


Chapter 49

Machine Learning Application With Avatar–Based Management Security to Reduce Cyber Threat

Vardan Mkrttchian


 <https://orcid.org/0000-0003-4871-5956>

HHH University, Australia

Leyla Gamidullaeva

Penza State University, Russia & K. G. Razumovsky Moscow State University of Technologies and Management, Russia

Yulia Vertakova

 <https://orcid.org/0000-0002-1685-2625>

Southwest State University, Russia

Svetlana Panasenکو

Plekhanov Russian University of Economics, Russia

ABSTRACT

This chapter is devoted to studying the opportunities of machine learning with avatar-based management techniques aimed at optimizing threat for cyber security professionals. The authors of the chapter developed a triangular scheme of machine learning, which included at each vertex one participant: a trainee, training, and an expert. To realize the goal set by the authors, an intelligent agent is included in the triangular scheme. The authors developed the innovation tools using intelligent visualization techniques for big data analytic with avatar-based management in sliding mode introduced by V. Mkrttchian in his books and chapters published by IGI Global in 2017-18. The developed algorithm, in contrast to the well-known, uses a three-loop feedback system that regulates the current state of the program depending on the user's actions, virtual state, and the status of implementation of available hardware resources. The algorithm of automatic situational selection of interactive software component configuration in virtual machine learning environment in intelligent-analytic platforms was developed.

DOI: 10.4018/978-1-6684-6291-1.ch049

INTRODUCTION

Existing security systems offer a reasonable level of protection; however, they cannot cope with the growing complexity of computer networks and hacking techniques. Moreover, 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).

In connection with the widespread use of information technologies in the military and state fields, along with the classical requirements for the controlling system (stability, continuity, efficiency, secrecy, efficiency), today also introduces fundamentally new requirements, such as:

- adaptability to changing conditions and methods of using the Armed Forces and State;
- providing a single information space on the battlefield;
- openness in terms of building and capacity building;
- possibility of reducing the operational and maintenance staff;
- evolution in development;
- technological independence.

Thus, 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.

Among the reasons for this situation can be called:

- The absence of an international legal basis prohibiting the use of information weapons and conducting information operations;

11 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/machine-learning-application-with-avatar-based-management-security-to-reduce-cyber-threat/307492

Related Content

Survey of Recent Applications of Artificial Intelligence for Detection and Analysis of COVID-19 and Other Infectious Diseases

Richard S. Segall and Vidhya Sankarasubbu (2022). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-30).

www.irma-international.org/article/survey-of-recent-applications-of-artificial-intelligence-for-detection-and-analysis-of-covid-19-and-other-infectious-diseases/313574

Sensor Fusion of Odometer, Compass and Beacon Distance for Mobile Robots

Rufus Fraanje, René Beltman, Fidelis Theinert, Michiel van Osch, Teade Punterand John Bolte (2020). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-17).

www.irma-international.org/article/sensor-fusion-of-odometer-compass-and-beacon-distance-for-mobile-robots/249249

Comparing Machine Learning Algorithms and DNN for Anomaly Detection

Apinaya Prethi K. N., Sangeetha M. and Nithya S. (2022). *Real-Time Applications of Machine Learning in Cyber-Physical Systems* (pp. 173-184).

www.irma-international.org/chapter/comparing-machine-learning-algorithms-and-dnn-for-anomaly-detection/299161

Machine Learning and Emotions: The Hidden Language in Your Voice

Jesús Heriberto Orduño-Osuna, María E. Raygoza L., Roxana Jiménez-Sánchez, Guillermo M. Limón-Molina and Fabian N. Murrieta-Rico (2024). *Machine and Deep Learning Techniques for Emotion Detection* (pp. 1-23).

www.irma-international.org/chapter/machine-learning-and-emotions/347289

An Integrated Process for Verifying Deep Learning Classifiers Using Dataset Dissimilarity Measures

Darryl Hond, Hamid Asgari, Daniel Jeffery and Mike Newman (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-21).

www.irma-international.org/article/an-integrated-process-for-verifying-deep-learning-classifiers-using-dataset-dissimilarity-measures/289536