Chapter 9
The Role of Artificial Intelligence in Cyber Security

Kirti Raj Bhatele
RJIT, India

Harsh Shrivastava
RJIT, India

Neha Kumari
RJIT, India

ABSTRACT

Cyber security has become a major concern in the digital era. Data breaches, ID theft, cracking the captcha, and other such stories abound, affecting millions of individuals as well as organizations. The challenges have always been endless in inventing right controls and procedures and implementing them with acute perfection for tackling with cyber attacks and crimes. The ever-increasing risk of cyber attacks and crimes grew exponentially with recent advancements in artificial intelligence. It has been applied in almost every field of sciences and engineering. From healthcare to robotics, AI has created a revolution. This ball of fire couldn't be kept away from cyber criminals, and thus, the "usual" cyber attacks have now become "intelligent" cyber attacks. In this chapter, the authors discuss specific techniques in artificial intelligence that are promising. They cover the applications of those techniques in cyber security. They end the discussion talking about the future scope of artificial intelligence and cyber security.

DOI: 10.4018/978-1-5225-8241-0.ch009

INTRODUCTION

Is artificial intelligence less than our intelligence. (Jonze, S., 2017)

"Intelligence" is only the property that distinguishes human from anything else on this planet. The idea of having that Intelligence in man-made machines is quite fascinating although the machines can't have that inherited intelligence. Instead of natural human intelligence, the scientific, philosophical and other communities working for understanding human mind started pondering over this "Why can't machines think?" As a result of multidisciplinary efforts in areas of cognitive science, neuroscience and computer science, this idea of creating "Artificial Intelligence" began to attract the attention of researchers around the world. Around the 1960s and 70s, researchers started expecting very high from AI Research, but it was pretty much in vain without any breakthroughs.

We can define Artificial Intelligence as the scientific field that tries to understand and model human intelligence. Many Researchers have their own understanding of AI such as quoting Peter Norvig and Stuart Russel's Artificial Intelligence: A Modern Perspective "Artificial Intelligence is the study of agents that exist in the environment and perceive and act".

There has been an effort for decades to create such systems that can understand, think, learn, and behave like humans. We'll discuss some of the important approaches for AI that has pushed AI research further (Russell, S., J., & Norvig, P., 2000).

Historical Attempts

Warren McCulloch and Walter Pitts in 1943, for the first time, attempted to create an intelligent system. They proposed a model of the Artificial networked neural structure and claimed that if this structure would be defined properly, then it could learn like the human brain.

Recently after some year, Alan Turing published "Computer Machinery and Intelligence "in which he explored the idea of "Artificial Intelligence". In his work, he also proposed "Turing test" as a test to measure the machine's ability to exhibit intelligence. The setup for the test requires a natural language generating a machine, an evaluator (which is human) and a human. The evaluator will converse (interact) with the machine and the human and try to identify the machine based on the conversation. Both the machine and human will try to persuade evaluator that he or she is interacting with a human on the other side. If the evaluator fails to distinguish machine conversation from the human conversation, then the machine will be considered intelligent.