Chapter 10

Ensemble Learning Mechanisms for Threat Detection: A Survey

Rajakumar Arul
https://orcid.org/0000-0002-1385-7965
Amrita Vishwa Vidyapeetham, India

Rajalakshmi Shenbaga Moorthy
St. Joseph’s Institute of Technology, India

Ali Kashif Bashir
Manchester Metropolitan University, UK

ABSTRACT

Technology evolution in the network security space has been through many dramatic changes recently. Enhancements in the field of telecommunication systems invite fruitful security solutions to address various threats that arise due to the exponential growth in the number of users. It’s crucial for upgrading the entire infrastructure to safeguard the system from specific threats. So, there is a huge demand for the learning mechanism to realize the behavior of attacks. Recent upcoming technologies like machine learning and deep learning can support in the process of learning the behavior of all types of attacks irrespective of their deployment criteria. In this chapter, the analysis of various machine learning algorithms with respect to a few scenarios that can be adopted for the benefits of improving the security standard of the network. This chapter briefly discusses various known attacks and their classification and how machine learning algorithms can be involved to overcome the popular attacks. Also, various intrusion detection and prevention schemes were discussed in detail.

DOI: 10.4018/978-1-5225-8100-0.ch010
INTRODUCTION

The synonym of cyber is given as “through use of a computer” also called cyberspace. The term security refers to safe. These two words joined to form cyber security which means making cyberspace safe from threats. Over the past decade, the adventurous growth of technology imposes severe challenges on security. The technology keeps on growing in three dimensions viz. computation, storage, and connectivity. When the technology grows the threats associated with it also grows, i.e., the growth of technology is directly proportional to the threats possible. Thus Security is the prime concern for Information and Communication Technology (ICT). The various ICT devices such as smartphones, sensors, actuators, RFID devices are interdependent and communicate with one another, which increases network traffic, is subjected to various security attacks. The mechanism of giving protection to ICT Systems is termed to be cybersecurity. Cybersecurity is the act of i) securing a computer, and its associated hardware, software, and data stored in it ii) securing computer networks, its associated hardware, software and data transferred across it. Thus to provide cybersecurity it is essential to understand about attacks, and the mechanisms to secure against those attacks. A good security system must protect the following objectives: i) confidentiality, refers to unauthorized access of information ii) Integrity, refers to the unauthorized modification of information iii) Availability, refers to the denial of service of prevention of information from authorized access. The attacks in the networks are broadly classified into two categories: i) Passive Attack, which is silently listening communication ii) Active Attack which is modifying the data transferred across the network. Security is the process, and it is not an end state. Several mechanisms are used in day to day life to impose maximum security.

In this pervasive world, the technology changes our lifestyle, the way we did business, and the way we had communication with friends, relatives or neighbors. It was all made possible with one word “Internet.” When everyone is using the internet, a huge amount of data gets generated, transferred across networks and stored in the system. Thus the growth of Internet sophisticates people’s life and at the same time it paves the growth of Cyber criminals. Cybercriminals are those who steal one’s personal information stored on the computer. Even though there are security mechanisms, the criminals find a hole to come out of it. Thus there is always intense violence between cybercriminals and cyber security providers. The conventional security mechanisms always focus on protection from attack rather than detection of an attack. Traditionally network is protected using a firewall, and the computer system can be protected using antivirus software. Traditional threat protection mechanism depends on signature and a pattern. When a threat to the system ever seen before arises, will the tool able to protect the system is a miserable question?
The Belief Model of Sentience: Cognitive Dynamics of Mediated Conversations With God
www.igi-global.com/chapter/the-belief-model-of-sentience/229327?camid=4v1a