

# Artificial Intelligence Based Systems for Secure, Sustainable and Sound Business

**Yachna Sharma**

Georgia Tech Scheller School of Business, Atlanta, Georgia

## Abstract

Last decade witnessed tremendous growth and adoption of artificial intelligence (AI) systems by the industry in various domains. Many businesses are still trying to transition and take advantage of the technology. Most of the emphasis has been on developing sophisticated algorithms, massive data collection and curation to train complex deep neural nets that provide near human performance in several domains such as computer vision and natural language processing. Despite this tremendous success, ML/AI algorithms are frequently criticized for not being fair and explainable. Moreover, the current global business landscape, target customer segments, socioeconomic, geopolitical and industry trends also affect how ML/AI based products need to be designed, secured, sustained and evolved so they continue to provide the maximum benefit to the target customers. Since organizations spend tons of money on developing the complex algorithms, churning lot of data to eventually arrive to an unexplainable predictive black box, a holistic customer and business centric approach to ML/AI products is required. This is especially important in the era of cyber warfare as security of ML/AI systems is more important than ever before for autonomous systems that make or assist humans on critical decisions. Even if those decisions are eventually reviewed by humans, their perturbation could trigger either a misguided response from a human or a chain of verifications from multiple humans. Finally, there might be a limit on how much one can achieve from AI and it is important to assess the business sustainability and operational balance on human versus machine efforts. Even though we can't fully explain the decision making of AI systems with existing technologies, we can certainly provide risk assessments on the operational spectrum from fully human to fully automated under different scenarios. Besides risk, we may also want to establish fairness/bias benchmarks on known data diversities and best effort design strategies to operate in new global environments with yet undiscovered or unaccounted bias sources. This talk presents a customer centric strategic approach to discovery, design and deployment of ML/AI based products. The 7E approach comprises of: Existence ☐ Expression ☐ Execution ☐ Empowerment ☐ Entrepreneurship ☐ Envision ☐ Evolution. The approach is examined with reference to ML/AI based solutions with some concepts and ideas derived from Natural sustainable systems.

## Biography

Yachna Sharma completed her PhD in 2014 with research in computer vision and machine learning. She is a business and research professional with over 15 years of diverse domain experiences in satellite and wireless communications, artificial intelligence, machine learning, data science and process optimization. She specializes in

management of technology in disruptive technical domains. Her current focus is on business strategy and research on emergent technologies to design, innovate and deliver secure, verified and minimally biased ML/AI systems in highly regulated environments. Her works are frequently inspired by her academic background in biodiversity and Natural forest ecosystems.