


Chapter 1

Applications of Computational Intelligence in Computing Security: A Review

Yousif Abdullatif Albastaki

 <https://orcid.org/0000-0002-6866-2268>
Ahlia University, Bahrain

ABSTRACT

This chapter is an introductory chapter that attempts to highlight the concept of computational intelligence and its application in the field of computing security; it starts with a brief description of the underlying principles of artificial intelligence and discusses the role of computational intelligence in overcoming conventional artificial intelligence limitations. The chapter then briefly introduces various tools or components of computational intelligence such as neural networks, evolutionary computing, swarm intelligence, artificial immune systems, and fuzzy systems. The application of each component in the field of computing security is highlighted.

INTRODUCTION

The aim of artificial intelligence (AI) is to simulate human intelligence on machines so that they can act and think like humans. AI is regarded as a wide field of knowledge that involves reasoning, machine learning, planning, intelligent search and building perception. Reasoning aims to reach a predetermined objective of a problem using a set of facts supplied and a predefined base of information or what we call a

DOI: 10.4018/978-1-7998-2418-3.ch001

knowledge base. The knowledge base consists of a compilation of IF-THEN rules or a conceptual graphic structure reflecting the knowledge of the professional in a specialized field. On the other hand, learning can be described as a process of encoding the situation-action pairs at memory so that the memory can remember the correct action. The learning process is carried out on machines either by training the machine with established situation-action pairs or by enabling the machine to adjust the parameters of the specified learning rule in a trial sense. Whereas preparation is about the sequence of steps to solve a problem. To be more precise, provided a knowledge base and a set of facts, preparation calls for the sequencing of the rule firing phase, so that there is at least one such target lading sequence.

Therefore, AI's main goals are to develop methods and systems for solving problems that are normally solved by human intellectual activity, such as image recognition, language and speech processing, preparation and forecasting, thereby enhancing computer information systems; and to develop models that simulate living organisms and, in general, the human brain, thereby improving our understanding. There is a large AI literature (Jain and Lazzerini, 199), (Jain, 1999) and (Mitchell, 1997) that covers various techniques of representation of information, reasoning (Shapiro, 2010) and (Rashmi & Neha, 2017)., machine learning (Shai & Shai, 2014) and (Yu-Wei, 2015), image and language understanding (Mishra, 2018) and (Rastgarpour & Shanbehzadeh, 2011), planning, smart search and realization of knowledge. A detailed discussion on these issues goes beyond this chapter's reach.

It is clearly reported by a number of researchers that AI was incompetent to meet the growing demand for search, optimization and machine learning in information systems with broad biological and commercial databases and factory automation for the steel, aerospace, energy and pharmaceutical industries claims Konar (2005). These pitfalls of traditional AI can be summarised as follows:

- Traditional problem-solving approaches in AI are primarily concerned with the representation of problem states by symbols and the construction of a set of rules to define transitions in problem states.
- In general AI is a tool with the capability to handle inductive and analogy-based learning, but is inefficient for supervised
- Traditionally, AI is utilized functionally in search algorithm, but conventional AI is not very qualified to deal with real world optimization problems.

The shortcoming of this classical AI has opened up new opportunities for non-classical models in different intelligent based applications. Such computational analytical tools and techniques have led to a new field called computational intelligence.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/applications-of-computational-intelligence-in-computing-security/250604

Related Content

Integration of Artificial Intelligence in the Modern Classroom: Prospects for Digitization in Education

Muhammad Mujtaba Asad, Shahzeen Younas, Sarfraz Ali, Prathamesh Padmakar Churiand Anand Nayyar (2023). *AI-Assisted Special Education for Students With Exceptional Needs* (pp. 110-136).

www.irma-international.org/chapter/integration-of-artificial-intelligence-in-the-modern-classroom/331736

A Neuro-Fuzzy Expert System Trained by Particle Swarm Optimization for Stock Price Prediction

Mohammad Hossein Fazel Zarandi, Milad Avazbeigiand Meysam Alizadeh (2012). *Cross-Disciplinary Applications of Artificial Intelligence and Pattern Recognition: Advancing Technologies* (pp. 633-650).

www.irma-international.org/chapter/neuro-fuzzy-expert-system-trained/62711

Local Brand Impact During COVID-19

Sai Sreeja Nainalaand Snehamayee Gowribidanur Matam (2023). *AI-Driven Intelligent Models for Business Excellence* (pp. 199-208).

www.irma-international.org/chapter/local-brand-impact-during-covid-19/315402

Secured Sharing of Data in Cloud via Dual Authentication, Dynamic Unidirectional PRE, and CPABE

Neha Agarwal, Ajay Rana, J.P. Pandeyand Amit Agarwal (2021). *Research Anthology on Artificial Intelligence Applications in Security* (pp. 504-527).

www.irma-international.org/chapter/secured-sharing-of-data-in-cloud-via-dual-authentication-dynamic-unidirectional-pre-and-cpabe/270614

Entropy-Based Feature Selection for Network Intrusion Detection Systems

Sellappan Devaraju, Srinivasan Ramakrishnan, Sundaram Jawahar, Dheresh Soniand Alagappan Somasundaram (2022). *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics* (pp. 201-225).

www.irma-international.org/chapter/entropy-based-feature-selection-for-network-intrusion-detection-systems/306867