



# AIoT processing techniques for efficiently extracting and analyzing large amounts of IoT information

Y. S. Jeong<sup>1</sup>

<sup>1</sup>Division of Information and Communication Convergence Engineering, Mokwon University, 88 Doanbuk-ro, Seo-gu, Daejeon 35349, Korea

## Abstract

Background/Objectives: Recently, as the usability of IoT devices increases, the kinds of information processed by IoT devices are also diversifying. For this reason, research to ensure the high-speed processing and integrity of information generated from IoT devices continues steadily. In particular, research using various hash techniques is actively underway to minimize IoT information errors. Methods/Statistical analysis: In this paper, instead of sending IoT information directly to the server (data center), we propose an AIoT technique that allows AIoT to pre-analyze and delivers only important information. Findings: The proposed technique allows easy control of IoT information operation after analyzing patterns of information collected from IoT devices to extract and analyze large amounts of IoT information. Furthermore, the proposed technique minimizes network delay as well as minimizes server (data center) processing and analysis time by reducing network traffic that can occur when information collected from numerous IoT devices is delivered to the server (data center). Improvements/Applications: AIoT, IoT information, Extract and Analysis, Artificial, Depp Learning, hash techniques Performance evaluation compared the storage efficiency of servers and the number of transactions of IoT information sent and received per second between IoT devices and AIoT devices while varying the hash length of IoT information from 16 bits to 128 bits.

## Index Terms

AIoT, IoT information, Extract and Analysis, Artificial, Depp Learning, Hash techniques

**Corresponding author : Y. S. Jeong**

bukmunro@gmail.com

- Manuscript received December 16, 2020.
- Revised January 15, 2021; Accepted February 2, 2021.
- Date of publication March 31, 2020.

© The Academic Society of Convergence Science Inc.

2546-1583 © 2017 IJEMR. Personal use is permitted, but republication/redistribution requires IJEMR permission.

## **I. INTRODUCTION**

Over the past few years, studies have been steadily studied that can be used in various ways in healthcare, transportation, the environment, and defense using Internet of Things (IoT) devices [1]. IoT systems used in cloud environments consist of sensors, computing, actuators, etc., and applications for better utilization of IoT systems have been developed, enabling new business creation in various environments [2].

However, with the pre-analysis of IoT information and the emergence of several problems that may arise in the network (increase network latency, increase traffic when sending and receiving IoT information, server overhead as data grows, security, etc.) in addition to servers in the cloud environment [3-5].

Recently, hash methods have been applied to deep learning techniques to ensure the integrity of information processed by AIoT devices. In recent studies, most studies are underway, focusing on the Closvue hash and deep learning hash, to ensure better processing time and minimal latency than traditional methods. In particular, in the search efficiency section, information loss is minimized by combining deep learning and hashing learning.

In this paper, we propose an AIoT processing technique that allows AIoT to efficiently extract and analyze large amounts of IoT information by pre-filtering IoT information before it is delivered to servers (data centers). The proposed technique improves network latency and integrity by applying weights of IoT information between layers  $n+1$  and  $n-1$  using blockchain for the information collected from IoT devices. In particular, IoT information scheduling was applied at a certain interval to efficiently analyze IoT information on AIoT devices, while ensuring that AIoT's location is located closest to IoT devices.

The composition of this paper is as follows. Chapter 2 explores existing research related to IoT and AIoT. Chapter 3 proposes data extraction techniques using AIoT devices, and Chapter 4 compares and analyzes performance evaluations based on whether or not to use AIoT. Finally, we conclude in Chapter 5.

## **II. BACKGROUND**

Foreoohifar et al. have been designed to distribute the learning of machines performed in cloud environments, ensuring the complexity and reliability that can arise from machine learning [6]. However, it failed to improve the latency and energy consumption of IoT devices to be transmitted and received in cloud environments.

Kang et al. To solve the problem in [6], we propose a method that can lighten the scheduler to perform DNN operations on AIoT devices [7]. However, the latency did not significantly improve when the amount of IoT information processed by the scheduler

increases.

Zhao et al. proposed an optimized three-tier framework to minimize the energy consumption of IoT devices [8]. However, it has been shown that this method is optimized for mobile edge environments rather than IoT environments.

Yang et al. proposed a framework for performing hierarchical deep learning tasks by separating CNN models into two layers in an overlay network [9].

Wang et al. are reducing the loss of resources between local updates and parameter aggregation to minimize IoT resources [10].

Mills et al. proposed a technique that reduced runtime considering distributed datasets and communication costs [11]. The biggest feature of this technique is not the process of collaborating with the cloud.

Figurnov et al. is performing a classification task first to enable conditional learning of DNNs to dynamically perform IoT information [12].

Bolukbasi et al. proposed an early shutdown plan to avoid activating the entire layer to improve the processing time and accuracy of numerous DNN information [13].

Figurnov et al. propose an architecture that dynamically adjusts the number of layers in the image area [14].

Teerapittayanon et al. proposed an architecture that allows the deployment of DNNs of end devices to dynamically adjust the number of layers in different regions [15]. This method reduces the prediction accuracy whenever new events occur so that the initialization of the same model does not change all models.

## **III. DATA EXTRACTION TECHNIQUES USING AIOT DEVICES**

### **A. Overview**

Recently, artificial intelligence technology has been in the spotlight all over the world, and various IoT devices are being used to collect data from industrial sites. In particular, the accuracy of IoT collection information is recognized as a very important factor, as industrial sites that collect critical data have a variety of results depending on how accurate the information collected is.

Information collected from IoT devices requires the user to control the settings because IoT devices cannot filter themselves. Also, problems such as speed and latency for data analysis arise because the information collected from IoT devices is sent to the cloud server (data center) and then used after filtering the importance of information according to the policies of the server (data center).

Through analysis capabilities (intelligent filtering) that can evaluate data as quickly as it occurs from IoT

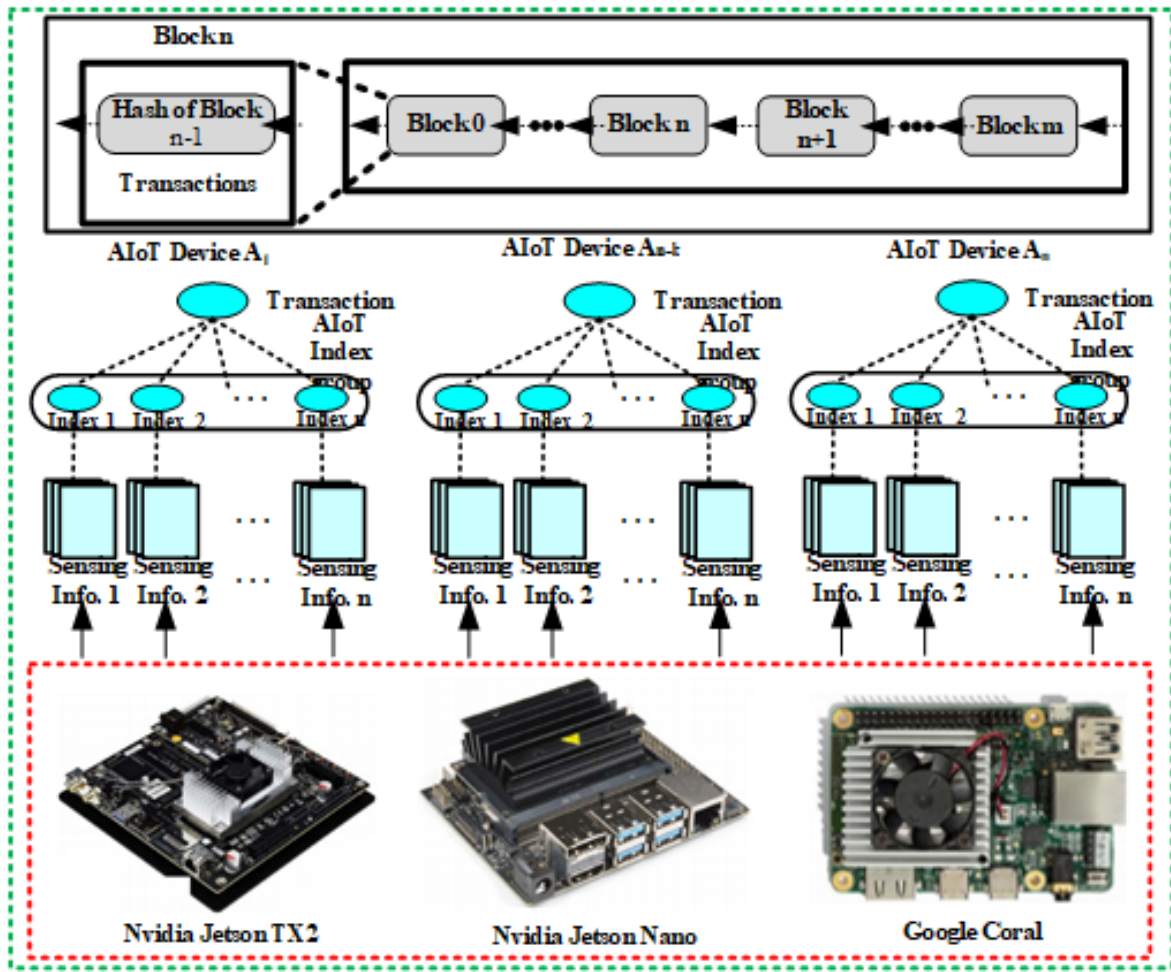


Fig. 1. Gathering information using various devices

devices and convert it into useful information that can be actioned, the various added value of industrial sites can be created in terms of intelligence, not connection.

In this paper, we reflect the requirements of these industrial sites to pre-process the information collected from IoT devices on AIoT devices and then perform the action shown in Figure 1 to form a blockchain and send important data to the server (data center). Through the process shown in Figure 1, the proposed technique can have several advantages. First, network delays can be minimized by minimizing the network traffic that can occur when information collected from numerous IoT devices is delivered to the server (data center). Second, information collected from IoT devices can be pre-processed to minimize processing time for servers (data centers) to process and analyze. Third, we can improve convenience by analyzing patterns of information collected from IoT devices by controlling device operation. Fourth, data analysis using artificial intelligence technologies such as deep learning can be easily used for other application services.

The proposed technique allows faster processing and integrity than conventional methods because it

processes transactions of index information in IoT information by placing it in a DNN model when information collected from IoT devices is filtered by AIoT. Furthermore, the proposed technique proposes dynamic memory resources of AIoT devices to classify inaccurate information after comparing the information processed in AIoT with a pre-stored dataset.

### B. Link IoT information in AIoT devices using hierarchical subnets

Various kinds of information collected from IoT devices generate linked information as shown in Figure 2 to be asymmetrically processed by AIoT. The linked information generated in the course of Figure 2 consists of a pairwise contrast matrix and constructs IoT information in a hierarchical structure. The reason for doing this is to exploit the low bandwidth of information collected from IoT devices and the load balance information processed by the hash function to support fast processing.

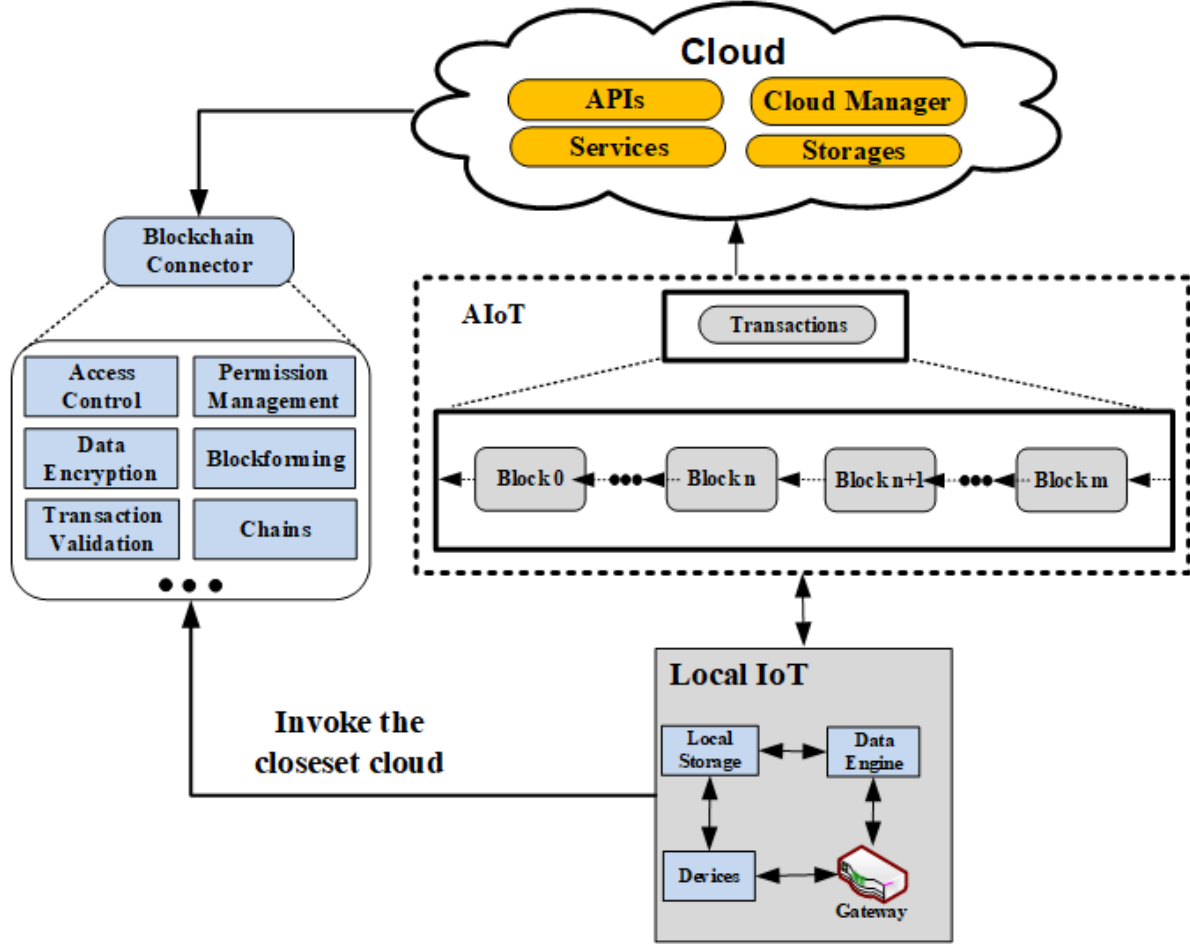


Fig. 3. IoT information Scheduling

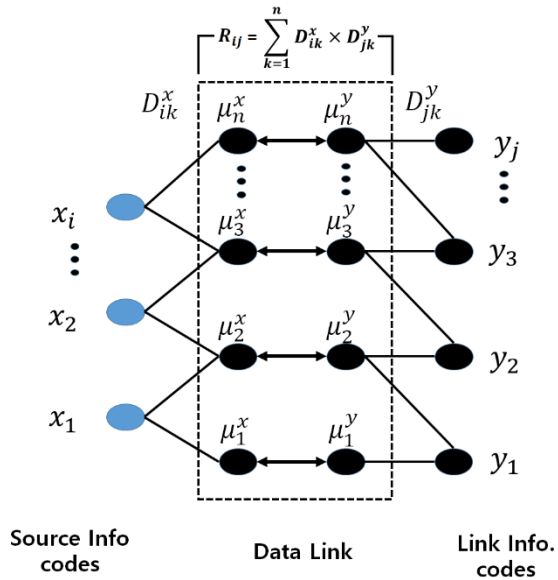


Fig. 2. IoT Information Connection Processing

In Figure 2,  $R_{ij}$  means the association information of the  $i$ -th and  $j$ -th of the pairwise contrast matrix  $d_{ij}$ .  $x_1, x_2, \dots$ , and  $x_n$  refer to the source information code of the IoT device, and  $y_1, y_2, \dots$ , and  $y_n$  refer to

the link information code generated by the hash chain.

In the proposed techniques, processes such as Figure 2 allow us to easily maintain links between IoT information as well as eliminate redundant information collected from IoT devices.

### C. Scheduling of IoT information

As shown in Figure 3, the proposed technique allows us to reflect the scheduling policy at regular intervals to efficiently analyze and process information collected from heterogeneous IoT devices in AIoT. Furthermore, the proposed technique applies the weight of IoT information between layers  $n+1$  and  $n-1$  by using blockchain in a hierarchical distributed structure to reduce bottlenecks in the process of sending and receiving IoT information. In particular, for improving the efficiency of IoT information scheduling and minimizing latency, the location of AIoT is maintained in the closest position to IoT devices.

### D. Calculate the importance of IoT information

The proposed technique yields the importance of IoT information by pairing IoT information and IoT-linked information with blockchain to perform hierarchical multi-linked information collected from

heterogeneous IoT devices. The importance of IoT information in the proposed technique represents the importance of IoT information as the entropy of probability values in the same way as expression (1).

$$E_{IoT} = \begin{cases} \sum_{i=1}^n P_i \log \frac{1}{P_i} & P_i > 0.5 \\ -\sum_{i=1}^n P_i \log P_i & P_i < 0.5 \end{cases} \quad (1)$$

Where  $P_i$  means the importance of IoT information expressed as probability information.

In the proposed technique, IoT-critical information is expressed as  $H_{IoT} : \{0,1\} \rightarrow Z_N$ , while hierarchical IoT-critical information is expressed as  $H_{IoT} : \{0,1\}^* \times Z_N \rightarrow Z_N$ .

## IV. PERFORMANCE EVALUATION

### A. Simulation Environment Settings

For simulation purposes, the experimental environment is as shown in Table 2. The experimental parameters of Table 1 are used to evaluate the performance that can occur in networks and servers when AIoT devices collect data and filter only critical data based on weight information. The purpose of the simulation is to minimize the margin of error of each assessment item when the proposed techniques are applied to the actual environment.

**Table 1.** MAJOR PARAMETERS FOR THE SIMULATION ENVIRONMENT

Parameter	Value
Learning rate	0.00025 to 0.00005
Mini-batch size	16, 32, 64
Replay memory size	2Gbyte
Discount factor	0.99
Training time steps	4M

In particular, the main parameters of Table 2 were simulated by referring to the environment of [1] with Deep Q-Networks (DQN), which incorporates Q learning and deep cardiac networks (DNNs).

### B. Evaluation

Table 2 shows a comparison of the storage efficiency of servers by dividing information collected from IoT devices into those analyzed and not analyzed by AIoT, changing the hash length of linked information codes from 16 bits to 128 bits. As a result, we obtain an average 8.4% improvement over the case where we process the linked information code of IoT information using AIoT. These results allow for direct processing of information classified in n

sizes in the higher layers, rather than just one to reduce network bandwidth, when delivering classified and processed information in AIoT to higher layers.

**Table 2.** SERVER STORAGE EFFICIENCY(%)

Method	Hash code length			
	16	32	64	128
Not using AIoT	61.367	65.865	68.653	70.091
Using AIoT	67.283	75.624	79.324	82.375

Table 3 shows the number of transactions of IoT information sent and received per second between IoT devices and AIoT devices. From the results in Table 3, the proposed technique achieves an average 2.34x improvement over the case with AIoT. These results are due to the efficient processing of information transmitted and received between IoT devices based on blockchain and probability theory. Furthermore, the proposed technique has weighted the IoT information to distribute the blockchain of n bits in the n+1 and n-1 layers out of numerous IoT information in two directions.

**Table 3.** TRANSACTION NUMBER OF AIoT  
UNITS: PROCESS NUMBER/SECOND

Method	Response of IoT			
	1	2	5	10
Not using AIoT	2.19	5.37	9.41	14.52
Using AIoT	8.63	14.42	19.63	24.38

(A) RESPONSE BY IoT DEVICE COUNT

UNITS: PROCESS NUMBER/SECOND

Method	Response of IoT			
	1	2	5	10
Not using AIoT	5.74	8.61	14.68	17.46
Using AIoT	11.13	15.74	22.69	31.21

(B) REQUEST COUNT BY IoT DEVICE COUNT

Table 4 results from evaluating the rate of asymmetric processing according to the hash code length of IoT information to asymmetrically process information generated by different heterogeneous IoT devices. In Table 4, we obtain an average 16.2% improvement over the case with AIoT. These results are a result of deep learning to load balance each

information after asymmetric hash processing of the information collected in AIoT. In particular, the proposed technique has improved asymmetric storage rates according to hash code paths because it load-balances the asymmetric processing of IoT information.

**Table 4.** IoT INFORMATION PROCESSING SPEED BY HASH LENGTH

Method	Response of IoT			
	16	32	64	128
Not using AIoT	0.585	0.602	0.631	0.675
Using AIoT	0.298	0.322	0.385	0.438

UNITS: MS

## V. CONCLUSION

Recently, application services using IoT have been increasing as IoT devices have been used in various fields. As IoT devices are widely used in everyday life, various studies that can improve convenience and usefulness based on information collected from IoT devices have begun to create problems for IoT devices (network traffic, processing latency, server overhead, security, etc.).

In this paper, we propose an AIoT processing technique that allows information collected from IoT devices to be preprocessed from AIoT devices and then send critical data to servers (data centers) in blockchain form. The proposed technique is characterized by minimizing network traffic and network delays that can occur when information collected from numerous IoT devices is delivered to the server (data center). The proposed technique controlled device operation by analyzing patterns of information collected from IoT devices and made it easy to utilize for other application services through data analysis using artificial intelligence technologies such as deep learning.

Performance evaluation, an average 8.4% improvement was achieved when processing the linked information code of IoT information using AIoT than otherwise. Furthermore, the proposed technique achieves an average 2.34x improvement over the case with AIoT.

Based on this study, the future study plans to apply experimental figures to various environments to various services to conduct evaluations of performance differences in real-world environments.

## REFERENCES

- [1] Stankovic, J. A., Lee, I., Mok, A. & Rajkumar, R. (2005). Opportunities and obligations for physical computing systems. *Computer*, 38(11), 23-31.
- [2] Reyna A., Mart'ın C., Chen J., Soler E & D'ıaz M. (2018). On blockchain and its integration with IoT. challenges and opportunities, *Future Generation Computer Systems*. 88. 173–190.
- [3] Roman, R., Zhou, J. & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things, *Computer Networks*, 57(10), 2266-2279.
- [4] Xu, L. D., He, W. & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions Industrial Informatics*, 10(4), 2233-2243.
- [5] Liang, X., Zhao, J., Shetty, S. & Li, D. (2017). Towards data assurance and resilience in IoT using blockchain. *Proceedings of the IEEE Military Communications Conference*, 261–266.
- [6] Forooghifar, F., Aminifar, A. & Atienza, D. (2019). Resource-Aware Distributed Epilepsy Monitoring Using Self-Awareness From Edge to Cloud. *IEEE Transactions on Biomedical Circuits and Systems*, 13(6), 1338-1350.
- [7] Kang, Y., Hauswald, J., Gao, C., Rovinski, A., Mudge, T. N., Mars, J. & Tang, L. (2017). Neurosurgeon: Collaborative intelligence between the cloud and mobile edge. *Proceedings of International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 615-629.
- [8] Zhao, Z., Zhao, R., Xia, J., Lei, X., Li, D., Yuen, C. & Fan, L. (2020). A Novel Framework of Three-Hierarchical Offloading Optimization for MEC in Industrial IoT Networks. *IEEE Transactions on Industrial Informatics (TII)*, 16(8), 5424-5434.
- [9] Yang, B., Cao, X., Yuen, C. & Qian, L. (2020). Offloading Optimization in Edge Computing for Deep Learning Enabled Target Tracking by Internet-of UAVs. *IEEE Internet of Things Journal(Early Access)*, 1-1.
- [10] Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T. & Chan, K. (2019). Adaptive Federated Learning in Resource Constrained Edge Computing Systems. *IEEE Journal of Selected Areas in Communications (JSAC)*, 37(6), 1205-1221.
- [11] Mills, J., Hu, J. & Min, G. (2020). Communication-Efficient Federated Learning for Wireless Edge Intelligence in IoT. *IEEE Internet of Things Journal (IoTJ)*, 7(7), 5986-5994.
- [12] Fıgurnov, M., Collins, M. D., Zhu, Y., Zhang, L., Huang, J., Vetrov, D. P. & Salakhutdinov, R. (2017). Spatially adaptive computation time for residual networks. *Proceedings of Conference on Computer Vision and Pattern Recognition (CVPR)*, 1790-1799.
- [13] Bolukbasi, T., Wang, J., Dekel, O. & Saligrama, V. (2017). Adaptive neural networks for efficient inference. *Proceedings of International Conference on Machine Learning (ICML)*, 527-536.
- [14] Teerapittayanon, S., McDanel, B. & Kung, H. T. (2017). Distributed Deep Neural Networks Over the Cloud, the Edge and End Devices. *Proceedings of International Conference on Distributed Computing Systems (ICDCS)*, 328-339.
- [15] Volodymyr, M., Koray, K., David, S., Andrei, A. R., Joel, V., Marc, G. B., Alex, G., Martin, R., Andreas, K. F., Georg, O., Stig, P., Charles, B., Amir, S., Ioannis, A., Helen, K., Dharshan, K., Daan, W., Shane, L & Demis, H. (2015). Human-level control through deep reinforcement learning, *Nature*, 518.7540, 529-533.