Chapter 5
Applications of Machine Learning in Cyber Security

Charu Virmani
Manav Rachna International Institute of Research and Studies, India

Tanu Choudhary
Manav Rachna International Institute of Research and Studies, India

Anuradha Pillai
J. C. Bose University of Science and Technology YMCA, India

Manisha Rani
D. N. College, India

ABSTRACT

With the exponential rise in technological awareness in the recent decades, technology has taken over our lives for good, but with the application of computer-aided technological systems in various domains of our day-to-day lives, the potential risks and threats have also come to the fore, aiming at the various security features that include confidentiality, integrity, authentication, authorization, and so on. Computer scientists the world over have tried to come up, time and again, with solutions to these impending problems. With time, attackers have played out complicated attacks on systems that are hard to comprehend and even harder to mitigate. The very fact that a huge amount of data is processed each second in organizations gave birth to the concept of Big Data, thereby making the systems more adept and intelligent in dealing with unprecedented attacks on a real-time basis. This chapter presents a study about applications of machine learning algorithms in cyber security.

INTRODUCTION

With the exponential rise in technological awareness in the recent decades, technology has taken over our lives for good but with the application of computer aided technological systems in various domains of our day to day lives, the potential risks and threats have also come to the fore aiming at the various security features that include confidentiality, integrity, authentication, authorization and so on. Computer

DOI: 10.4018/978-1-5225-9611-0.ch005

scientists, the world over have tried to come up, time and again with solutions to these impending problems. With time, attackers have played out complicated attacks on systems that are hard to comprehend and even harder to mitigate. Even upon recognition, responding in real time remained a problem. The capability of the system was hence extended using artificial intelligence and machine learning techniques. The very fact that a huge of data is processed each second in organizations gave birth to the concept of Big Data, thereby making the systems more and adept and intelligent in dealing with unprecedented attacks on a real time basis. Various authors having worked on the problem, devised a host of algorithms that may be used for purposes such as image processing, speech recognition, biomedical area, and of course cyber security domain.

The chapter primarily presents a survey about the role of machine learning when applied in the domain of cyber security. The chapter aims at introducing the reader to the basics of machine learning along with its various components and tasks associated with it. The chapter presents in detail a set of approaches to classify the various Machine Learning algorithms and goes on to recount the application of Machine Learning in our day-to-day lives. Having introduced the reader to the basics, a detailed description of the cyber security tasks in machine learning aided with examples are narrated in the later sections.

WHAT IS MACHINE LEARNING?

As the scientists focused more on solving the issues related with the computer systems including the security aspect, they drove themselves closer to a technology that acted like humans. This was the beginning of AI (Artificial Intelligence) applications that surpassed their detection as computer systems by users. Initially generated, AI applications aimed at clearing the Turing Test which is a test of a machine's ability to showcase intelligent behavior that is tantamount to or indiscernible from that of a human intelligence. But since AI was initiated with the very purpose of specific application domains such as face recognition, object recognition, it was soon realized that creating an AI that worked in terms of the human brain completely was an arduous task. Hence, the concept of Machine Learning was evolved.

Machine Learning is essentially an approach to Artificial intelligence that makes use of any system that is adept in learning like humans, i.e., from experience (Al-Jarrah et al., 2015; Buczak & Guven eta l, 2016). Just like a human brain, it aims at recognizing the patterns and upgrades itself to apply them in the future decisions. Thus, it defies the old traditions of feeding data into the systems through programming and learns by examples. The decisions in Machine Learning are driven by data rather than algorithms and also change its behavior, upon accommodating new information, that sets' it apart from the lot of technologies aiming to achieve cyber security (Michalski, 2013). Simply put, Machine Learning is a type of Artificial intelligence that allows the system to learn without being explicitly programmed wherein computer programs are developed in such a way that they change whenever exposed to new data (Cavelty, 2010).

The ultimate aim of Machine Learning techniques can be thought of as enabling software's to be able to make decisions much like humans do in cases of cyber attacks that have been previously encountered by the system and also those not encountered before. The breach of data in big organizations has incurred a huge loss, with the average cost being over $3 million. Since cyber crimes have become rhetoric in the current scenario, it is the most researched field today and the scientists have been struggling to devise techniques that could reduce the cost factor while dealing with the attacks.