Chapter 6
Approaches for Detecting and Predicting Attacks Based on Deep and Reinforcement Learning to Improve Information Security

Nayana Hegde
https://orcid.org/0000-0001-7467-2553
REVA University, India

Sunilkumar S. Manvi
REVA University, India

ABSTRACT

The continued growth and widespread use of the internet benefit many network users in various ways. Meanwhile, network protection becomes increasingly essential as the internet becomes more widely used. Though, as the number of internet-connected systems in finance, e-commerce, and the military grows, they are becoming targets of network attacks, posing a noteworthy challenge and causing significant harm. Essentially, practical strategies for detecting and defending against attacks, as well as maintaining network protection, are needed. Furthermore, various types of attacks must typically be dealt with in different ways. This chapter summarizes some of the important deep learning techniques and reinforcement techniques for information security by providing various methods for attack detection and corrections.

INTRODUCTION

The ongoing growth and worldwide usage of the Internet satisfies numerous network users in a variety of methods. Meanwhile, as the Internet becomes more widely used, network protection becomes very important and challenging task. Network protection is concerned with computers, networks, applications

DOI: 10.4018/978-1-6684-6275-1.ch006

Copyright © 2023, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

and different data, among other things, with the aim of preventing unauthorized access and alteration as given in Mohamed Amine (2020). Originally, essential approaches for identifying and securing attacks, additionally sustaining network protection, are entailed. Additionally, different categories of attacks typically should be taken care with specific methods. The key problem in the area of information security need to be resolved is how to identify different types of network risks, especially those attacks that were not experienced earlier.

Due to diverse possessions regarding the technological breakthrough, threats to computer networks, IoT systems, and devices gets translated as increasing privacy issues. IoT systems were practical and efficient due to their characteristics such as: collecting a lot of data, connecting the physical and virtual worlds, complicated environments, architecture that is more centralized. Malicious hackers, though, might exploit vulnerabilities. An overview of the IoT attack surface areas can be found below:

- Device: Device might be the primary means of starting a cyber-attack. Memory, computing micro-programs, the hardware interfacing, the Internet application, and communications networks are illustrations of modules where vulnerability might well be found inside a device.
- Channels: Attacks may come through the media that connects different IoT devices together.
- Software applications: System may be harmed as a result of bugs in internet apps and Internet of things applications. Web apps can be used to steal user credentials or fraudulent system software updates, for example.

Numerous computer and network security research areas fall under the umbrella of cyber situational awareness or have some connection to it. However, an enterprise's capacity for cyber situational awareness is currently severely constrained for a number of reasons, including but not limited to:

- Incomplete and inaccurate forensics, intrusion detection, and vulnerability analysis.
- Unable to track certain microscopic systems or assault patterns.
- Restricted capacity for navigating ambiguity.

Challenges of Predicting Cyber-Attacks

Given the number of potential entry points, the attackers' goals, and the increasing reliance on connection and cloud storage, it is difficult to forecast cyber-attacks with current technology. Some of the challenges in predicting cyber-attacks are discussed as follows.

- Rising number of cyber-attacks: The frequency and severity of attacks are only going to increase as cyber threat actors hone their methods and make use of automation and machine learning.
- Active cyber pandemic: In order to enable the remote workforce and achieve the aims of the digital transformation, the development of remote work made users, computers, and personal devices the first line of defense, and the spike in cloud use generated new avenues of attack for cyber threat players.
- Mobile devices create more security threats: Cybercriminals changed their strategies to benefit on the rising use of mobile devices. There are several new mobile virus Trojan.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/approaches-for-detecting-and-predicting-attacks-based-on-deep-and-reinforcement-learning-to-improve-information-security/316017

Related Content

Network Survivability in Optical Networks with IP Prospective
Hongsik Choiand Seung S. Yang (2008). *Encyclopedia of Internet Technologies and Applications (pp. 346-352).*
www.irma-international.org/chapter/network-survivability-optical-networks-prospective/16874

A Comparative Analysis of Hierarchical Routing Protocols in Wireless Sensor Networks
Anar Abdel Hady, Sherine M. Abd El-kader, Hussein S. Eissa, Ashraf Salemand Hossam M.A. Fahmy (2012). *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications (pp. 212-246).*
www.irma-international.org/chapter/comparative-analysis-hierarchical-routing-protocols/63552

Important Factors on RIAs Development
(2015). *Frameworks, Methodologies, and Tools for Developing Rich Internet Applications (pp. 59-75).*
www.irma-international.org/chapter/important-factors-on-rias-development/117378

Thing Theory: Connecting Humans to Smart Healthcare
Sally A. Applinand Michael D. Fischer (2017). *Internet of Things and Advanced Application in Healthcare (pp. 249-265).*
www.irma-international.org/chapter/thing-theory/170243

Clustering in Wireless Sensor Networks: Context-Aware Approaches
Enamul Haqueand Norihiko Yoshida (2012). *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications (pp. 197-211).*
www.irma-international.org/chapter/clustering-wireless-sensor-networks/63551