IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 10, No. 2, June 2021, pp. 382~388
ISSN: 2252-8938, DOI: 10.11591/ijai.v10.i2.pp382-388

DDoS attack detection using deep learning

Thapanarath Khempetch, Pongpisit Wuttidittachotti
Department of Data Communication and Networking, King Mongkut's University of Technology North Bangkok, Thailand

Article Info

Article history:

Received Mar 15, 2020
Revised Oct 24, 2020
Accepted Apr 5, 2021

Keywords:

CICDDoS2019
DDoS
Deep learning
DNN
LSTM

ABSTRACT

Nowadays, IoT devices are widely used both in daily life and in corporate and industrial environments. The use of these devices has increased dramatically and by 2030 it is estimated that their usage will rise to 125 billion devices causing enormous flow of information. It is likely that it will also increase distributed denial-of-service (DDoS) attack surface. As IoT devices have limited resources, it is impossible to add additional security structures to it. Therefore, the risk of DDoS attacks by malicious people who can take control of IoT devices, remain extremely high. In this paper, we use the CICDDoS2019 dataset as a dataset that has improved the bugs and introducing a new taxonomy for DDoS attacks, including new classification based on flows network. We propose DDoS attack detection using the deep neural network (DNN) and long short-term memory (LSTM) algorithm. Our results show that it can detect more than 99.90% of all three types of DDoS attacks. The results indicate that deep learning is another option for detecting attacks that may cause disruptions in the future.

Corresponding Author:

Pongpisit Wuttidittachotti
Data Communication and Networking
King Mongkut's University of Technology North Bangkok
1518 Pracharat 1 Road, Wongsawang, Bang Sue District, Bangkok 10800, Thailand
Email: pongpisit.w@it.kmutnb.ac.th

1. INTRODUCTION

Nowadays, the Internet has become an integral part of our daily lives. It makes communication easier. The internet of things (IoT) is becoming more widely used both in everyday life and in the industry. IoT devices are small and able to communicate with each other without requiring a human being during communication [1], [2]. It can apply to a variety of systems such as smart home, smart farm, smart factory, increasing IoT devices. It is predicted that by 2030, there would be 125 billion IoT devices connected to the internet [3]. This would likely put all such devices at risk of being used in DDoS attacks because IoT devices cannot support the complex security structure given it's limited resources as in processors or backup memory, thus making these devices especially vulnerable. If this vulnerability is not fixed, there is a chance of it being attacked and compromised as IoT devices for use in DDoS attacks [4], [5].

DDoS attacks have been around for a long time. The first occurred on July 22, 1999, when a computer at the University of Minnesota, containing a dangerous script named Trin00, attacked 114 other computers [6], [7]. On October 21, 2016, Dyn, a DNS service provider, was attacked, causing Twitter, GitHub, Playstation Network, and other websites to be unavailable for a while. The IT security company said the attack linked to the Mirai IoT DDoS Botnet [8], [9], and on February 28, 2018, GitHub was hit by a 1.35 Tbps DDoS attack with 126.9 million packages per second [10]. Aside from being unable to be of service after being attacked it can also cause financial damage. Kaspersky Lab reports estimated average damage to medium-sized businesses (SMBs) are $120K, and to large companies are $2 million per attack [11].

Threats arising from the growing number of IoT devices and new DDoS attack techniques have resulted in the detection and blocking of attacks with deep learning (DL). DL is useful in finding relationships between the prominent features of the dataset that distinguish between "normal" and "abnormal" and can predict the likelihood if new attacks would occur in the future by learning from existing examples [12], [13]. Nowadays, DL is very popular due to its efficiency and non-linear multi-layer processing, including Python, with support libraries allowing us to create artificial neural networks more quickly than in the past [14].

Unal *et al*. presented DDoS attacks on the network with deep learning, using NSL-KDD datasets to show their IDS performance. The dataset consists of 23 different attacks with 41 features. They have reviewed the literature to reduce it to only 24 features related to DDoS attacks. The accuracy is 98.8% [15]. Diro and Chilamkurti, also presented a distributed attack detection in IoT with deep learning using the same dataset but using apache spark techniques to help train the modelling process and securing an accuracy of 96-99%. However, the dataset used is the old dataset and therefore it may not predict new attacks that could occur [16].

Doshi *et al*. used machine learning to detect DDoS in the IoT using data collected from real IoT devices. They simulated the Botnet attack environment using five algorithms to measure performance: KN, LSVM, DT, RF, NN. From the results, the neural network had 98.9% accuracy with the dataset they created [17].

In this research, we use the dataset of CICDDoS2019, which is the dataset of DDoS attack, and uses the classification algorithm of deep learning, learning from the dataset order to find a suitable neural network structure that can differentiate between standard data and attack data. Authors have organized this presentation into the following sections: Introduction - Research Method - Results and Discussion – Conclusion.

1.1. Distributed denial-of-service attack

DDoS attacks are caused by computer equipment or IoT devices infected with malware and trying to prevent online services from providing services to users usually by blocking or causing the server to stop service temporarily, DDoS is often used from a large number of occupied devices through the distribution of Botnet, which is different from DoS attacks with a single device connecting to the internet and flooding attacks to the target machine [18], [19].

1.2. Artificial neural network

Artificial neural networks (ANNs) are a set of algorithms inspired by the biological structure of the human and animal brain. ANN consists of interconnected "units." In biology, these units are called a neurons. These neurons are processed and sent to another neuron, acting as a switch to turn on and off. The elements of the artificial neural network are quite simple, but the complexity and energy of this system is derived from the interaction between the various components.

In the 50s, the first artificial neural network (ANN) was created to perform simple logical functions. AI can be used in algebra, geometry, language, and robotics. In recent years, access to a large amount of information is possible. The computing power and machine learning techniques (ML) are becoming increasingly useful in businesses, and especially in the advent of a graphics processing unit (GPU) that can be used to train models with large neural networks efficiently which we know of as deep neural networks (DNNs) [20].

1.3. Deep neural network (DNN) and long short-term memory (LSTM)

A deep neural network is a network for multi-layered inference based on logistic regression models with two-dimensional input. All the neural networks consist of an input layer, an output layer, and one or many hidden layers. If there are many hidden layers, we will call them deep neural networks. LSTMs are caused by using RNNs to improve the vanishing gradient and exploding gradient problems by creating an architecture that can remember information for a long time. From the above structure, DNN and LSTM can correlate each data including the use of supervised learning techniques to assist in the training process, allowing DDoS to be detected more efficiently [21], [22].

2. RESEARCH METHOD

The operation overview in Figure 1 shows the divided process in 5 steps. Starting with the first step, after we get the datasets, they are not immediately available. Therefore, we need to proceed to the next step. The second step is the data preparation process. We will do data cleaning, feature selection, and feature engineering to prepare the data for this step. Then we will split the datasets into three sets in the third step to

creating a set of training data, validation data and testing data for use in the training process. After that, we will go through the fourth step about designing a deep neural network structure. In this step of the process, the training data and validation data will be used. The tuning of the hyperparameters is done in conjunction with the validation process to determine the optimal structure. Once the structure is optimized for the datasets, the fifth step is to evaluate the designed models' measurement using testing data to measure the results.

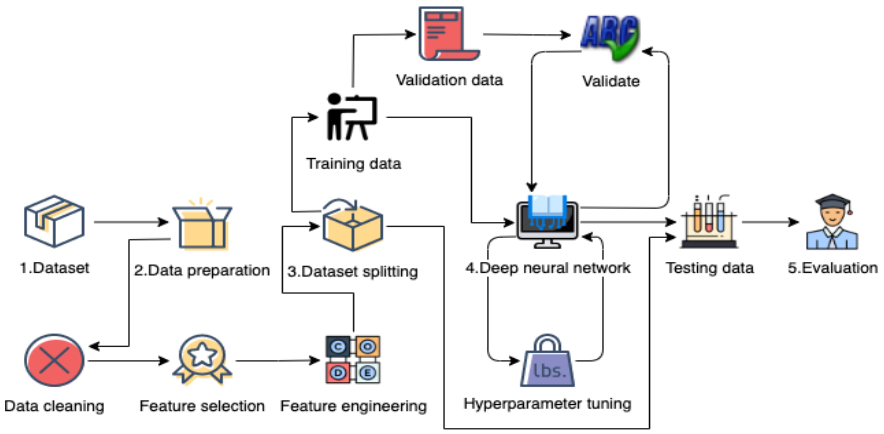

Figure 1. Operation overview

2.1. Dataset

In this paper, we use the CICDDoS2019 dataset of the "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" research. They have improved the existing dataset and have presented a new taxonomy for DDoS attacks, including bug fixes including new classification based on flows network. It also has features for detecting different types of DDoS attacks with a consistent weight [23].

2.2. Data preparation

After the dataset has loaded it will not be able to work with deep learning at all, therefore it must go through the data preparation process first. 1) Data cleaning is to remove data that is not usable, such as empty data, and special characters. 2) Feature selection is selecting the relevant feature for DDoS attack detection. It can be chosen by using the Weka algorithm or reviewing literature from proper research in order to minimize the irrelevant attack detection features. 3) Feature engineering, is to transform the data into a form that deep learning can use in the training process.

2.3. Dataset splitting

After we have the dataset, the training model is usually divided into three parts: training data, validation data, and testing data. In the classification training process, we use the training dataset [24].

2.4. Deep neural network

The first step is to define the structure of the deep neural network. It is the structure to use to learn data from the dataset we entered. It usually consists of three main layers: 1) The input layer is responsible for receiving data from the dataset. Typically, one node is equal to one dimension or the number of features contained in the dataset. 2) The hidden layer is the layer that receives data from the input layer. The data obtained is weighted. In this class, the number of nodes must be set appropriately in order to be able to learn complex information. 3) Output layer is the last layer that receives data from the previous layer. In this layer, the value is the number of probabilities, with the numbers being 0.00 to 1.00 only.

In the second step, hyperparameter optimization is an enhancement that is related to the training model process for better results. The adjustment will consist of: 1) The learning rate affects the finding of the loss by having to find the most suitable value in order not to make the loss worse. 2) Batch size affects the accuracy of the model and it increases the time to train the model. If the adjustment is too small, it will take a long time to train. If the alignment is too large, it will use a lot of resources. 3) Epochs the number of cycles of the model trend. If the loss value continues to decrease, we can increase the number of rounds until it reaches a point where the loss value does not change. 4) Hidden layer, the more multiple layers, the more

accurate. Therefore, adjust the number of layers to suit our dataset. 5) Hidden units, the number of nodes in the hidden layer must be optimized, and there is enough to learn the complexity of the data. 6) Dropout is a technique that is used to drop connections between nodes randomly. It can be done during model training since some nodes may coincide and also helps to reduce overfitting occurrences [25].

2.5. Evaluation

We can measure the effectiveness of the deep learning model that we will use to detect DDoS attacks by using indicators from the standard matrix as follows: 1) Accuracy is the model's overall accuracy. 2) Precision is the probability that the model will predict the correct attack. 3) The recall is the probability that the model can detect attacks from the total number of attacks. 4) F-Measure or F1-Score is a harmonic mean between precision and recall. The formulas for calculating values are in the bottom equation.

$$Accuracy = (TP+TN)/(TP+TN+FP+FN)$$
$$Precision = TP/(TP+FP)$$
$$Recall = TP/(TP+FN)$$
$$F\text{-}Measure = 2((Precision*Recall)/(Precision+Recall))$$

Where TP, TN, FP, and FN stand for true positives, true negatives, false positives, and false negatives, respectively. This step will help us find the best model for the dataset we choose to use, as well as how well the selected model will work in the future.

3. RESULTS AND DISCUSSION

3.1. Experimental settings and results

In the testing process, the DDoS attack detection model tested using Python 3.6.9 and Keras 2.2.5 in the Google Colab environment: Intel Xeon CPU, 2.20GHz, 12.48GB memory with OS Ubuntu 18.04.3 LTS. The structure of deep learning as shown in Figures 2 and 3, designed to detect all three types of DDoS attacks: Syn Flood, UDP, and UDP-Lag. Dropout inserts to reduce overfitting during model training The comparison was also conducted between the DNN model and the LSTM model. The DNN and LSTM structures are designed for performance comparisons. The DNN structures consist of four dense layers and three dropout layers, as shown in Figure 2. The LSTM structure consists of one LSTM layer, three dense layers, and three dropout layers, as shown in Figure 3. We assign 20 nodes to the first layer in each structure, 40 nodes and 60 nodes for the second and third layers, respectively. The layer is inserted with the dropout layer.

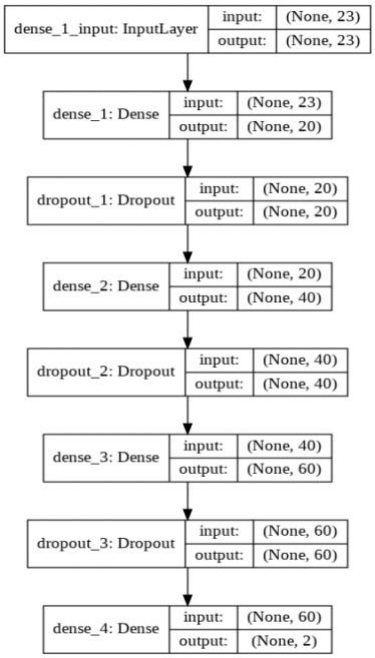

Figure 2. DNN structure

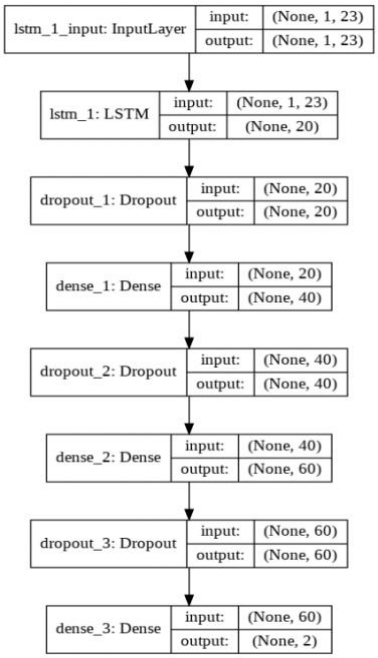

Figure 3. LSTM structure

As for the characteristics as shown in Figure 4, choose to use the attributes according to the research of the dataset due to the better detection performance compared to the experiments that we experimented with selecting the characteristics ourselves. The datasets that we choose to use are the Syn, UDP, and UDP-Lag attack datasets. Each dataset divided into Training data (60%), validation data (10%), and test data (10%), respectively, and we feed the training data into our deep network models.

```
' Destination Port'              int64
' Protocol'                      int64
' Flow Duration'                 int64
'Total Length of Fwd Packets'    int64
' Fwd Packet Length Max'         int64
' Fwd Packet Length Min'         int64
' Fwd Packet Length Std'       float64
' Flow IAT Mean'               float64
' Flow IAT Max'                  int64
' Flow IAT Min'                  int64
'Fwd IAT Total'                  int64
' Fwd IAT Mean'                float64
' Fwd IAT Max'                   int64
' Fwd Header Length'             int64
'Fwd Packets/s'                float64
' Min Packet Length'             int64
' Max Packet Length'             int64
' Packet Length Std'           float64
' ACK Flag Count'                int64
' Average Packet Size'         float64
' Subflow Fwd Bytes'             int64
Init_Win_bytes_forward           int64
' min_seg_size_forward'          int64
Class                            int64
dtype: object
```

Figure 4. Features selection [23]

From Table 1, is to determine the hyperparameter and optimizer we use RAdam instead of Adam because it is more smooth in the training process by setting total_steps = 5,000, warmup_proportion = 0.1, min_lr = 0.001, and set the number of Epochs as ten because after this model it can no longer reduce losses. The results of the DNN and LSTM tests achieved almost the same performance, but LSTM was able to capture Syn Flood, and UDP Flood attacks a little better. DNN detected slightly better UDP-Lag attacks. In the attack detection tests as shown in Tables 2 and 3, it can see that the DNN shows the F1 score or F-Measure at .9995-.9997, and the accuracy is .9993-.9995. LSTM, the effectiveness of F1-Score or F-Measure is .9994-.9998, and the accuracy is .9990-.9997 for all three types of DDoS classification.

Table 1. Model parameters

Variable	Values
Loss	categorical_crossentropy
Activation	Relu
Optimizer	RAdam
Epochs	10
Batch size	64

Table 2. The performance of DNN

	Accuracy	Precision	Recall	F-Measure
Syn	0.9995	0.9998	0.9997	0.9997
UDP	0.9995	0.9995	1.0	0.9997
UDP-Lag	0.9993	0.9994	0.9997	0.9995

Table 3. The performance of LSTM

	Accuracy	Precision	Recall	F-Measure
Syn	0.9997	0.9998	0.9998	0.9998
UDP	0.9996	0.9996	1.0	0.9998
UDP-Lag	0.9990	0.9989	1.0	0.9994

4. CONCLUSION

In this article, we propose deep learning based DDoS detection methods using the DNN and LSTM algorithms. We designed the deep neural network structure that is appropriate for the classification of attacks in the CICDDoS2019 dataset by the results of the three attack detection experiments. The types of Syn Flood, UDP Flood, and UDP-Lag can distinguish "normal" and "abnormal" data from each other, with an average accuracy of 99.90-99.97%. For future work, we plan to increase the variety of learning to compare with the DNN and LSTM algorithms, as well as to bring models to test with the rest of the attack types such as DNS, NetBIOS, SNMP, to compare the performance of the model. We can include different kinds of dataset attacks to increase the challenge of detecting attacks and using the model created for testing in the real world.

ACKNOWLEDGEMENTS

Thank you to Mr. Bhaskar Laha, Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok, for English editing.

REFERENCES

[1] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures", *International Journal for Information Security Research (IJISR)*, vol. 5, no. 4, December 2015, https://doi.org/10.1109/ICITST.2015.7412116.

[2] O. Bello and S. Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things," in *IEEE Systems Journal*, vol. 10, no. 3, pp. 1172-1182, Sept. 2016, https://doi.org/10.1109/JSYST.2014.2298837.

[3] M. Miettinen and A. Sadeghi, "Keynote: Internet of Things or Threats? On Building Trust in IoT," *2018 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Turin, pp. 1-9, 2018, doi: 10.1109/CODESISSS.2018.8525931.

[4] M. Abomhara and G. M. Kien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," in *Journal of Cyber Security and Mobility*, vol. 4, no 1, pp. 65-88, Jan 2015, https://doi.org/10.13052/jcsm2245-1439.414.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, https://doi.org/10.1109/COMST.2015.2444095.

[6] "The first DDoS attack was 20 years ago," Emerging Technology from the arXiv. [Online]. Available: https://www.technologyreview.com/s/613331/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/

[7] X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, Hong Kong, pp. 1-8, 2017, https://doi.org/10.1109/SMARTCOMP.2017.7946998.

[8] J. Smith-perrone and J. Sims, "Securing cloud, SDN and large data network environments from emerging DDoS attacks," *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, Noida, pp. 466-469, 2017, doi: 10.1109/CONFLUENCE.2017.7943196.

[9] Abhishta, R. V. Rijswijk-Deij, and L. J. M. Nieuwenhuis, "Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 5, 70-76, January 2019, https://doi.org/10.1145/3310165.3310175.

[10] H. K. Hyder and C. Lung, "Closed-Loop DDoS Mitigation System in Software Defined Networks," *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, Kaohsiung, Taiwan, pp. 1-6, 2018, doi: 10.1109/DESEC.2018.8625125.

[11] "DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report," Woburn, MA. [Online]. Available:https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report/.

[12] Y. Xin *et al*., "Machine Learning and Deep Learning Methods for Cybersecurity," in *IEEE Access*, vol. 6, pp. 35365-35381, 2018, https://doi.org/10.1109/ACCESS.2018.2836950.

[13] Y. Imamverdiyev and F. Abdullayeva, "Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine," *Big Data*, vol. 6, no. 2, pp. 159-169, 2018, https://doi.org/10.1089/big.2018.0023.

[14] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning. *Nature* 521, 436–444, 2015, https://doi.org/10.1038/nature14539.

[15] A. S. Unal and M. Hacibeyoglu, "Detection of DDOS Attacks in Network Traffic Using Deep Learning," *International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES18)*. http://indexive.com/Paper/157/detection-of-ddos-attacks-in-network-traffic-using-deep-learning.

[16] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, May 2018, pp. 761-768, 2017, https://doi.org/10.1016/j.future.2017.08.043.

[17] R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, CA, pp. 29-35, 2018, https://doi.org/10.1109/SPW.2018.00013.

[18] Distributed denial of service attack (DDoS) definition.imperva. [Online]. Available: https://www.imperva.com/learn/application-security/ddos-attacks/
[19] K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, pp. 1-6, 2016, https://doi.org/10.1109/ISCO.2016.7727096.
[20] Marchi D. L., and Mitchell L., "Hands-On Neural Networks: Learn how to build and train your first neural network model using Python," *Packt Publishing*, 2019.
[21] M. Moocarme, M. Abdolahnejad, and R. Bhagwat, "The Deep Learning with Keras Workshop: An Interactive Approach to Understanding Deep Learning with Keras," 2nd Edition. *Packt Publishing*, 2020.
[22] C. D. McDermott, F. Majdani and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," *2018 International Joint Conference on Neural Networks (IJCNN)*, Rio de Janeiro, pp. 1-8, 2018. https://doi.org/10.1109/IJCNN.2018.8489489.
[23] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India, pp. 1-8, 2019, https://doi.org/10.1109/CCST.2019.8888419.
[24] Workflow of a Machine Learning project. Ayush Pant. [Online]. Available: https://towardsdatascience.com/workflow-of-a-machine-learning-project-ec1dba419b94/
[25] Hyperparameters in Deep Learning. Ayush Pant. [Online]. Available: https://towardsdatascience.com/hyperparameters-in-deep-learning-927f7b2084dd/

BIOGRAPHIES OF AUTHORS

Mr. Thapanarath Khempetch was born in Suphan Buri, in 1991. He received a Bachelor of Engineering Program in Computer Engineering from the Faculty of Engineering, Kasetsart University, in 2016. At present, He is studying for a Master of Science in Data Communication and Networking, King Mongkut's University of Technology North Bangkok, in 2018.

Dr. Pongpisit Wuttidittachotti is currently an associate professor and head of the Department of Data Communication and Networking at the Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. He received his Ph.D. in Networks, Telecommunications, Systems and Architectures from INPT-ENSEEIHT, in France. He received an outstanding employee award in social service at the university level in 2019, an outstanding employee award at the faculty level and the university level in 2020. He owns more than 30 recognized certifications, for example, CISSP, CISM, CISA, CRISC, CGEIT, IRCA ISO/IEC 27001:2013 Lead Auditor, COBIT 5 Foundation, COBIT 2019 Foundation, COBIT 2019 Design & Implementation, Data Protection Officer (DPO) etc. So far, Wuttidittachotti has over ten years of working experience covering software development, network, security, audit, risk management, IT governance, and standard, and compliance. His expertise has shown out as a member of the ISACA Bangkok Chapter committee since 2015, and an Accredited Trainer - COBIT® 2019 Foundation for ISACA Bangkok Chapter. He has conducted and published many research articles continually in information security and related topics.