Chapter 95
Deep Learning in Cybersecurity: Challenges and Approaches

Yadigar N. Imamverdiyev
https://orcid.org/0000-0002-3710-1046
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

Fargana J. Abdullayeva
https://orcid.org/0000-0003-2288-6255
Institute of Information Technology of Azerbaijan National Academy of Sciences, Baku, Azerbaijan

ABSTRACT

In this article, a review and summarization of the emerging scientific approaches of deep learning (DL) on cybersecurity are provided, a structured and comprehensive overview of the various cyberattack detection methods is conducted, existing cyberattack detection methods based on DL is categorized. Methods covering attacks to deep learning based on generative adversarial networks (GAN) are investigated. The datasets used for the evaluation of the efficiency proposed by researchers for cyberattack detection methods are discussed. The statistical analysis of papers published on cybersecurity with the application of DL over the years is conducted. Existing commercial cybersecurity solutions developed on deep learning are described.

INTRODUCTION

In recent years, the increase in the occurrence frequency of the network attacks has posed serious problems related to cybersecurity. The emergence of new smart network technologies requires the development of new methods in cybersecurity.

In protection of critical infrastructures from attacks and unauthorized access, cybersecurity seems very important. Cybersecurity includes many technologies and processes. Application security, information security, network security, disaster recovery, operational security, end-user education and so on are some categories of cybersecurity.

DOI: 10.4018/978-1-7998-7705-9.ch095

Cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century (Cyberspace Policy Review, 2009). The need to understand the motivations of cyberattackers is great.

Cyberattacks is a modern war without weapons yet most disastrous and pernicious leading to exposing sensitive personal and business information, disrupting critical operations, continuous vulnerabilities, unauthorized and illegal access to devices and software thereby imposing high costs on the country economy. Cybersecurity is a perennial problem for most of the reputed organizations such as banks, retail stores, critical infrastructures like SCADA, power grids, etc.

Cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. A cyberattack is employed by nation-states, individuals, groups, society or organizations. A cyberattack may originate from an anonymous source. A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system (Lin, 2016).

Although there is a sufficient number of currently available attack detection systems, the rapid increase in the number of attacks and the improvement of hacking skills make the development of new detection systems necessary. Although existing machine learning techniques have been successful in recent decades, these methods face great difficulties in detecting cyberattacks in large distributed environments, and the scalability of these methods over the large network is little. One of the drawbacks of traditional machine learning algorithms is that they use handcrafted features for the recognition task. But it is desirable that the machine itself found and structured the features for attack detection (Imamverdiyev, 2018).

Currently, deep learning is one of the most intensive research trends in the field of artificial intelligence and opens wide opportunities to overcome the constraints of traditional machine learning methods. In traditional machine learning algorithms, the features are extracted by humans. There is a special research direction—feature engineering. But in the big data processing, deep neural networks work better than a human in feature extraction (Imamverdiyev, 2018).

DL provides more accurate and faster processing because of its sophistication and self-learning capability. The success of DL in various disciplines and the limitation of traditional approaches in cybersecurity calls for the investigation of DL application in security domains. DL can be successfully applied to cybersecurity domains such as cyberattack detection (Tang, 2016; Wang, 2015).

Although DL methods have been successfully applied in images, speech and object recognition, these methods are currently being applied very little in cyberattack detection.

The inability of existing cybersecurity solutions to cope with the growing dynamics of cyberattacks, failure to detect new threats, difficulties in the analysis process of the complex events, and limitations of effective scalability by increasing the volume of data and attack, are the main challenges ahead of the new cybersecurity solutions creating area. The application of DL methods that will eliminate these problems is the key approach that attracts the attention of researchers. DL methods have extensive capabilities for successful application in the cybersecurity issues, such as DDoS attack detection, behavioral anomalies detection, malware and protocols detection, CAPTCHA codes detection, botnet detection and identification of the person by voice.

In this paper, the current state of research on cybersecurity methods based on various DL architectures is analysed, basic approaches in these studies, their advantages and problems are discussed, and the public datasets applied on experimental investigations of the methods are described.

The focus of our study is the investigation of the DL approach for cybersecurity attack detection. Thus, in this paper, our main contribution includes: