Perspective Tools to Improve Machine Learning Applications for Cyber Security

5

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

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

INTRODUCTION

Today security systems suffer from low detection rates and high false alarm rates. In order to overcome such challenging problems, there has been a great number of research conducted to apply Machine Learning (ML) algorithms (Tran, et al., 2012).

Machine learning techniques have been successfully applied to several real world problems in areas as diverse as image analysis, Semantic Web, bioinformatics, text processing, natural language processing, telecommunications, finance, medical diagnosis, and so forth (Gama, and Carvalho, 2012). Recent definition of machine learning is developed by I. Cadez, P. Smyth, H. Mannila, A. Salah, E. Alpaydin (*Cadez, et al., 2001; Salah and Alpaydin, 2004).*

The issues of the use of machine learning in cyber security are disclosed in many works *(Anagnostopoulos, 2018; Edgar and Manz, 2017; Yavanoglu and Aydos, 2017; Khan, et al., 2014; Khan, 2019; Dinur, 2018*). Using data mining and machine learning methods for cyber security intrusion detection is proposed by the authors (Kumar, et al., 2017). Object classification literature shows that computer software and hardware algorithms are increasingly showing signs of cognition and are necessarily evolving towards cognitive computing machines to meet the challenges of engineering problems (*Khan, et al, 2014).* For instance, in response to the continual mutating nature of cyber security threats, basic algorithms for intrusion detection are being forced to evolve and develop into autonomous and adaptive agents, in a manner that is emulative of human information processing mechanisms and processes *(Khan, et al., 2014; Khan, 2019).*

The maintenance of cyber security can significantly differ depending on the requirements for the control system, its purpose, the specificity of the managed object, the environmental conditions, the composition and state of the forces and controls, and the management order. Why do we need to distinguish between information and cyber security? What tasks can be achieved with this distinction?

This need is conditioned by the transition to a new socio-economic formation, called the information society. If earlier the problems of ensuring cyber security were relevant mainly for the military organization, in connection with the existence and development of the forces and means of information confrontation and electronic warfare, now such problems exist for the state as a whole.

Thus, the tasks of ensuring cyber security for today exist, both for the state as a whole, and for certain critical structures, systems and objects (Mkrttchian, et. al, 2019).

DOI: 10.4018/978-1-5225-9715-5.ch071

BACKGROUND

Modern economy networking now has become one of the most popular communication tools to have evolved over the past decade, making it a powerful new information sharing resource in world society. It is known, social-economy networking is the creation and maintenance of personal and business relationships especially through online social networking service that focuses on facilitating the building of social networks or social relations among people.

By embracing social networking tools and creating standards, policies, procedures, and security measures, educational organizations can ensure that these tools are beneficial.

The authors in this article show the essence, dignity, current state and development prospects of avatar-based management using blockchain technology for creation of new tools for machine learning applications (Mkrttchian, et al, 2016). The purpose of this article is not to review the existing published work on avatar-based models for policy advice, but to try an assessment of the merits and problems of avatar-based models as a solid basis for cyber security policy advice that is mainly based on the work and experience within the recently finished projects Triple H Avatar an Avatar-based Software Platform for HHH University, Sydney, Australia which was carried out 2008-2018 (Mkrttchian, et al., 2011,2012,2013,2014, 2015, 2016, 2017, 2018). The agenda of this project was to develop an avatar-based closed model with strong empirical grounding and micro-foundations that provides a uniform platform to address issues in different areas of digital economy. Particular emphasis was put on the possibility to generate an implementation of the model that allows for scaling of simulation runs to large numbers of avatars tools and to provide graphical user interfaces that allow researchers not familiar with the technical details of the implementation to design (parts of) the model as well as engineering and economy experiments and to analyze simulation output (Mkrttchian, 2015).

FOCUS OF THE ARTICLE

In this section, we discuss blockchain in relation to the visualization lifecycle including the following phases: identification, discovery, analysis, redesign, implementation, execution, monitoring, and adaptation. Using this lifecycle as a framework of reference allows us to discuss many incremental changes that blockchains might provide.

Process identification is concerned with the high-level description and evaluation of a company from a process-oriented perspective, thus connecting strategic alignment with process improvement. Currently, identification is mostly approached from an inward-looking perspective *(Dumas, et al., 2013).* Blockchain technology adds another relevant perspective for evaluating high-level processes in terms of the implied strengths, weaknesses, opportunities, and threats. For example, how can a company systematically identify the most suitable processes for blockchains or the most threatened ones? Research is needed into how this perspective can be integrated into the identification phase. Because blockchains have affinity with the support of inter-organizational processes, process identification may need to encompass not only the needs of one organization, but broader known and even unknown partners (Mkrttchian, et. al, 2019).

Process discovery refers to the collection of information about the current way a process operates and its representation as an as-is process model. Currently, methods for process discovery are largely based on interviews, walkthroughs and documentation analysis, complemented with auto-mated process discovery techniques over non-encrypted event logs generated by process-aware information systems *(Aalst, Wil, 2016).* Blockchain technology defines new challenges for process discovery techniques: the