Prediction of Cyber Attack Using Data Using Technique

Praveen Raj. S[1], Keerthanapriyan .p[2], K.M.Sai krithika[3]
[1, 2, 3] Dept of Computer Science Engineering
[1, 2, 3] GKM College of Engineering and Technology, Chennai, India

Abstract- *Cyber-attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. The state of the cyberspace portends uncertainty for the future Internet and its accelerated number of users. New paradigms add more concerns with big data collected through device sensors divulging large amounts of information, which can be used for targeted attacks. Though a plethora of extant approaches, models and algorithms have provided the basis for cyber-attack predictions, there is the need to consider new models and algorithms, which are based on data representations other than task-specific techniques. However, its non-linear information processing architecture can be adapted towards learning the different data representations of network traffic to classify type of network attack. In this paper, we model cyber-attack prediction as a classification problem, Networking sectors have to predict the type of Network attack from given dataset using machine learning techniques..*

Keywords- Cyber-attack & Deep learning

I. INTRODUCTION

Nowadays, it has become exceedingly difficult to ensure the security of our systems including both corporate and personal data. Major countries, such as the United States and the United Kingdom, struggle with cyber-attacks and crimes by producing various security strategies (Reid & Van Niekerk, 2014). Countries are striving to ensure security in cyber space and adapt to this field (Goel, 2020). Protecting the critical infrastructures has a vital importance for countries. Chemical, financial, health and energy sectors, even nuclear power plants in some countries can be counted among these (CISA, 2020). Due to millions of cyber-attacks, financial losses significantly increase day by day (Jang-Jaccard & Nepal, 2014). In 2020, data stolen from the information system of Airbus Company were put on the dark web market. Medical data of millions of people have been stolen and even state of emergency has been declared due to attacks on some cities (Check Point Security Report, 2020). The most important elements ensuring cyber security are integrity, confidentiality, authentication, authorization, nonrepudiation and availability (Bayuk et al., 2012).

With each passing day, the work force becomes insufficient in fighting against cyber incidents and new solutions are sought. Solutions such as autonomous cyber defense systems (Crawford, 2017), smart cyber security assistant architecture (Sayan, 2017) and intrusion detection systems (Ben-Asher & Gonzalez, 2015) are investigated in the fight against cyber-attacks and crimes. Researchers use machine-learning methods to detect power outages due to cyber-attacks (Wang et al., 2019) and to prevent vulnerabilities of the Internet of things (Zolanvari et al., 2019). Other areas of use are to determine spam and network attacks (Canbek, Sagiroglu & Temizel, 2018), to detect the phishing attacks against the banking sector (Moorthy & Pabitha, 2020) and to reduce sexual crimes on social media (Ngejane et al., 2018). These methods have been implemented in fields as stock prediction (Gurjar et al., 2018), risk mapping by crimes (Wheeler & Steenbeek, 2020) and cyber profiling (Zulfadhilah, Prayudi & Riadi, 2016). Predicting crime trend and pattern (Biswas & Basak, 2019), criminal identity detection (Bharathi, Indrani & Prabakar, 2017) and crime prevention (Lin, Chen & Yu, 2017) are also areas of implementation.

II. LITERATUREREVIEW

A literature review is a body of text that aims to review the critical points of current knowledge on and/or methodological approaches to a particular topic. It is secondary sources and discuss published information in a particular subject area and sometimes information in a particular subject area within a certain time period. Its ultimate goal is to bring the reader up to date with current literature on a topic and forms the basis for another goal, such as future research that may be needed in the area and precedes a research proposal and may be just a simple summary of sources. Usually, it has an organizational pattern and combines both summary and synthesis.

A summary is a recap of important information about the source, but a synthesis is a re-organization, reshuffling of

information. It might give a new interpretation of old material or combine new with old interpretations or itmight trace the intellectual progression of the field, including major debates. Depending on the situation, the literature review may evaluate the sources and advise the reader on the most pertinent or relevant of them.

Loan default trends have been long studied from a socio-economic stand point. Most economics surveys believe in empirical modeling of these complex systems in order to be able to predict the loan default rate for a particular individual. The use of machine learning for such tasks is a trend which it is observing now. Some of the survey's to understand the past and present perspective of loan approval or not.

III. FUTUREWORK

- Network sector want to automate the detecting the attacks of packet transfers from eligibility process (real time) based on the connection detail.
- To automate this process by show the prediction result in web application or desktop application.
- TooptimizetheworktoimplementinArtificialIntelligenceen vironment.

Tkinter:

Tkinter is Python's de-facto standard GUI (Graphical User Interface) package. It is a thin object-oriented layer on top of Tcl/Tk. Tkinter is not the only GUI Programming toolkit for Python. It is however the most commonly used one. ... Graphical User Interfaces with Tk, a chapter from the Python Documentation.

The tkinter package ("Tk interface") is the standard Python interface to the Tcl/Tk GUI toolkit. Both Tk and tkinter are available on most Unix platforms, including macOS, as well as on Windows systems.

Running python –m tkinter from the command line should open a window demonstrating a simple Tk interface, letting you know that tkinter is properly installed on your system, and also showing what version of Tcl/Tk is installed, so you can read the Tcl/Tk documentation specific to that version.

IV. CONCLUSION

The analytical process started from data cleaning and processing, missing value, exploratory analysis and finally model building and evaluation. The best accuracy on public test set is higher accuracy score will be find out by comparing each algorithm with type of all network attacks for future prediction results by finding best connections. This brings some of the following insights about diagnose the network attack of each new connection. To presented a prediction model with the aid of artificial intelligence to improve over human accuracy and provide with the scope of early detection. It can be inferred from this model that, area analysis and use of machine learning technique is useful in developing prediction models that can helps to network sectors reduce the long process of diagnosis and eradicate any human error.

REFERENCES

[1] Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

[2] This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TEVC.2018.2880458, IEEE Transactions on Evolutionary Computation

[3] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things," *Eur. Trans. Telecomm.*, vol. 25, no. 1, pp. 81-93, Jan. 2014.

[4] L. D. Xu, W. He, S. C. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014.

[5] F. Tao, Y. Zuo, L. D. Xu, L. Zhang, "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing," *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1547-1557, May. 2014.

[6] Y. S. Ding, Y. L. Jin, L. H. Ren, K. R. Hao, "An intelligent self-organization scheme for the Internet of Things," *IEEE Comput. Intell. Mag.*, vol. 8, no. 3, pp. 41-53, Aug. 2013.

[7] M. Gigli, S. Koo, "Internet of Things: Services and applications categorization," *Advances Internet Things.*, vol. 1, no. 2, pp. 27-31, Jul. 2011.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 4, pp. 2347-2376, Nov. 2015.

[9] G. Fortino, C. Savaglio, and M. C. Zhou, "Toward opportunistic services for the industrial Internet of Things," in *Proc. IEEE Conf. Autom. Sci. Eng (CASE).*, Xi'an, China, Aug. 2017, pp. 825-830.

[10] A. Zaslavsky, C. Perera, D. Georgakopoulos, "Sensing as a service and big data," in *Proc. Int. Conf. Cloud Comput (ACC).*, Bengaluru, India, Jul. 2012, pp. 21–29.

[11] C. Perera, A. Zaslavsky, C. H. Liu, M. Compton, P. Christen, D. Georgakopoulos, "Sensor search techniques for sensing as a service architecture for the Internet of Things," *IEEE Sens. J.*, vol. 14, no. 2, pp. 406-420, Feb. 2014.

[12] M. E. Khanouche, Y. Amirat, A. Chibani, M. Kerkar, A. Yachir, "Energy-centered and QoS-aware services selection for Internet of Things," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1256-1269, Jul. 2016.