number 3 May 2009, ISSN: 0163-5948, USA.
- Dinesh Kumar Saini, Jabar H. Yousif, and Wail M. Omar "Enhanced Inquiry Method for Malicious Object Identification" ACM SIGSOFT Volume 34 Number 3 May 2009, ISSN: 0163-5948, USA.
- J Zhu, Z Nie, JR Wen, B Zhang Proceedings of the 22nd 2d conditional random fields for web information extraction; extracted from microsoft. com, 2005dl. acm. org
Keywords
Cyber Security  Compartmentalization  Cyber hardening  Authentication  Access control
Confidentiality
Integrity