Abstract

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol 19. S3

Artificial Intelligence & Big Data Analytics for Cyber Security Applications

Jemili Farah,
University of Sousse, Tunisia

Abstract

Artificial intelligence in cyber security increases efficiency and precision of the system to detect any potential threat in Manufacturing Systems. Manufactories expanding their horizon to different geographies are generating voluminous data to gain insights and are also using analysis techniques to enhance their product offerings. Global AI in cyber security market is predicted to grow at 35.0% CAGR during the forecast period with the market size reaching USD 31.2 billion by 2024 [2]. The market is driven by the factors such as increasing stringent data privacy regulations, increasing number of cyber-attacks, increasing adoption of digital solutions, and increasing inclination towards cloud-based solutions from on-premise. The continuous research and development for technologically advanced systems for anomaly detection, web filtering, intrusion detection, and data loss prevention among others. Further fuels the growth of the market. The market for AI in cyber security devices is primarily driven by increasing data frauds and cyber-attacks worldwide. The increasing use of connected technologies makes the smart manufacturing system vulnerable to cyber risks. This creates utmost need of certain systems and programs which can detect predict process and analyze such threats and keep manufactories safe from cyber-attacks. AI offers the solution to the threat to a great extent and therefore different industry players are focusing on utilizing AI for cyber security, thereby fueling the growth of the global market. Security is a broad term, and in industry there are a myriad of "security" contexts on a variety of levels wide. Artificial intelligence and machine learning technologies are being applied and developed across this spectrum. Artificial intelligence and security were – in many ways – made for each other, and the modern approaches of machine learning seem to be arriving just in time to fill in the gaps of previous rule-based data security systems. The purpose of this article is to introduce Industrial Artificial Intelligence, shed light on current trends and applications, in industry, at the intersection of artificial intelligence and the security field. In addition to a spotlight on current uses (real world examples), we also present our contribution and touch on up-and-coming applications. The potential future applications is meant to spark ideas about some of the directions in which AI technologies are headed, and also illuminate a handful of key obstacles and challenges that need to be reconciled before the technology can begin to reach its full potential.

Biography

Farah JEMILI received the Engineer degree in Computer Science in 2002 and the Ph.D degree in 2010. She is currently Assistant Professor at Higher Institute of Computer Science and Telecom of Hammam Sousse (ISITCOM), University of Sousse, Tunisia. She is a senior Researcher at MARS Laboratory (ISITCOM –Tunisia). Her research interests include Artificial Intelligence, Cyber Security, Big Data Analysis, Cloud Computing and Distributed Systems. She served as reviewer for many international conferences and journals. She has many publications; 6 book chapters, 5 journal publications and more than 15 conference papers.