Editorial
Volume 10:S5, 2021

International Journal of Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Effectiveness of Machine Learning in the Field of Cyber Security

Lapon Dorji*

Department of Electrical Engineering, College of Science and Technology, Phuntsholing, Bhutan

Description

The advancement of Internet and online media adds to multiplying the information delivered on the Internet and the associated hubs, yet the default installation and the setup of assortment of software systems address some security openings and shortcomings, while most of Internet users have not actually set up safety awareness, prompting high security risk. With the improvement of network attack methods, each host on the Internet has turned into the target of attacks. Therefore, the network data security can't be overlooked as an issue. To manage 0-day and future attack, the honeypot strategy can be utilized latently as a data framework, yet in addition to support the traditional defence systems against future attack.

Machine Learning is a subarea of artificial intelligence that mainly focus on the learning ability of the computer; its plan of action allow understanding the data structure and coordinating them into models that can be perceived and used to tackle complex issues in real-life situations, and its techniques address a proficient device to address the significant difficulties posted by the big data.

Organizations have invested a plenty of arrangement on time and money in manual networks reconfiguration, to save data systems from infiltration. It is notable that the locks break and the keys can be replicated; in this manner, it is a deception to believe that a lock and a key address perfect security. So, the genuine challenge in terms of digital protection is to acknowledge the likelihood of a forthcoming attack and to get what is truly happening inside complex data frameworks. Conventional security tools like IDS, Firewalls, and IPS can ensure frameworks against basic attacks that utilize similar devices and strategies over and over. They are executed autonomously; hence, there is no contact between them to hinder interruption recognized in IDS by the firewall, for instance, they address a passive solution when it is around 0-day attack.

The proposed arrangement based on Machine Learning (ML) procedures combination as tools for gathering data, investigation, and threat predictions, to guarantee the security of organization's network. The execution of honeypots relies upon the administrations proposed to clients by the servers of the production organization. To screen dubious profiles through the services given by this organization, in similar honeypot server, three virtual machines can be implemented, and everyone is arranged to imitate one of the past services with the safe shell (SSH) module to permit remote access to any of the virtual machines.

This execution permits identifying dubious profile patterns on services, for anticipating attacker profiles dependent on Artificial Intelligence analysis. Choices will allow reconfiguring the security strategy (e.g., Firewall) to impede the attackers. Subsequently, the firewall ought to be arranged in a manner to divert dubious flow to the honeypots to accumulate data about the application and the transport layers. The gathered information will be submitted to a combination of algorithms. A grouping strategy will be utilized to bunch the information into homogenous classes and create the client profile. Then the profile will be classified into an attacker or non-attacker profile dependent on another classification algorithm.

Conflict Of Interest

The authors declare that he has no conflicts of interest.

How to cite this article: Dorji, Lapon . "Effectiveness of Machine Learning in the Field of Cyber Security." *J Sens Netw Data Commun* S5 (2021) : e004.

***Address to correspondence:** Lapon Dorji, Department of Electrical Engineering, College of Science and Technology, Phuntsholing, Bhutan; E-mail: dor.23lapon@edu.bt*

Received: 02 December, 2021; **Accepted:** 15 December, 2021; **Published:** 22 December, 2021