IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

Cyber Hacking Breaches Prediction using Machine Learning

Sampath Kumar R[1], Krishna V R[2], N Ashok Reddy[2], N Naveen Upadhyaya[4], Abdula Muaz Ali[5]
Assistant Professor, Department of Computer Science[1]
Students, Department of Computer Science[2,3,4,5]
Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, Karnataka, India
krishna.cse.rymec@gmail.com, ashokreddy.cse.rymec@gmail.com,
naveen.cse.rymec@gmail.com, muiz.cse.rymec@gmail.com

Abstract: *Cyber-attacks are a major threat to these systems. Unlike faults that occur by accidents in cyber-physical systems, cyber-attacks occur intelligently and stealthily. Some of these attacks which are called deception attacks, inject false data from sensors or controllers, and also by compromising with some cyber components, corrupt data, or enter misinformation into the system. If the system is unaware of the existence of these attacks, it won't be able to detect them, and performance may be disrupted or disabled altogether. The proposed method in this study is to use the structure of deep neural networks for the detection phase, which should inform the system of the existence of the attack in the initial moments of the attack. In the presented control method, after the attack detection phase with the use of a deep neural network, the control system uses the reputation algorithm to isolate the misbehaving agent. Experimental analysis shows us that deep learning algorithms can detect attacks with higher performance than usual methods and can make cyber security simpler, more proactive, less expensive, and far more effective.*

Keywords: Cyber-attacks, Cyber Hacking, Cyber-hacking breaches

REFERENCES

[1]. "Security analysis for cyber-physical systems against stealthy deception attacks". In 2013 American control conference. Available [online]:
[2]. "Design and implementation of attack-resilient cyber-physical systems: With a focus on attack-resilient state estimators." IEEE Control Systems Magazine (2017). Available [online]:
[3]. "Consensus formation control for a class of networked multiple mobile robot systems." Journal of Control Science and Engineering 2012 (2012). Available [online]:
[4]. "Resilient distributed control in the presence of misbehaving agents in networked control systems."IEEE Transactions on Cybernetics (2014). Available [online]:
[5]. "Resilient control of networked control systems with stochastic denial of service attacks." Neurocomputing (2017). Available [online]:
[6]. "Robustness of information diffusion algorithms to locally bounded adversaries." In 2012 American Control Conference (ACC), IEEE (2012). Available [online]:
[7]. "Resilient Consensus of Discrete-Time Complex Cyber-Physical Networks under Deception Attacks." IEEE Transactions on Industrial Informatics (2019). Available [online]:
[8]. "Machine learning methods for attack detection in the smart grid." IEEE Transactions on neural networks and learning systems 27, (2015). Available [online]:
[9]. "Data mining based cyber-attack detection." System simulation technology 13, (2017). Available [online]:
[10]. "Attack detection and identification in cyber-physical systems." IEEE Transactions on Automatic Control (2013). Available [online]: