IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2020, accepted April 21, 2020, date of publication April 29, 2020, date of current version May 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2991273

Intelligent Application Protection Mechanism for Transportation in V2C Environment

HYUNJIN KIM[1], SANG HONG[2], JINSUL KIM[3], (Member, IEEE), AND JAECHEOL RYOU[1]
[1]Department of Computer Engineering, Chungnam National University, Daejeon 34134, South Korea
[2]Department of Computer Science, School of Business, Saint Leo University, St Leo, FL 33574, USA
[3]School of Electronics and Computer Engineering, Chonnam National University, Gwangju 61186, South Korea

Corresponding author: Jaecheol Ryou (jcryou@cnu.ac.kr)

This work was supported by the Research Fund of Chungnam National University.

ABSTRACT The emergence of vehicle-to-cloud (V2C) technology is changing cloud computing and transportation ecosystems. V2C technology enables the development of smart services, such as driving assistance and vehicle maintenance, that transmit information to the driver. Recent studies have primarily focused on services. To date, there has not been sufficient research on security functions to detect abnormal behaviors on virtual application. If an abnormal behavior occurs in the application, the service not only notices the wrong information to driver, but also affects the transportation system around the vehicle. To defend against distributed denial of service (DDoS) attacks, system resources should be monitored constantly. However, continuous monitoring is difficult because V2C services change dynamically according to the service environment. In addition, rule-based or supervised monitoring is impossible for each of the numerous services provided by a cloud computing center. In this paper, we propose an intelligent application protection mechanism for smart vehicle services in a V2C environment that detects abnormal behavior through image-based system resource monitoring using artificial intelligence (ISRM-AI) to improve cloud vehicle service security. The ISRM-AI generates images about system information such as CPU, network, memory on V2C cloud services. Also, the mechanism analyzes the status using a convolutional neural network (CNN) to detect abnormal behavior of the each services. We constructed a service environment to test the performance of the proposed mechanism. In addition, we simulated the proposed mechanism's ability to detect DDoS attacks using real attack data. The proposed mechanism guarantees the reliability of a smart service by enhancing the security of the V2C environment.

INDEX TERMS Vehicle to cloud, V2C service, cloud computing, detection mechanism, transportation, artificial intelligence.

I. INTRODUCTION

Cloud computing has been used to reduce capital and operational expenditures using a logical network. Recent interest in virtualization technology and services based on cloud computing is increasing because virtualization technology can quickly adapt to changing service environments by creating logical networks without forming physical networks. Cloud services are customized to provide a cost-effective solution for multiple tenants in a cloud environment [1]. Moreover, multi-tenant cloud architecture facilitates a single instance of the software and its supporting infrastructure can serve multiple users. Each service shares the same software application as well as the same database and applications. The data in the database are isolated and remain invisible to other tenants.

Continuing research on virtualization technology has led to considerable advances in next-generation network core technology and network function virtualization (NFV), which decouples network function from the network hardware. Additionally, NFV can provide scalability and flexibility to achieve optimal performance [2]. Therefore, internet of things (IoT) infrastructure can be lightweight using NFV technology. A system using NFV technology utilizes resources dynamically and efficiently to satisfy users in virtualized space [3, 4]. This advantage allows cloud services

The associate editor coordinating the review of this manuscript and approving it for publication was Dalin Zhang.

to combine microservices to create additional services. With the widespread penetration of NFV into vehicular services, microservices have moved from simple infrastructure environments to our lives. Apart from the amount of time spent at home and work, one spends a considerable amount of time commuting by vehicle. NFV allows a vehicle to develop advanced vehicle-to-cloud (V2C) services. V2C communication enables the exchange of information about various applications, such as driving assistance, entertainment, and vehicle maintenance. Although cloud systems are typically associated with large-scale industries, such as energy, transportation, and the smart home industry, V2C services allow a private vehicle to use information from other vehicles. V2C infrastructure not only offers better processing power and storage capabilities but also reduces the amount of existing in-car hardware and software and paves the way for a new range of services. However, V2C services must guarantee security functions that can detect abnormal service behaviors and entities.

If a malicious V2C service employed a botnet to perform abnormal behaviors, such as a distributed denial of service (DDoS) attack, many transportation services in the same tenant and cloud service user will be out of service. Then, the service not only provides wrong information to driver but also affects the transportation system around the vehicle. Therefore, to prevent such attacks, a mechanism to monitor system resources is important because the objective of a DDoS attack is resource exhaustion. Each V2C service in the tenant requires a security mechanism to prevent the spread of contamination from an infected V2C service. Therefore, monitoring V2C services and detecting attacks should be considered in the V2C environment, and a security mechanism is essential to ensure reliability in a cloud environment. However, detecting DDoS attacks is difficult because the cloud service environment is complex and can change dynamically. Moreover, it should be easy for administrator to detect abnormal behavior occurring in services. In this paper, we propose an intelligent application protection mechanism for smart vehicle service in a V2C environment that monitors each cloud service and can detect DDoS attacks. The proposed image-based system of resource monitoring using AI (ISRM-AI) generates images related to system information, including the CPU, network, and memory, on V2C cloud services. It also analyzes the system status using a CNN to detect abnormal behavior of each service. Unlike the conventional method of using neural networks by applying a preprocessing technique, such as the arrangement of data, in the proposed system, neural networks are used to classify the system status using images of cloud services only. Therefore, the proposed mechanism investigates changes to information using image models to detect abnormalities in services.

The remainder of this paper is organized as follows. In Section 2, we discuss concepts related to V2C services, abnormal behavior, and DDoS detection using artificial intelligence (AI). In Section 3, we describe the proposed ISRM-AI and subsystems. In Section 4, we simulate the performance of cloud services' abnormal behavior, such as operation overhead and detection error rate. Finally, we present conclusions and suggestions for future work in Section 5.

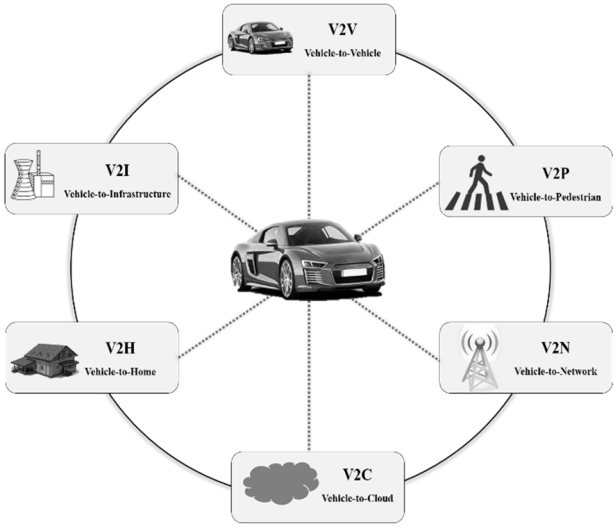

FIGURE 1. Types of V2X services.

II. RELATED WORK

A. VEHICLE-TO-CLOUD

Vehicle-to-everything (V2X) is vehicular communication that transmits information from a vehicle to any entity that may affect the vehicle and vice versa, as shown in Fig. 1. V2X includes to vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), vehicle-to-home (V2H), and vehicle-to-network/cloud (V2N/V2C) network connections [5].

Previous studies have investigated transferring vehicle data to the cloud for evaluation. Interest in V2C technology, whereby a vehicle is linked to various services, is increasing. V2C technology can help vehicles obtain various types of information, such as infotainment, and driving assistance. In addition, V2C technology supports location services, such as local dynamic map (LDM) services. LDM service involves a conceptual database to manage dynamic vehicle sensor data and static map data and to provide local traffic control, real-time road status notification, and on-board diagnostic services [6]. As the name implies, vehicular infotainment services combine driver entertainment and information services, such as intelligent personal assistance, media streaming, and vehicle maintenance. Driving assistance services help drivers with regard to safety and improved driving behavior, e.g., detecting abnormal driving operations, predicting driving behavior, and emergency handling services. In addition, driving assistance services can contribute to building intelligent transport systems, such as automated driving systems.

In other words, V2C technologies can improve traffic efficiency, reduce incidents of accidents, and improve traffic management [7]. To create these services, the virtualized function combines microservices comprising the smallest

unit of software and employs scale-up, scale-down, scale-in, and scale-out functions [8]. In the field of networks, virtualization

technology utilizes resources dynamically and efficiently to deliver satisfactory results to users.

However, V2C networks face various threats that can reduce performance. V2C application services are vulnerable to hackers due to low development thresholds and easy accessibility. Cloud service platforms not only face the problems associated with traditional network cloud platforms but also have problems caused by the principle of mutual trust, such as abnormal behaviors. Therefore, to advance V2C technology, security functions that can detect abnormal behavior of cloud services should be investigated.

B. ABNORMAL BEHAVIOR

Cloud computing is vulnerable to various security threats, such as denial of service (DoS) and DDoS attacks. Such attacks employ various means to flood a targeted system with traffic, thereby exhausting network and service resources [9], [10], [11]. For example, DoS and DDoS attacks cause high network communication latency, as well as network and node service unavailability [9]. There are Dos attacks such as jamming, tempering, and greedy. A jamming attack is an attack on the physical layer. The attacker jams the wireless communication channel using a jammer comprising electromagnetic interference, which increases V2X communication latency and reduces network reliability.

Bandwidth and resource consumption attacks and application attacks are representative types of DDoS attacks [12], [13]. In bandwidth consumption attacks, the attacker controls many zombie computers that generate a sufficiently large number of packets and to exceed network bandwidth capacity [14]. In particular, bandwidth consumption attacks cause connection failures to other systems in the same network. UDP and ICMP flooding are typical bandwidth consumption attacks [15], [16]. In resource consumption attacks, the attacker increases the CPU load by increasing the packet throughput using the TCP. Rather than increasing bps, resource consumption attacks generate system overhead by increasing the packet per second (pps) rate. A SYN packet flooding attack is a representative resource consumption attack [17]. Finally, in application attacks, the attacker generates a disorder of system services through excessive application accesses. For example, the Slowloris DDoS attack is a representative application attack [18]. Here, the attacker employs the HCCP CC method to interrupt cache use by the system and HTTP GET flooding, where a large number of HTTP GET messages are generated [19].

The NFV environment is a virtual environment; thus, attackers load multiple services in the tenant. Therefore, using this characteristic, attackers cause bandwidth exhaustion attacks that deplete the virtual network bandwidth in the network and can paralyze entire networks. In other words, if an attacker makes a botnet with a service in a tenant, the botnet infects and paralyzes all services. It is possible to detect such abnormal behaviors by continuously monitoring the service's CPU utilization, network I/O, and memory map changes.

C. DDoS DETECTION-BASED AI

DDoS detection and mitigation have been studied in industry for several years. The related literature reveals that several studies have proposed solutions to address with DDoS detection and mitigation in a general manner.

AI requires a long learning time; however, we can determine whether various input traffic patterns are an attack. In other words, deep learning has led to advances in learning the deep hidden features in many artificial intelligence processes, such as bots and digital assistance, cognitive computing, object recognition, and text mining [20]. Neural networks have the advantage of multilayer features in computer vision tasks and abnormal behavior detection [21], [22]. In some studies, deep learning models based on CNNs that use pattern recognition in training datasets consisting of raw data have been constructed [23], [24]. CNNs can also be used to learn mappings from image pixels to 3D coordinates [25]. This technique detects abnormal traffic patterns from large amounts of data and identifies attacks in these patterns. We determine abnormal traffic with services in the virtual environment. DDoS attacks are difficult to defense from network attacks and are the most extensive and dangerous type of attack. A new type of DDoS attack, i.e., the distributed reflector denial of service (DRDoS), has appeared in recent years. It is more dangerous than traditional DDoS attacks because it has more effective disguise mechanics [26]. DRDoS is an attack based on traffic reflection and amplification. This kind of attack uses the nodes that generate requests to replace the source IP address with the IP address of the attacked host. These requests are sent to servers or other devices that can be used to reflect network traffic. The replies to these requests are sent to the target node. The traffic reflection mechanism increases the complexity of identifying the real source of the attack. When DRDoS attacks occur, network traffic patterns are analyzed by fuzzy association rules with path restriction. The DRDoS attacks' defensive architecture based on multi-agent (DAMA) is set up to realize the detection, orientation, and defensive function [27]. DAMA is validated using network simulator 2 (NS-2) platform to quickly detect the attack source, screen the attack source, and stop transmitting attack traffic. However, the detection mechanism is difficult to adopt in complicated and dynamic virtual network environments. Moreover, the real environment is different from the NS-2 platform. In addition, V2C services change dynamically according to the service environment.

Therefore, it is difficult for a service administrator to detect DDoS attacks. Thus, we propose a DDoS detection mechanism that uses image-based system resource monitoring. The proposed ISRM-AI method detects abnormal behaviors in services for V2C services by analyzing various system information, e.g., CPU utilization, network I/O, and memory, using a convolutional neural network (CNN).

TABLE 1. Service data information.

Field	Contents
CPU_util	CPU utilization
Memory_Info	memory Usage
Network_Input	network Input
Network_Output	network Output
Service_ID	service ID for monitoring
Image_Info	graph image for cpu, network, memory
Extensions	Reserved field

III. IMAGE-BASED SYSTEM RESOURCE MONITORING SYSTEM USING ARTIFICIAL INTELLIGENCE

The proposed ISRM-AI comprises an image unification (IMU) subsystem and CNN-based attack detection (CAD). The goal of DDoS attacks is to disable a service by exhausting system resources, e.g., CPU utilization, network I/O, and memory changes. Therefore, we investigate changes to information using image models to detect abnormal services.

Figure 2-(A) shows the IMU subsystem used to unify graph images of CPU utilization, network I/O, and memory changes in cloud services, and Fig. 1-(B) shows the CAD system to identify DDoS attacks.

A. IMAGE UNIFICATION SUBSYSTEM

The IMU of ISRM-AI comprises a monitoring agent for service CPU utilization, network I/O, and memory changes, as well as an image preprocessing module to collect an image of the service's current status and the unification module. Table 1 shows the parameters of the IMU process.

Here, "*CPU_util*," "*Memory_Info*," "*Network_Input*," and "*Network_Output*" are the information used to check the system status, and "*Service_ID*" is the service ID for monitoring.

The information change image is a one-dimensional graph. Here, "*Image_info*" represents a set of unified images based on information. One image comprises graphs of CPU utilization and memory information, and the other image represents network I/O information. After image generation, the IMU transmits the graph images to the CAD subsystem.

In the process shown in Fig. 3-(1), the cloud services in the tenant transmit their current status, e.g., CPU utilization, network I/O, and memory changes, to the monitoring agent. Here, we employ a monitoring client and server configuration. In addition, the information is stored in a database to generate the graph images.

In Fig. 3-(2), the image preprocessing module generates graph images using raw information about the cloud services. This process uses computer algorithm to perform image processing on digital image. It allows a much wider range of algorithms to be applied to the input data. In Fig. 3-(3), the IMU module unifies three sets of information to multidimensional images. This module converts color images to gray scale to reduce computation complexity before executing the abnormal behavior detection process. Moreover, the module improves the appearance of the image to recognition rate. The images are shown as below.

The IMU transmits the CPU utilization and memory usage and network I/O graphs to the CAD subsystem to detect an attack.

TABLE 2. Parameters of convolution equation.

Parameter	Contents
X	unified image
F	image filter
F_H	height of the filter 'F'
F_W	width Reserved field

B. CNN-BASED ATTACK DETECTION

In the proposed of ISRM-AI method, the CAD comprises an attack detection module subsystem. In addition, the learning, validation, and detection module comprises a CAD subsystem.

As shown in Fig. 6-(1), the CAD receives unification images from the IMU subsystem. Here, the normalization module resizes the image to a unified dimension and removes the image to enhance attack detection accuracy. The images with unified dimension are processed and scaled to identical widths and heights prior to applying the algorithm.

The CAD trains the detection model using a training dataset of images with unified dimension. After generating images of unified dimension, the images are transmitted to the learning module (Fig. 6-(2)). The module is trained using CNN with a multilayer perceptron, which is commonly applied in visual imagery analysis. The CNN consists of a convolutional pooling layer that extracts features from data and a fully connected layer that performs classification based on the extracted features.

The CAD process involves feature extraction, shift and distortion invariance, and classification. For feature extraction, a received image is abstracted to a feature map with shape including the number of images, feature map width, feature map height, and feature map channels. Table 2 shows the parameters of the convolution equation.

The hundreds of layers that make up a CNN can be trained to detect different characteristics of the images. The equation for the convolution process is given as follows.

$$C_{ij} = F(i) * X(j) = \sum_{m=0}^{F_H-1} \sum_{n=0}^{F_W-1} X(i-m)\,(\text{j-n})\,F(m,n) \quad (1)$$

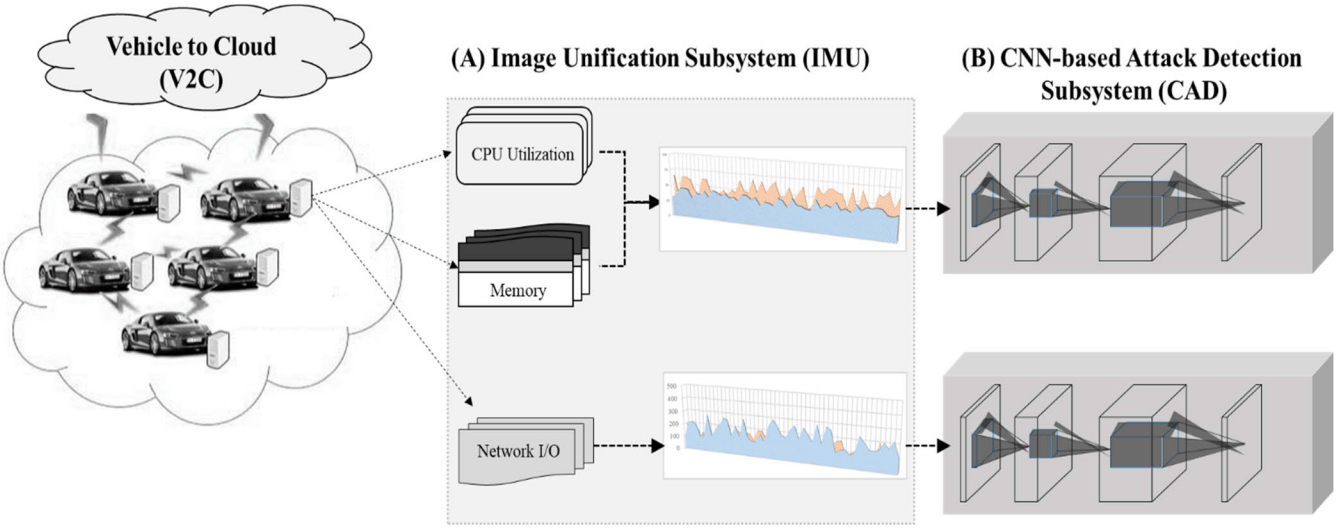

FIGURE 2. ISRM-AI architecture.

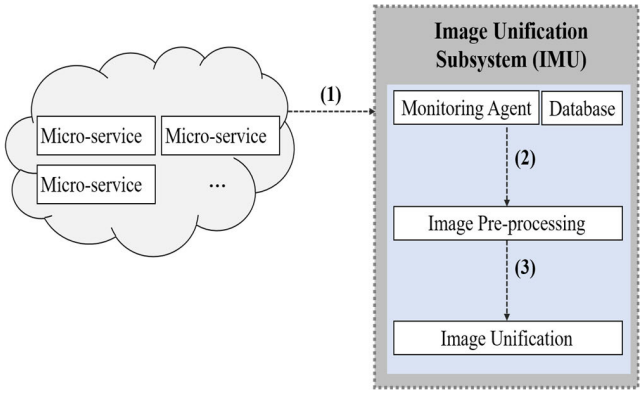

FIGURE 3. V2C service unification process.

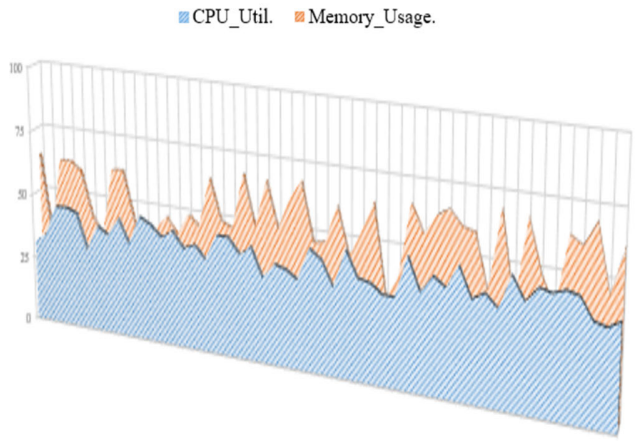

FIGURE 4. The CPU utilization and memory usage of service.

The training image can be represented as a matrix. Here, the i-th row and j-th column of the image are calculated as the convolution of the original image X and filter F.

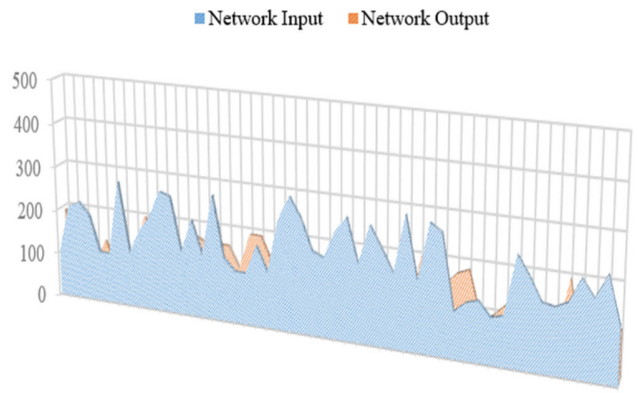

FIGURE 5. Network I/O traffic of service.

The filter is applied at different resolutions to each training image, and the output of the filter is used as the input to the next layer. Filters can begin with very simple features, e.g., brightness and edges, and develop more complexly to object's unique feature. The convolution operation reduces the number of hyper-parameters, which allows a deeper network with fewer parameters to be produced. In this process, the optimization algorithm minimizes the error function, which is a function dependent on the learning parameters of the model used in computing the prediction. The learnable parameters, such as weight and bias, are learned and updated in the direction of the optimal solution in the neural network.

In addition, the model must be evaluated periodically using the validation process shown in Fig. 6-(3). In the process, the model enhances the accuracy by calculating loss, e.g., error rate. The output layer back propagates to backward. The backpropagation equation is given as follows.

$$\frac{\partial E}{\partial w} = \frac{\partial E}{\partial x}\frac{\partial x}{\partial s}\frac{\partial s}{\partial w} \tag{2}$$

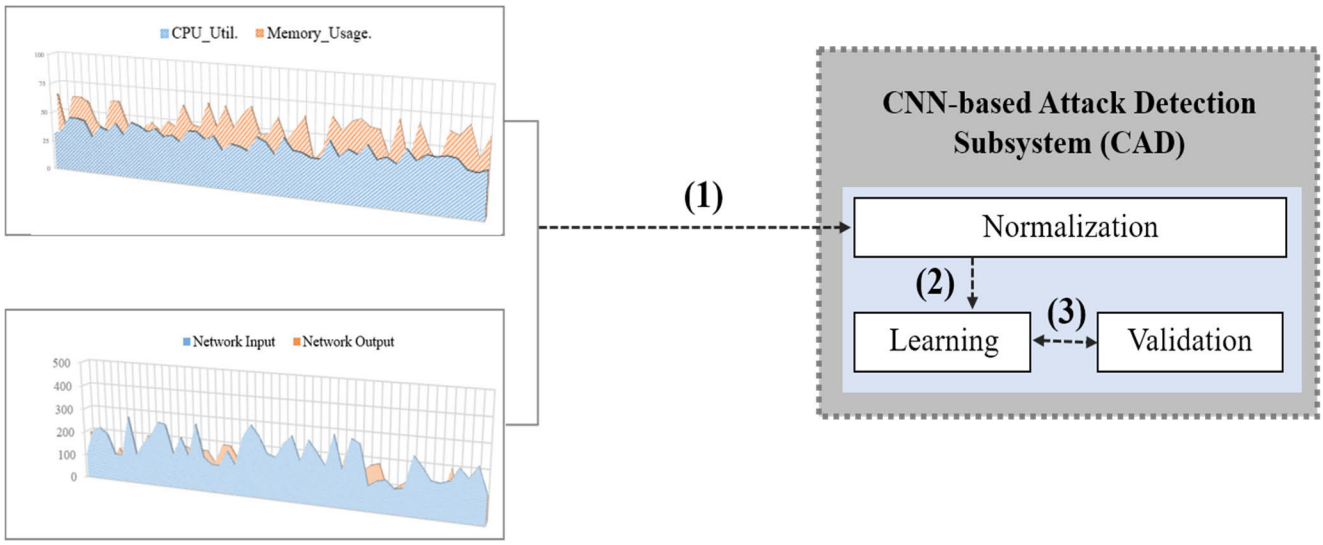

FIGURE 6. CNN-based attack detection process.

To calculate the degree to which weight w should change for the error value for the output x. For shifting and distortion invariance, the pooling layers reduce the dimensionality. The pooling layers down-sample each feature map independently, thereby reducing the height and width. The activation functions and the pooling layer enhance the nonlinear learning ability of the network. In the model, the dropout operation is used to reduce overfitting in neural networks by preventing complex co-adaptations of the training data. By dropping a unit, the model temporarily removes the unit from the network along with all its incoming and outgoing connections.

The following is the pseudo-code used for the validation and updating process.

The learning and validation processes are repeated to reconfigure the learning parameters based on the frequent evaluation results obtained on the validation set. To validate the classifier, the CAD sorts the misclassified data using the validation dataset D_{Val}. The error labed set is included the training dataset D_{Train}. The D_{Error} is excluded from D_{Train}. As a result of the validation process, the classifier is updated and the accuracy of the abnormal behavior detection is enhanced. Finally, the detection model for DDoS is generated, and we detect attacks using the CNN.

Algorithm The Validation & Update Process of CNN based Attack Detection Model

Training Process
Train a CNN classifier with the labeled training dataset D_{Train}
Abnormal labeled set $X = \{x_1, x_2, \ldots, x_m\}$, m is the total number of services
Normal labeled set $Y = \{y_1, y_2, \ldots, y_n\}$, n is the total number of services
CNN $\leftarrow$ X,Y

Validation Process
do{
Validate the resulting classifier with the validation dataset D_{Val}
Sort misclassifed examples by false positives
Select the misclassified examples as error- labeled set D_{Error}
Update datasets
$D_{Train} = D_{Train} \cup D_{Error}$
$D_{Val} = D_{Val}$ - D_{Error}
}
While(D_{Test} ! = { } && D_{Error} != { })

Testing Process
Test the resulting classifer using D_{Test}

IV. IMPLEMENTATION AND PERFORMANCE

In this section, we analyze the performance of the proposed ISRM-AI method. For performance of ISRM-AI, we classify experiments by overhead on host system and detection performance. Three tenants were used in the experiment, and there were 10 VMs in each tenant. To execute the proposed ISRM-AI with the CNN, a host system allocated graphics processing units (GPU) 8118 MB. In addition, we set one service for each VM and allocated one CPU and 2 GB of memory. Further, we used Zabbix agent and server to monitor the state of cloud services on the host system. The network topology is illustrated in Fig. 7.

A. SYSTEM OVERHEAD

We implemented tests to analyze the overhead of the protection mechanism. In the test, we analyzed the system

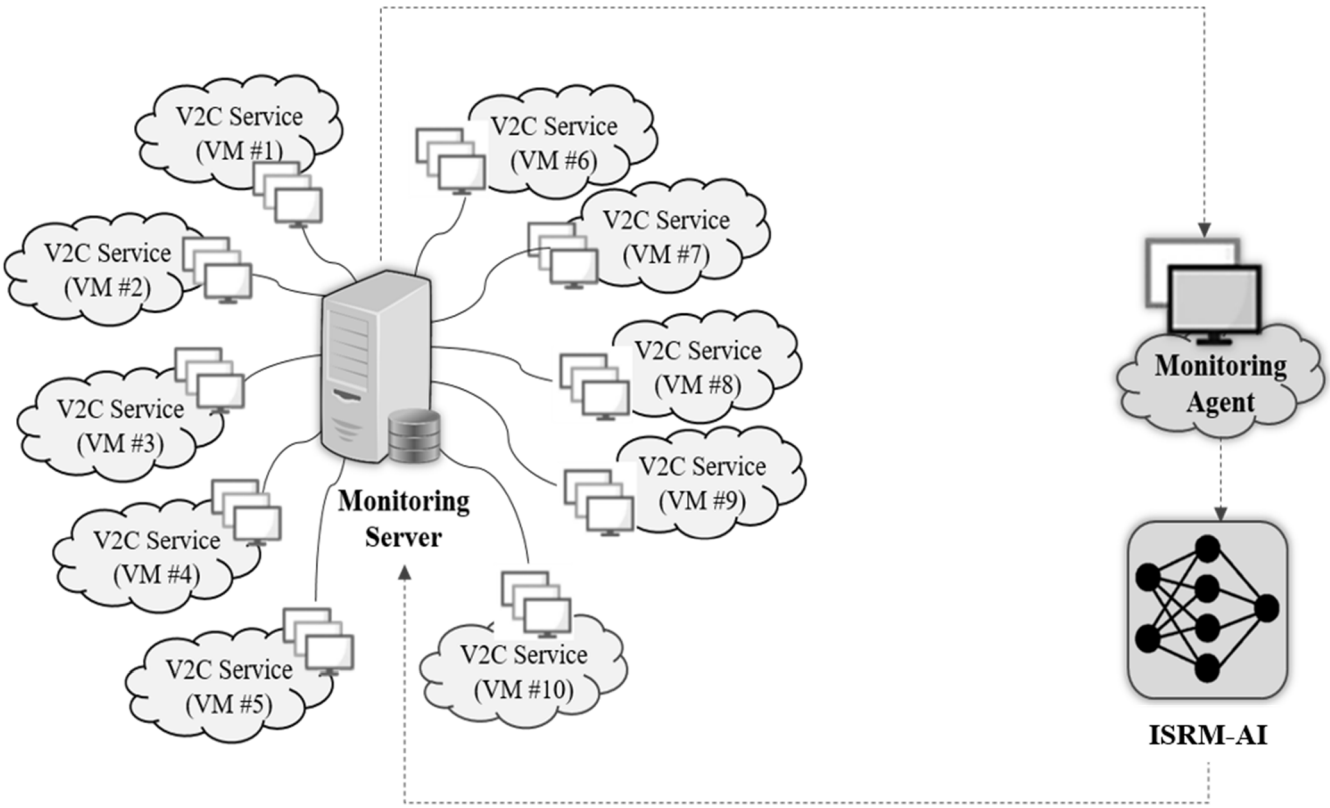

FIGURE 7. Topology for ISRM-AI performance evaluation.

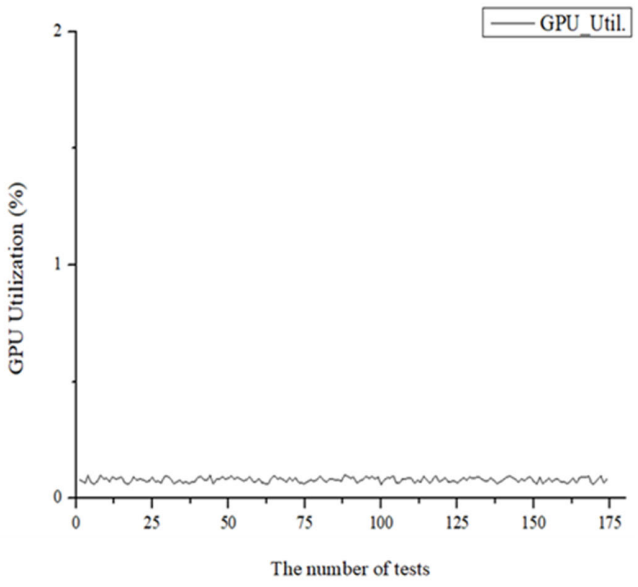

FIGURE 8. GPU utilization for ISRM-AI on host system.

resources of the host system on which the proposed ISRM-AI was applied to the service. The first experiment compared the detection rate for a DDoS attack in a service environment, and the second experiment compared the time required to detect a DDoS attack with 50 and 100 services in a tenant.

TABLE 3. Input traffic.

ICMP Traffic	SYN Traffic	UDP Traffic
74 bytes~1000 bytes	1500 bytes	74 bytes~1000 bytes

A shown in Fig. 8, GPU utilization increased by less than 0.2% compared with 15–20 MB in total when ISRM-AI was operating. The proposed ISRM-AI should be directly proportional to the number of cloud services in the tenant. The DDM-AI simply classifies whether the system status image is normal or abnormal caused by DDoS.

Therefore, because the host system has increased within 0.2%, we confirm that there is no performance degradation on the host system owing to the ISRM-AI.

In addition, we analyzed the time required to detect an attack on services in a tenant. The results are shown in Fig. 9.

Figure 9 shows that the average time required to detect an attack was 903 ms on 50 services and 1,517 ms on 100 services. The time required to detect an attack depends on the number of virtual services in the tenant, and the detection time increased as the number of virtual services in the tenant also increased. Therefore, we confirm that the proposed method

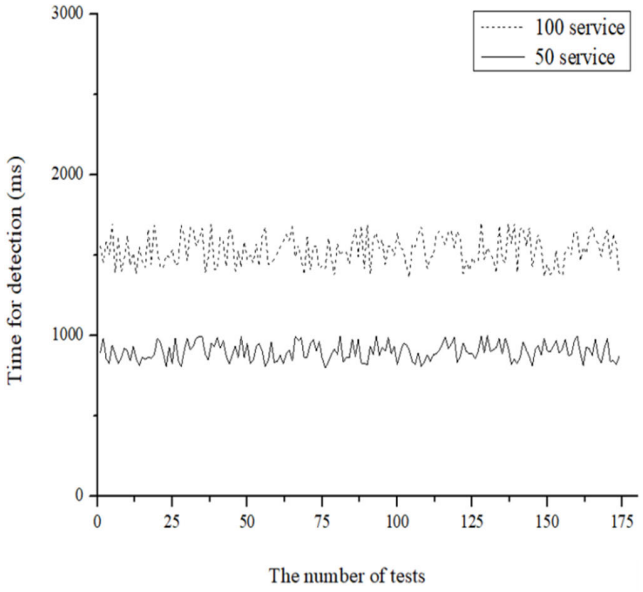

FIGURE 9. Time to detect attack with 50 and 100 services in one group.

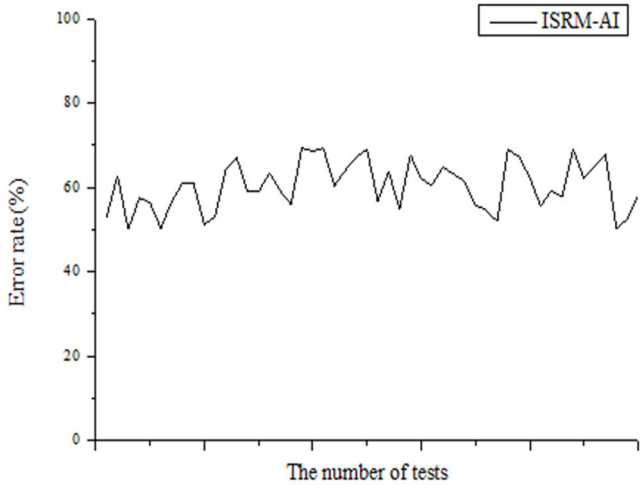

FIGURE 10. Error rate for detecting attack using CPU utilization.

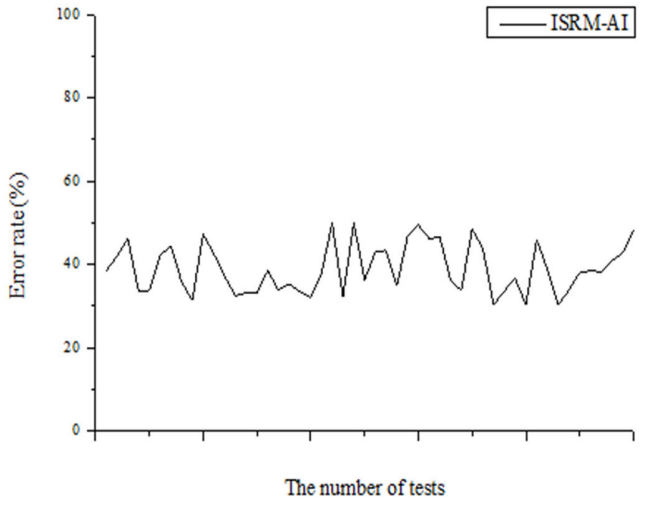

FIGURE 11. Error rate for detecting attack using memory usage.

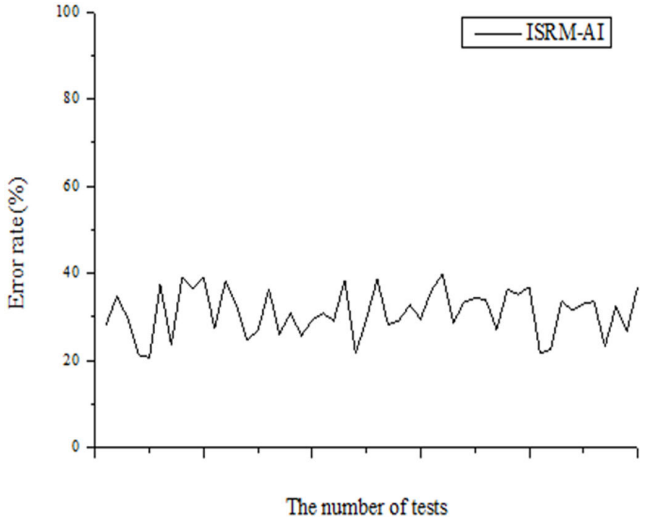

FIGURE 12. Error rate for detecting attack using network I/O.

incurs no performance degradation and no overhead on the host system.

B. EVALUATION OF DDoS DETECTION USING ISRM-AI

We performed tests to analyze the proposed method's attack detection performance using system information.

On 2009, important sites of national agency in United States, South Korea were the targets of attacks. These attacks are referred to as the 7.7 DDoS attacks. This attack was based on many well-known DDoS attack methods and targeted 25 popular sites. High-rate attacks use ICMP and/or UDP flooding to waste network resources. Because a single flow carries a large amount of data, the byte and flow counts are correlated. However, in low-rate attacks, the data rate in a single flow is low and each attack packet is a unique flow.

We generated the attack traffic as simulation data from the 7.7 DDoS attacks [28]. The protocols of the attack traffic are ICMP, SYN, and UDP. The network speed (bps) is up to 200 Kbps, and pps is up to 3 Kpps. The input attack traffic used in the test is detailed in Table 3.

Then, we analyzed the proposed ISRM-AI method's DDoS attack detection performance. We performed three detection experiments using only one information, i.e., memory usage, network I/O, CPU utilization. The results of detection performance analysis using memory usage are described in the following.

Figure 10 shows that the false positive rate was approximately 60.387%. Thus, we confirm that detection performance is not outstanding. The results of analyzing detection performance using CPU utilization are summarized as follows.

Figure 11 shows that the false positive rate was approximately 38.99%. Thus, we discovered that the detection rate

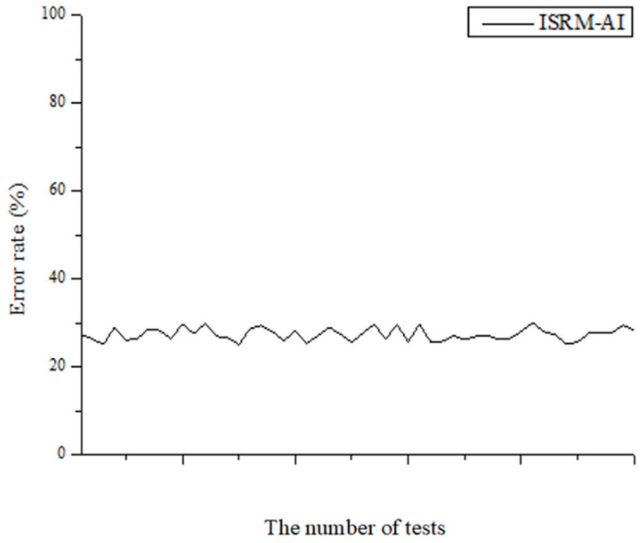

FIGURE 13. Error rate for detecting attack using memory usage and network I/O.

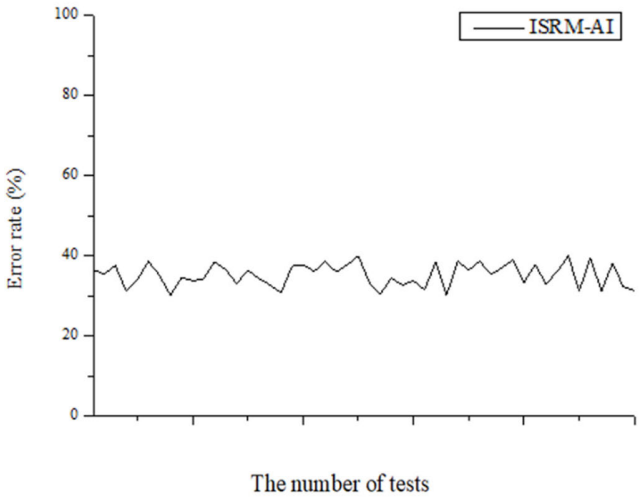

FIGURE 14. Error rate for detecting attack using CPU utilization and network I/O.

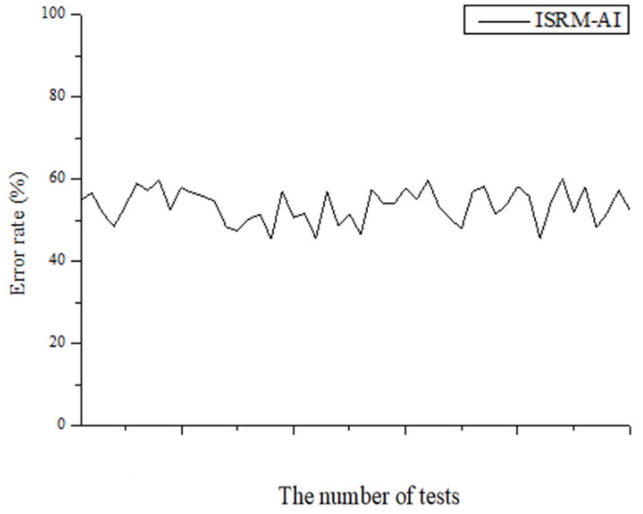

FIGURE 15. Error rate for detecting attack using CPU utilization and memory usage.

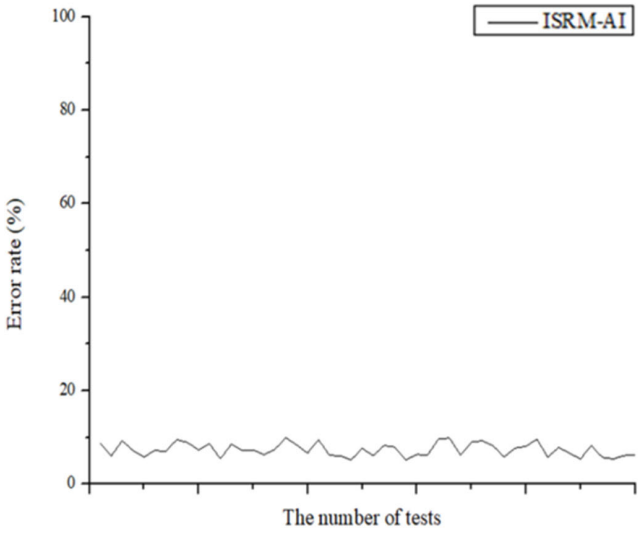

FIGURE 16. Error rate for detecting attack using CPU utilization, memory usage, and network IO.

of the test using memory usage was better than when using CPU utilization.

Figure 12 shows that the false positive rate was approximately 31.041%. We confirmed that the detection rate of the test using network I/O is the best of the three experiments.

We also performed three detection experiments using two types of information: memory usage and network I/O, CPU utilization and network I/O, and CPU utilization and memory usage. The results of the analysis of the detection performance of the experiment that used memory usage and network I/O are described in the following.

Figure 13 shows that the false positive rate was approximately 35.162%. This confirms that the detection performance was not outstanding. The corresponding results for the performance of the detection using CPU utilization and network I/O are summarized below.

Figure 14 shows that the false positive rate was approximately 27.329%. We discovered that the detection rate of the test using CPU utilization and network I/O was better than when using memory usage and network I/O. The results of analysis of detection performance using CPU utilization and memory usage are summarized as follows.

Figure 15 shows that the error rate of attack detection was approximately 53.411%. In the three experiments using sets of two information on system have high error rate on DDoS detection because the DDoS packets comprise various protocol, e.g., ICMP, TCP, and UDP. Finally, we analyzed the detection performance of the proposed ISRM-AI method using CPU utilization, memory usage, and network I/O.

As shown in Fig. 16, the error rate of detecting an attack was approximately 7.36%. Thus, using three sets of information yielded significantly higher accuracy compared to

the previous three experiments with two sets of information. Therefore, we confirm that the proposed ISRM-AI method with three sets of system information is effective for detecting various protocol-based DDoS attacks. As a result, the collaboration with CPU utilization, network I/O, memory information is necessary for DDoS.

V. CONCLUSION

With the emergence of widespread NFV penetration in to vehicle, V2C technique exchanges information about applications of the vehicle such as driving assistance, entertainment, and vehicle maintenance. These services related to transportation allow the vehicle to use information from other vehicles, though the cloud systems are connected with industries such as energy, transportation, and smart homes. However, in order to use the cloud service in V2C, it needs to guarantee security functions for the detection of abnormal service and DDoS. If a malicious V2C service polluted a botnet for DDoS, many of the services in the same tenant and the subscriber can be out of service.

However, detecting DDoS attacks is difficult because the cloud service environment is complex and can change dynamically. In addition, it should be easy for administrator to detect the abnormal behavior that occur in the services.

Therefore, we have proposed a DDoS detection method that uses an image-based system resource monitoring with AI for V2C environments. In the proposed ISRM-AI, the IMU monitors the system status and generates a multidimensional graph image. In the CAD process, the detection model is trained using the multidimensional image generated by the IMU. The image is processed to npy value. Then, the mechanism detects that the system is in an abnormal state using a CNN. To evaluate the performance of the proposed ISRM-AI in a V2C environment, we analyzed the overhead on the host system and attack detection performance. For distinguishing the normal and abnormal state, we verified the performance of this mechanism by evaluating its performance using a DDoS attack similar to the one that occurred in Korea and the USA on July 7th, 2009. Becaues this DDoS attack is representative attack caused by the lack of collaborative between network and security device. The simulation results demonstrated that GPU utilization for the host system was 0.2%, and the detection error rate was 7.36%. In addition, the time required to detect an attack was 903 ms with 50 services and 1,517 ms for 100 services. Therefore, the proposed ISRM-AI guarantees the security for V2C services using AI. Therefore, we conclude that the results outperform in terms of security enhancement.

For future research, it is necessary to analyze the application of the proposed ISRM-AI. Especially, field experiments should be conducted with real-site data, establish the possible affecting factors and parameters to configure our proposal systematically. The second is necessary to objective experiments in real networks because DDoS detection mechanism is required various tests for the recent and actual situation. Lastly, the image-based detection technology requires the design and development of integrated detection system, after that its effect can be quantified and analyzed systematically. Thus, we consider that the proposed attack detection method for cloud services can be used to secure communication between V2C services and transportation system in a smart society.

REFERENCES

[1] *Network Functions Virtualisation (NFV); Management and Orchestration, the European Telecommunications Standards Institute (ETSI)*, ETSI Standard DGS/NFV-MAN001, Valbonne, France, 2014.
[2] H.-M. Yoon, Z. Liu, W.-S. Yang, J.-H. Kim, and J.-O. Lee, "A virtualized application service for QoS management," *Int. J. u- e- Service, Sci. Technol.*, vol. 10, no. 9, pp. 49–60, Sep. 2017.
[3] H. Zhang, F. Wang, J. Xu, and J. Guo, "Selection and configuration optimization for customizable cloud services," *Int. J. Signal Process., Image Process. Pattern Recognit.*, vol. 9, no. 4, pp. 443–454, Apr. 2016.
[4] D. R. Lopez, "Network functions virtualization: Beyond carrier-grade clouds," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, San Francisco, CA, USA, Mar. 2014, pp. 1–18.
[5] S. Rangarajan, M. Verma, A. Kannan, A. Sharma, and I. Schoen, "V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Aug. 2012, pp. 148–154.
[6] K. Kumar and P. D. Kaur, "A novel approach for congestion control in war state battle field using cloud sensor for collision detection and prevention," *Int. J. Signal Process., Image Process. Pattern Recognit.*, vol. 8, no. 8, pp. 11–20, Aug. 2015.
[7] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: A generic cloud computing model for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 96–102, Feb. 2015.
[8] A. Sheoran, P. Sharma, S. Fahmy, and V. Saxena, "Contain-ed: An NFV micro-service system for containing e2e latency," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 5, pp. 54–60, Oct. 2017.
[9] N. Singh and P. D. Kaur, "A hybrid approach for encrypting data on cloud to prevent DoS attacks," *Int. J. Database Theory Appl.*, vol. 8, no. 3, pp. 145–154, Jun. 2015.
[10] B. Mihir *et al.*, "Relations among notions of security for public-key encryption schemes," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 1462. 1998.
[11] K.-W. Park, J. Han, J. Chung, and K. H. Park, "THEMIS: A mutually verifiable billing system for the cloud computing environment," *IEEE Trans. Services Comput.*, vol. 6, no. 3, pp. 300–313, Jul. 2013.
[12] S. Acharya and N. Tiwari, "Survey of DDoS attacks based on TCP/IP protocol vulnerabilities," *IOSR J. Comput. Eng.*, vol. 18, no. 3, pp. 68–76, 2016.
[13] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-Centric Comput. Inf. Sci.*, vol. 7, no. 1, p. 6, Dec. 2017.
[14] R. Das, A. Karabade, and G. Tuna, "Common network attack types and defense mechanisms," in *Proc. 23nd Signal Process. Commun. Appl. Conf. (SIU)*, May 2015, pp. 658–661.
[15] S. M. Hussain and G. R. Beigh, "Impact of DDoS attack (UDP Flooding) on queuing models," in *Proc. 4th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Sep. 2013, pp 210-216,
[16] N. Gupta, A. Jain, P. Saini, and V. Gupta, "DDoS attack algorithm using ICMP flood," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 4082–4084.
[17] D. Moustis and P. Kotzanikolaou, "Evaluating security controls against HTTP-based DDoS attacks," in *Proc. 4th Int. Conf. Inf. Intell. Syst. Appl. (IISA)*, Jul. 2013, pp. 1–6.
[18] W. Chen and D.-Y. Yeung, "Defending against TCP SYN flooding attacks under different types of IP spoofing," in *Proc. Int. Conf. Netw., Int. Conf. Syst. Int. Conf. Mobile Commun. Learn. Technol. (ICNICONSMCL06)*, Apr. 2006, p. 38.
[19] F. Guenane, M. Nogueira, and A. Serhrouchni, "DDOS mitigation cloud-based service," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 1363–1368.

[20] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, "Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services," *IEEE Internet Things J.*, early access, Dec. 2, 2019, doi: 10.1109/JIOT.2019.2956827.
[21] J. Yu, M. Tan, H. Zhang, D. Tao, and Y. Rui, "Hierarchical deep click feature prediction for fine-grained image recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, early access, Jul. 30, 2019, doi: 10.1109/TPAMI.2019.2932058.
[22] J. Yu, J. Li, Z. Yu, and Q. Huang, "Multimodal transformer with multi-view visual representation for image captioning," *IEEE Trans. Circuits Syst. Video Technol.*, early access, Oct. 15, 2019, doi: 10.1109/TCSVT.2019.2947482.
[23] I. H. Seo, K.-T. Lee, J. Yu, and S. Kim, "CNN based real-time DNS DDoS attack detection system," *KIPS Trans. Comput. Commun. Syst.*, vol. 6, no. 3, pp. 135–142, Mar. 2017.
[24] J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1317–1332, May 2018.
[25] Y. Jin, X. Guo, Y. Li, J. Xing, and H. Tian, "Towards stabilizing facial landmark detection and tracking via hierarchical filtering: A new method," *J. Franklin Inst.*, vol. 357, no. 5, pp. 3019–3037, Mar. 2020.
[26] Y. Gao, Y. Feng, J. Kawamoto, and K. Sakurai, "A machine learning based approach for detecting DRDoS attacks and its performance evaluation," in *Proc. 11th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*, Aug. 2016, pp. 80–86.
[27] R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, "A DRDoS detection and defense method based on deep forest in the big data environment," *Symmetry*, vol. 11, no. 1, p. 78, 2019.
[28] S.-S. Seo, Y. J. Won, and J. W.-K. Hong, "Witnessing distributed denial-of-service traffic from an attacker's network," in *Proc. 7th Int. Conf. Netw. Service Manage.*, Oct. 2011, pp. 1–7.

HYUNJIN KIM received the B.S. degree in information communications engineering and the M.S. degree in computer science and engineering from Chungnam National University, South Korea, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree with the Department of Computer Engineering.

His research interests include aspects of information security, both theoretical and practical, network function virtualization security, cloud service security, and applied cryptography.

SANG HONG received the M.S. degree in computer and information science and engineering (CISE) from the University of Florida, Gainesville, FL, USA, in 2009, and the Ph.D. degree in computer science from The University of Texas at Dallas.

He worked as a Research Engineer with the Electronics and Telecom-Communications Research Institute (ETRI) which is Korea Government Research Institute. He also worked as a Software Engineer with Samsung Electronics and SKC&C. He is currently teaching basic computer skills, theoretical foundation of computer science, system analysis and design, system security, and advanced network protocols with Saint Leo University. His research interests include virtual optical network design in multi-domain optical networks, broad range of research problems related to virtual optical networks (VONs) over flexible-grid multi-domain optical networks, such as survivability, security, and provisioning.

JINSUL KIM (Member, IEEE) received the B.S. degree in computer science from The University of Utah, Salt Lake City, UT, USA, in 1998, and the M.S. and Ph.D. degrees in digital media engineering from the Department of Information and Communications, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2004 and 2008, respectively.

From 2004 to 2009, he worked as a Researcher with the IPTV Infrastructure Technology Research Laboratory, Broadcasting/ Telecommunications Convergence Research Division, Electronics and Telecommunications Research Institute (ETRI), Daejeon. From 2009 to 2011, he worked as a Professor with Korea Nazarene University, Chonan, South Korea. He is currently a Professor with Chonnam National University, Gwangju, South Korea. His research interests include QoS/QoE, measurement/management, mobile-IPTV, socialTV, cloud computing multimedia communication, and digital media arts. He has been invited for Technical Program Committee (TPC) for IWITMA2009/2010, Program Chair (PC) for ICCCT2011, IWMWT2013/2014/2015, and General Chair for ICMWT2014. Since 2008, he has been an Invited Reviewer of the IEEE TRANSACTIONS ON MULTIMEDIA.

JAECHEOL RYOU received the B.S. degree in industrial engineering from Hanyang University, in 1985, the M.S. degree in computer science from Iowa State University, in 1988, and the Ph.D. degree in electrical engineering and computer science from Northwestern University, in 1990. He is currently a Professor with the Department of Computer Engineering, Chungnam National University, South Korea. His research interests are in internet security and electronic payment systems.