Chapter 1
Review on Intelligent Algorithms for Cyber Security

P. Subashini
https://orcid.org/0000-0002-8603-6826
Avinshilingam Institute for Home Science and Higher Education for Women, India

M. Krishnaveni
Avinashilingam Institute for Home Science and Higher Education for Women, India

T. T. Dhivyaprabha
Avinashilingam Institute for Home Science and Higher Education for Women, India

R. Shanmugavalli
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

Cyber security comprises of technologies, architecture, infrastructure, and software applications that are designed to protect computational resources against cyber-attacks. Cyber security concentrates on four main areas such as application security, disaster security, information security, and network security. Numerous cyber security algorithms and computational methods are introduced by researchers to protect cyberspace from undesirable invaders and susceptibilities. But, the performance of traditional cyber security algorithms suffers due to different types of offensive actions that target computer infrastructures, architectures and computer networks. The implementation of intelligent algorithms in encountering the wide range of cyber security problems is surveyed, namely, nature-inspired computing (NIC) paradigms, machine learning algorithms, and deep learning algorithms, based on exploratory analyses to identify the advantages of employing in enhancing cyber security techniques.

DOI: 10.4018/978-1-5225-9611-0.ch001

INTRODUCTION

In the recent scenarios, there is a significant growth in the usage of digital technologies, such as, Internet of Things (IoT), smart devices, sensors, cloud computing, big data, internet, mobile, wireless technologies and artificial intelligence covers that includes education, healthcare, communication, banking, government sector, armed force and enterprise in the world wide. The usages of digital technologies cause big challenges on the level of security, data protection and regulations followed by organizations to tackle threats in the cyber space. Providing and ensuring security mechanism in cyber space is a highly complex task. In order to meet these challenges, cyber security industry have developed several secured infrastructure, security algorithms, architecture and software applications to protect computational resources that involve software, hardware, electronic data and network from unauthorized access or vulnerability attacks that intended for exploitation. The primary areas covered in cyber security are application security, disaster security, information security and network security which are briefly stated below (Deepa, 2014). Application security focus on developing security measures to protect against threats detected in the application design, application development, deployment and maintenance. Disaster security deals with the development of cyber security processes that include developing risk assessment plans, setting priorities and establishing recovery strategies if any disaster occurred. Network security concentrates on ensuring protection, integrity, usability and reliability in the network connectivity. The components of network security include anti-virus or spyware, firewalls, virtual private network and intrusion prevention system to detect rapidly spreading threats in the computer networks. Finally, information security focuses on providing security to the information from unauthorized access. The statistical report and facts of cyber security in 2017-2018 posted (Dennis Anon on 11 September 2018) website states that Top 10 countries are affected by target attacks in which 303 known attacks present in Figure 1. It is understood that currently India occupies the second place with 133 cyber-attacks.

Cyber Security R & D Center (CSRDC) established by U.S. Department of Homeland Security has introduced several security technologies, infrastructures, operators and algorithms to protect vulnerable threats retrieved from 5 February 2019). Information Security Research Association (ISRA) is a non-profit organization which is focused on developing security technologies for web application security, wireless security, offensive security, malware protection and creates cyber security awareness in the society

(retrieved from 5 February 2019). An Annual cyber security report released by Cisco states that mobile phone is the first device targeted by several attackers that are intended for exploitation. Overall, 34% security professionals completely focuses on machine learning and artificial intelligence techniques for developing cyber security algorithms to defend against intruders especially, IoT threats, ransomware, big data, cloud environment, damaging General Data Protection Regulation (GDPR), smart devices, insider attacks, sensors and crypto currency mining (retrieved from 5 February 2019) (retrieved from 5 February 2019). Specifically, NIC paradigms, machine learning algorithms and deep learning algorithms play a vital role to improve the performance of cyber security algorithms and enhanced information technology security protocols in the recent era. Intelligent algorithms are essential to develop strong cyber security strategies that defend against malicious attacks.

Intelligent algorithms have capability to discover hidden patterns and detect threats in the computer information systems. The development of hybrid cyber security methods and building computational systems that integrates with intelligent algorithms is needful to analyze big data, mitigate threats and protect against the new invaders. The implementation of optimization techniques is a continuous evolution process in improving the performance of cyber security algorithms in order to yield promising