Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 12, December 2021, pg.32 – 38

Deep Reinforcement Learning for Cybersecurity Applications

Alex Mathew
Department of Cybersecurity, Bethany College, USA
dr.alex.soh@gmail.com
DOI: 10.47760/ijcsmc.2021.v10i12.005

Abstract*— There has been a rapid growth of the devices connected to the internet in the last decade for the various internet (IoT) of things applications. The increase of these smart devices has posed a great security concern in the internet of things ecosystem. The internet of things ecosystem must be protected from these threats. Reinforcement learning has been proposed by the cybersecurity professionals to provide the needed security tools for securing the IoT system since it is able to interact with the environment and learn how to detect the threats. This paper presents a comprehensive research on cybersecurity threats to the IoT system applications. The RL algorithms are also presented to understand the attacks on the IoT. Reinforcement learning is widely employed in cybersecurity because it can learn on its own experience by investigating and capitalizing on the unknown ecosystem, this enables it solve many complex problems. The RL capabilities on dealing with cybercrime challenges are also exploited in this paper.

***Keywords*— Cybersecurity, Reinforcement Algorithms, Machine Learning, Cyber-threats, Supervised learning, unsupervised learning**

I. Introduction

Technological and computer network advancement has led to exponential increase of smart devices connected to internet in the past decades. The interconnections between devices and other entities to the internet have led to emergence of the Internet of Things (IoT) ecosystem. The IoT systems are made up of the combination of both computer hardware and software to perform a specific task in IoT ecosystem (Kouicem et al., 2018). The connection of these devices to internet exposes them to different cyber security threats, which compromises the integrity and privacy of these devices.

II. Cyberspace Threats

According to Arulkumaran et al., (2017) the exponential growth of the IoT ecosystem has made the attacks more complex and hard to protect the devices because malware, malicious activities and other ransomware attacks have increased rapidly. Other security concerns include; denial of services (DoS), unauthorized access to personal or organization data, phishing and data and privacy violation. It also causes social disruption and breach of individual data as explained by Behzadan, V. (2021). Therefore, there is a need to develop cyber-security tools to eliminate and reduce the effects of cyberspace attacks. Cyber security is combination of all technological techniques created to safe guard the IoT devices such as computers software, networks programs and personal data from unauthorized access, malicious activities and attacks (Nguyen, T. T., & Reddi, V. J., 2020). Cybercrimes are very complex that the traditional known security tools such as encryption, antivirus, and other user authentication and firewall cannot protect these systems effectively. Therefore, there is a need for effective cybersecurity management tools and techniques to protect these IoT devices in cyberspace.

III. Reinforcement Algorithms and Applications.

Supervised and unsupervised learning methods are some of the ML applications used to address the challenges of cybersecurity in the IoT ecosystem as explained by (Kouicem et al., 2018). Reinforcement Learning is widely used for security purposes because it can learn different environments by its own experience, to investigate data patterns in the system by use of reinforcement algorithms as explained below.

1) Multi-layer Perceptron (MLP) Algorithm

MLP is one of the supervised learning algorithm network with a well-combined neural network. The input layer gets input information while the output layer determines the input signal. MLP also contains other layers in between the input and output layer, which are used for computational purposes in the network. All the nodes in a given layer are fully linked to the other nodes in the next layer. The output of the network is determined by the activation function elements such as ReLU. MLP applies a Backpropagation method to train its network. The backpropagation technique is used for network weights optimization and maps all the inputs to respective target output. MLP is used in cyber security to analyze security attacks and detect malicious botnet traffics. It can be used to learn non-linear models even in absolute time. MLP is shown in the MLP fig.1. below.

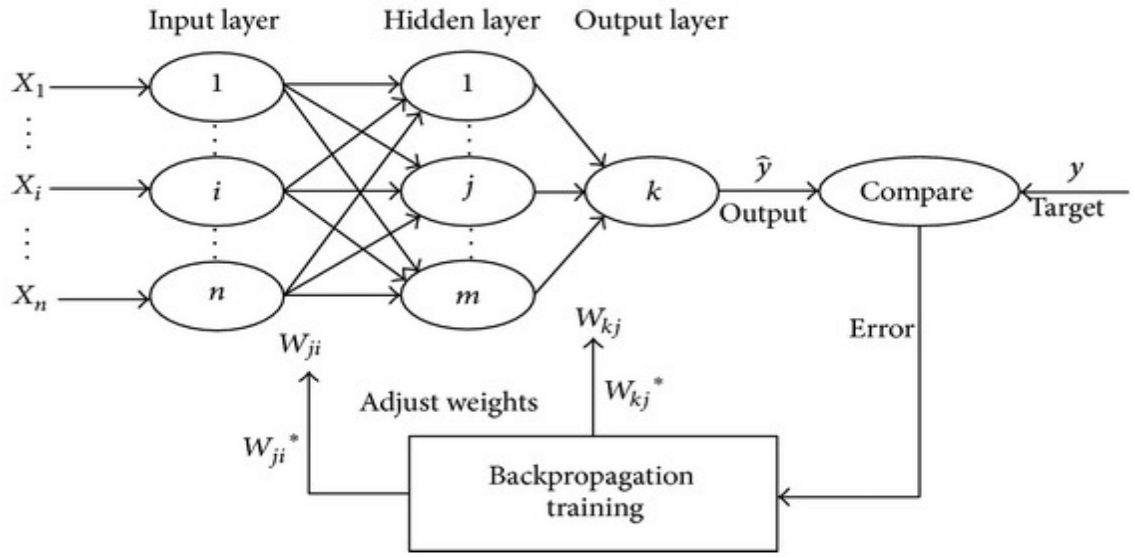

Fig.1.Above Shows an example of a Multi-Layer Perceptron (MLP) Algorithm.

2) Convolutional Neural Network (CNN) Algorithm

(CNN) is deep learning network design, which does not require extraction manual, learn the data structure, because it learns it directly. The CNN is made up of the following layer elements; input layer, fully connected layer, pooling, convolutional and output layers. This CNN helps in improving the ANN, which is also a multi-layer perceptron. CNN layers are optimized to provide a significant outcome. The optimization helps in reducing the complexity and it capitalizes on 'dropout' to deal with issue of over fitting, thus prevent a typical network.

The CNN fig.2. below shows CNN network.

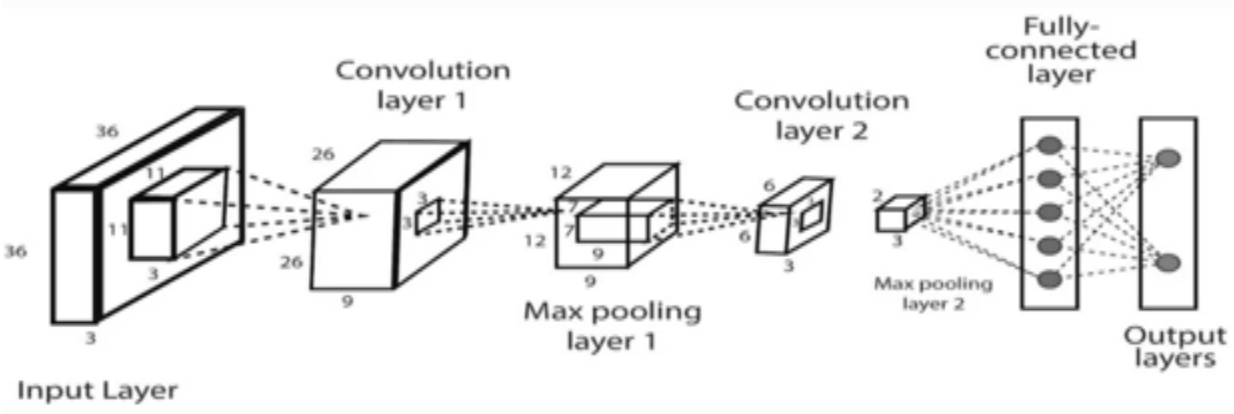

Fig.2.Above Shows an example of Convolution Neural Network(CNN) Algorithm

CNN are designed to deal with any 2D images. Therefore, it is applied in visual images and medical image analysis it is also used in financial time series. For the cyber security, CNN assists in intrusion detection such as denial of service threats in IoT ecosystem. CNN helps in detecting malware. CNN is more powerful than ANN is since it detects crucial features without supervision Sarker, I. H. (2021).

3) Recurrent Neural Network (RNN) Algorithm

Recurrent neural network (RNN) is an artificial neural network that is able to generate a series of inputs and keep its state as it processes the subsequent series of inputs. The RNN contains a loop in its recurrent layer that enables it to retain information over period. For instance, Long Short term memory (LSTM) networks have special unit, which enables them to store information for long time.

The LSTM units help in dealing with the vanishing gradient challenges neural networks. The LSTM gates works collectively to regulate the flow of information in the LSTM unit Shersinsky, A. (2020). The forget gate determines the kind of information to be retained from the previous state cell, it also removes the data that is not required. The input gate determines the information to get into the cell state. The output gate determines and regulates the outputs in the unit cell. LSTM networks are applied in time series predictions, anomaly detection, voice recognition etc. LSTM is used in cyber security to detect security attacks such intrusion. It can also detect and analyze malicious applications. The Fig.3.below shows the LSTM unit

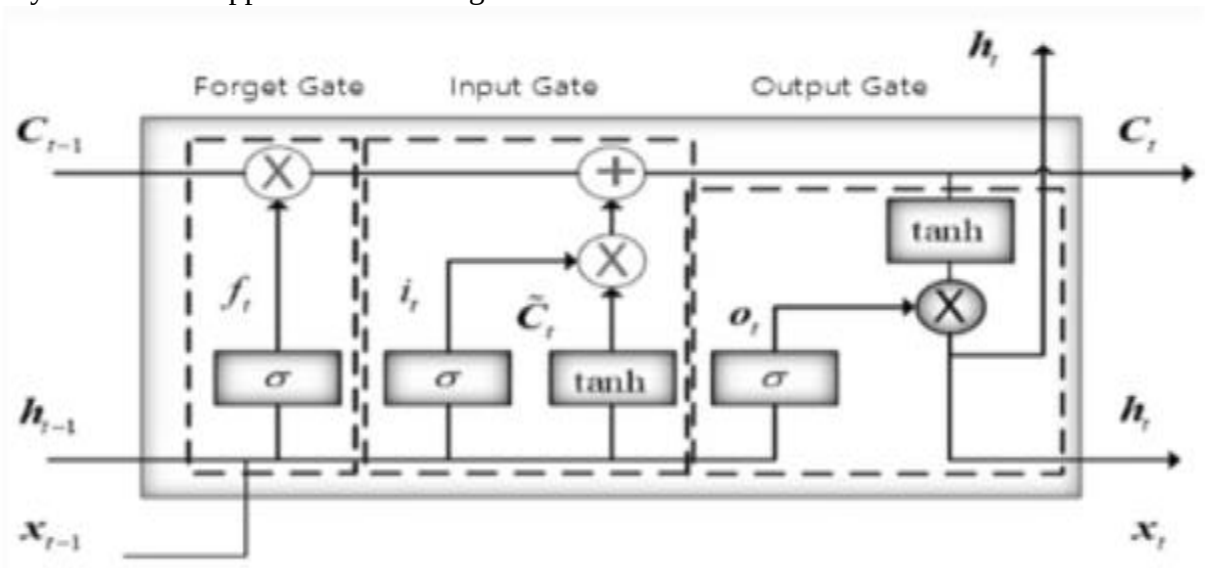

Fig.3. Above Shows an example of Recurrent Neural Network (RNN) Algorithm.

4) Self-Organizing Map (SOM) Algorithm

Self-organizing map (SOM) is a machine learning algorithm that follows an unsupervised learning model to train its network where the data sets are identified as they compete for representation. To start SOM mapping, a weight vector is loaded in the system. A sample vector is then selected and weight vectors map is searched to find the one that represents the sample. The weight is then selected from the neighboring weight vectors and then rewarded, as it is similar to random sample vector. The neighbors close to the weight are also rewarded for being resembling the selected sample vector; this reduces the number of neighbors vectors (Nilashi et al., 2020). Fig. 4. Below shows SOM Algorithm.

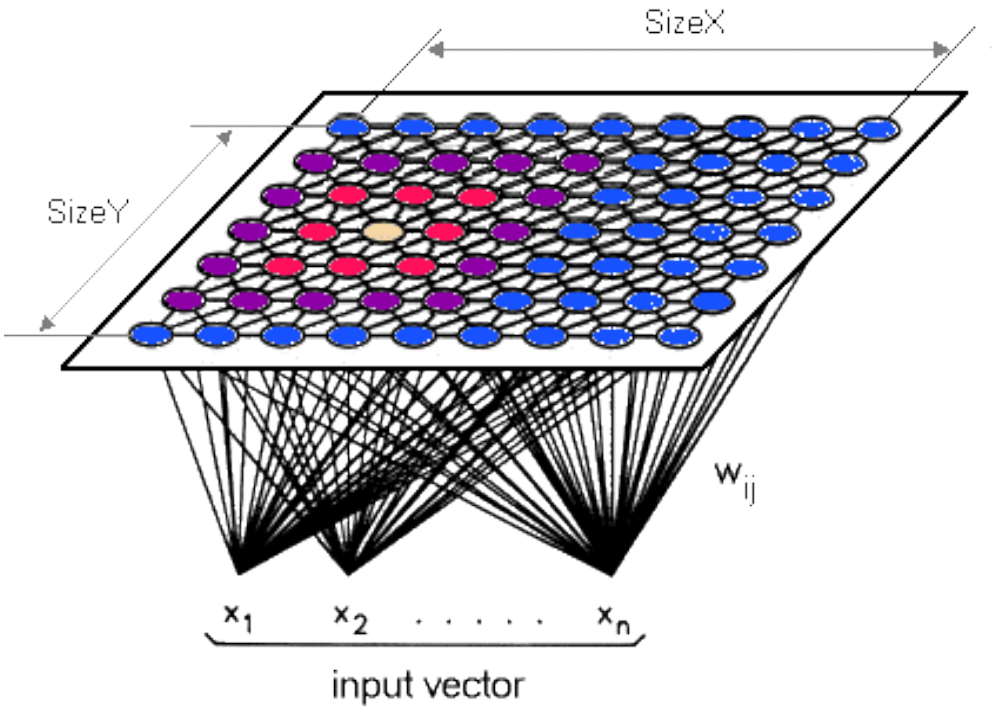

Fig.4. Above Shows an example of Self-Organizing Map (SOM) Algorithm.

SOM is used in medical diagnosis, pattern recognition. It is also used to detect virus attack. MOS has been used in cybersecurity to detect deadly network traffics and data analyses tool and visual mining and analyses the habits of the computer users such as security and fraud incidents. MOS makes it easy for data interpretation and understanding according to Nilashi et al., (2020). Thus, MOS can be used to create a data driven security algorithms, which largely relays on the data's characteristics.

5) Deep Transfer Learning (DTL) Algorithm

Deep transfer learning (DTL) is used in deep learning to address the challenges of insufficient data training. This enables the network in eliminating AI model training since it is able to train small amount of data. DTL is categorized into inductive transfer learning where the target changes from the source task. It applies instance, parameter, relational knowledge and features transfers. The other category is Transductive Transfer Learning where the target tasks and the source are equal, but the target domain and the source are not the same. Instance and feature transfers are applicable. Unsupervised transfer learning is the third category, and it is the same as inductive transfer (Long et al. 2017). DTL is applied in computer vision medical imaging sentiment categorization and voice identification. DTL is applied to solve cyber security problems because it is able to identify and classify malicious software in the network. It has classifier accuracy of 94.72% to 96.90% thus; security experts use it to train models for security purposes.

The fig.5. below shows the DTL Algorithm.

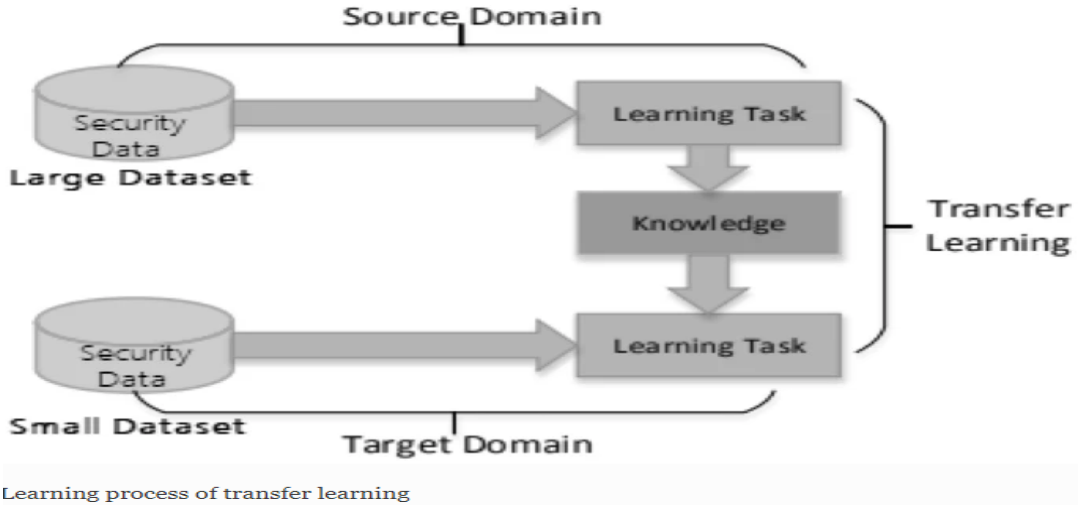

Fig.5. Above Shows an example of deep Transfer Learning(DTL) Algorithm.

IV. Results and Analysis

Reinforcement learning employs different algorithms for security procedures. These algorithms have different capabilities to execute their tasks. For instance, the MLP algorithm is supervised learning model, which applies a back propagation procedure to train its network. The backpropagation is used for weight optimization to map all the inputs to a given target. MLP is used to learn non-linear models in real time. The other RL algorithm is CNN, which learns the data directly, thus the extraction manual is not required. CNN layers are optimized to reduce complexity and relays on 'dropout' to prevent typical network due to over fitting effect. CNN is used to detect malware without supervision Sarker, I. H. (2021). The third RL algorithm is the Recurrent Neural Network (RNN), this one is able to generate a series of inputs while keeping its state as it processes the next series of input. RNN contains a loop in recurrent layer that helps it to store information for period. The LSTM gate controls the flow of information in LSTM unit; LSTM is used to detect intrusion and malicious apps Shersinsky, A. (2020). Self-organizing map (SOM) is RL algorithm that works on unsupervised learning model to train its network. Data sets in SOM are identified as the compete for representation. SOM is used to detect deadly network traffics and analysis the habits of computer user and fraud activities. It is used for data interpretations thus applied in data driven security algorithms. Deep Transfer Learning (DTL) is an algorithm used to tackle the challenges of insufficient data training. It trains small data and it is applied in cyber-security to identify and classify malicious software in the network. It has a classifier accuracy of 94.72% to 96.90% thus; it is used train models for security purposes.

V. Conclusion

Finally, security of all the devices connected to the internet is exposed to cybercrime threats, which can damage the system and compromise the data stored in the devices. It can also Cybercrime can cause social interruption because it can infer with the world's security. These attacks can also lead to breach of individual data. Therefore, cybersecurity experts must develop security technological tools to protect and reduce the damages and effects of cyberspace attacks. Reinforcement learning (RL) is one of the effective technological tools adopted by cyber-security professionals to address these security challenges.

References

[1]. Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (2017). Deep reinforcement learning: A brief survey. *IEEE Signal Processing Magazine*, *34*(6), 26-38.

[2]. Behzadan, V. (2021). Security of deep reinforcement learning. Retrieved 13 December 2021, from https://krex.k-state.edu/dspace/handle/2097/39799

[3]. Banerjee, I., Ling, Y., Chen, M. C., Hasan, S. A., Langlotz, C. P., Moradzadeh, N., ... & Lungren, M. P. (2019). Comparative effectiveness of convolutional neural network (CNN) and recurrent neural network (RNN) architectures for radiology text report classification. *Artificial intelligence in medicine*, *97*, 79-88.

[4]. Chauhan, R., Ghanshala, K. K., & Joshi, R. C. (2018, December). Convolutional neural network (CNN) for image detection and recognition. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 278-282). IEEE.

[5]. Gardner, W., Winkler, D. A., Ballabio, D., Muir, B. W., & Pigram, P. J. (2020). Analyzing 3D hyperspectral TOF-SIMS depth profile data using self-organizing map-relational perspective mapping. *Biointerphases*, *15*(6), 061004.

[6]. Gardner, W., Maliki, R., Cutts, S. M., Muir, B. W., Ballabio, D., Winkler, D. A., & Pigram, P. J. (2020). Self-organizing map and relational perspective mapping for the accurate visualization of high-dimensional hyperspectral data. *Analytical Chemistry*, *92*(15), 10450-10459.

[7]. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221.

[8]. Long, M., Zhu, H., Wang, J., & Jordan, M. I. (2017, July). Deep transfer learning with joint adaptation networks. In *International conference on machine learning* (pp. 2208-2217). PMLR.

[9]. Mern, J., Hatch, K., Silva, R., Brush, J., & Kochenderfer, M. J. (2021). Reinforcement Learning for Industrial Control Network Cyber Security Orchestration. *arXiv preprint arXiv: 2106.05332*.

[10]. Nguyen, T. T., & Reddi, V. J. (2020). Deep reinforcement learning for cyber security.

[11]. Nilashi, M., Ahmadi, H., Sheikhtaheri, A., Naemi, R., Alotaibi, R., Alarood, A. A., ... & Zhao, J. (2020). Remote Tracking of Parkinson's Disease Progression Using Ensembles of Deep Belief Network and Self-Organizing Map. *Expert Systems with Applications*, *159*, 113562.

[12]. Sherstinsky, A. (2020). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. *Physica D: Nonlinear Phenomena*, *404*, 132306.

[13]. Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, *2*(3), 1-16.

[14]. Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018, October). Internet of Things security: a survey. In *2018 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 162-166). IEEE.

[15]. Ye, C., Zhang, D., Hu, X., Huang, X., Feng, H., & Zhang, K. (2018, September). Recurrent neural network (RNN) based end-to-end nonlinear management for symmetrical 50Gbps NRZ PON with 29dB+ loss budget. In *2018 European Conference on Optical Communication (ECOC)* (pp. 1-3). IEEE.

