Chapter 2
A Review on Cyber Security Mechanisms Using Machine and Deep Learning Algorithms

Thiyagarajan P.
Central University of Tamil Nadu, India

ABSTRACT

Digitalization is the buzz word today by which every walk of our life has been computerized, and it has made our life more sophisticated. On one side, we are enjoying the privilege of digitalization. On the other side, security of our information in the internet is the most concerning element. A variety of security mechanisms, namely cryptography, algorithms which provide access to protected information, and authentication including biometric and steganography, provide security to our information in the Internet. In spite of the above mechanisms, recently artificial intelligence (AI) also contributes towards strengthening information security by providing machine learning and deep learning-based security mechanisms. The artificial intelligence (AI) contribution to cyber security is important as it serves as a provoked reaction and a response to hackers' malicious actions. The purpose of this chapter is to survey recent papers which are contributing to information security by using machine learning and deep learning techniques.

INTRODUCTION

Today is the era of Internet where everything become digitalized including purchasing items in mall, bank transactions, ticket reservations, online shopping, top secrets in government organisation especially in military and defence. On one hand we are enjoying the privilege of digitalization which results on accumulating data in terabytes, but on the other hand the accumulated data need to be converted to information and the information need to be mined to get knowledge to enhance user experience in usage of Internet.

DOI: 10.4018/978-1-5225-9611-0.ch002

While the users are enjoying the advantage of Internet, the most concerning thing about Internet is the safety our data. The technique of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation is called Cyber Security.

The digital world is replacing the physical, the more realistic view is that the two worlds are coming together. Organizations are not really prepared to face the challenges which is the result of the amalgamation of digital and physical world. In the case of cybercrime, it states that it isn't displacing physical acts of crime, they are occurring in concert. Criminals who might once have used explosives to cripple critical infrastructure, such as transportation, power grids or water systems, for example, may be now able to achieve their goals remotely by attacking the computers that operate those systems, incurring less risk in the process.

Cyber Security is broadly categorised into four major areas, they are:

1. Application Security
2. Information Security
3. Disaster Recovery
4. Network Security

Approach to Cyber Security

In the case of Cyber Security, securing the data is a very big challenge. The attacks are increasing at a very high speed and the tools which can break the security are becoming popular. Nowadays, it is possible even for the layman without any technical knowledge to use different types of tools to break the security.

In the current context, it is not only necessary for us to protect the data but also is highly necessary for us to protect whole information system. The unexpected and drastic increase of attackers makes the security of data in Internet a major concern. In addition to the various security mechanism available now artificial intelligence and machine learning also contributes in strengthening the Information Security.

Cyber Threats in US from 2010-2018 Statistics

Annual number of data breaches and exposed records in the United States from 2010 to 2018 (in millions) in shown in Figure.1.

Impact of Various Threats in Cyber World (Present and Future):

With a serious lack of digital security mechanisms and experts to battle progressively refined invaders combined with a developing reliance on innovation, the cybercrime pose a potential threat in forthcoming years in Internet. Here are a few of the numerous digital dangers anticipated to cause hurt in the year ahead.

Automated Cars with Connection: We are in the digital age of making driverless cars and vehicles. To optimize the performance and make the customers zone comfortable the driverless cars are associated with inbuilt sensors. This is done by embedding and integrating the devices by the smartphone. As the advancement of the technology, the security can be breached as it is connected with the sensors.

Insider support Attacks: Beyond hackers hoping to make a benefit through taking individual and corporate information, whole country states are presently utilizing their digital aptitudes to invade dif-