Machine Learning and Cyber Security:
Future Potential of the Research

Vardan Mkrttchian
https://orcid.org/0000-0003-4871-5956
HHH University, Australia

Sergey Kanarev
Penza State University, Russia

Leyla Gamidullaeva
https://orcid.org/0000-0003-3042-7550
Penza State University, Russia

INTRODUCTION

Cyber security has become an important subject of national, international, economic, and social importance that affects multiple nations (Walker, 2012). Many countries have come to understanding that this is an issue and has developed policies to handle this in an effort to mitigate the threats (Dawson, Omar, & Abramson, 2015). To address the issue of cyber security, various frameworks and models have been developed. Traditional approaches to managing security breaches is proving to be less effective as the growth of security breaches are growing in volume, variation and velocity (Bhatti & Sami, 2015). The purpose of this article is to show what future cyber security as engineering science and technology expects. In addition, the authors propose future solutions for the use of computer with a Sleptsov Net-processor when it will be actually created and practically implemented. The authors of the article did not consider the credibility issues of Sleptsov network computing but completely trusted the creator of Sleptsov net as a processor, based on open sources, in particular on publications and webinars of IGI Global (Zaitsev, 2016; Zaitsev, et al., 2016; Zaitsev, 2018). Based solely on these publications the authors research the emerging trends and perspectives of digital transformation of the economy using machine learning with avatar-based management at the platform of Sleptsov Net-processor and propose further prospects for development of hyper-computation (Mkrttchian, et al., 2019).

BACKGROUND

Many researchers compare machine learning solutions for cyber security by considering one specific application (e.g., Buczak and Guven, 2016; Blanzieri and Bryl, 2008; Gardiner and Nagaraja, 2016) and are typically oriented to Artificial Intelligence experts.

DOI: 10.4018/978-1-5225-9715-5.ch070

The term "cyber security" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware devices and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavor, including research and analysis, aimed at implementing those activities and improving their quality (Jenab, et al., 2018).

At the same time, our previous research of the problem of cyber security showed that cyber security is a section of information security, within the framework of which the processes of formation, functioning and evolution of cyber objects are studied. It is necessary to identify sources of cyber-danger formed while determining their characteristics, as well as their classification and formation of regulatory documents, implementation of security systems in future. However, working on the application of the machine learning for Cyber Security applications with the use of developed by the authors Avatars-Based Management techniques, we came to the conclusion that this is not so, and the built-in cyber security systems can be destroyed by the same artificial intelligence.

The search for a solution to this discrepancy leads to a thought about advantages of natural intelligence displayed by humans where everything is interconnected, logical and protected (Mkrttchian, et al., 2015).

This paper is specifically aims to research the emerging trends and perspectives of cyber security development in the conditions of digital economic transformation using machine learning with avatar-based management at the platform of Sleptsov Net-processor, and to identify their main limitations.

Sleptsov net concept mends the flaw of Petri nets, consisting in incremental character of computations, which makes Sleptsov net computing a prospective approach for ultra-performance concurrent computing (Zaitsev, 2018).

A Sleptsov net (SN) is a bipartite directed multi-graph supplied with a dynamic process (Zaitsev, 2016). An SN is denoted as N=(P,T,W,μ0), where P and T are disjoint sets of vertices called places and transitions respectively, the mapping F specifies arcs between vertices, and μ0 represents the initial state (marking). The mapping W: (P×T)→N∪{-1}, (T×P)→N defines arcs, their types and multiplicities, where a zero value corresponds to the arc absence, a positive value – to the regular arc with indicated multiplicity, and a minus unit – to the inhibitor arc which checks a place on zero marking. N denotes the set of natural numbers. To avoid nested indices we denote w,i j j− = w(p, t) and+ =) . The mapping μ: P→N specifies the place marking (Zaitsev, 2018).

Based on the previous research, performed by D. Zaitsev (2018; 2019), the main conclusion was drawn that Sleptsov networks are executed exponentially faster than Petri nets that makes it possible to recommend them as a parallel computing model for subsequent practical implementation.

Calculations on the networks of Sleptsov acquire all new applications presented in the works. First of all, computations on Sleptsov networks may be used for those applications in which parallel programming style can bring significant acceleration of computations.

Effective practical implementation of computations on Sleptsov networks requires the development of appropriate specialized automation systems for programming and hardware implementation of processors of Sleptsov networks. In addition, further development of theoretical methods of proving the correctness of programs in the language of Sleptsov networks and the development of universal networks that use mass parallelism are needed.