https://doi.org/10.5392/JKCA.2021.21.02.587

# 인공지능 기술기반의 서비스거부공격 대응 위한 서비스 모델 개발 방안

## A Service Model Development Plan for Countering Denial of Service Attacks based on Artificial Intelligence Technology

**김동맹, 조인준**
배재대학교 대학원 사이버보안과

Dong-Maeong Kim(ppagak@naver.com), In-June Jo(injune@pcu.ac.kr)

**요약**

본 논문에서는 나날이 발전하는 대규모 서비스거부공격에 대해 고전적인 방식의 DDoS 대응시스템에서 벗어나, 4차 혁명 시대의 핵심기술 중의 하나인 인공지능 기반의 기술을 활용해 지능화된 서비스거부공격을 효율적으로 감내 할 수 있는 서비스모델 개발방안을 제안하였다. 즉, 다수의 보안장비, 웹서버로부터 수집된 다량의 데이터를 대상으로 머신러닝 인공지능 학습을 통해 서비스거부공격을 탐지하고 피해를 최소화할 수 있는 방안을 제안하였다. 특히, 인공지능기술을 활용하기 위한 모델을 개발은 일정한 트래픽 변화를 반복하며 안정적 흐름의 데이터를 전송이 이루어지다가 서비스거부공격이 발생하면 다른 양상의 데이터 흐름을 보인다는 점에 착안하여 서비스서부공격 탐지에 인공지능기술을 활용하였다. 서비스거부공격이 발생하면 확률기반의 실제 트래픽과 예측값과의 편차가 발생하기 때문에 공격성 데이터로 판단하여 대응이 가능하다. 이 논문에서는 보안장비나 서버에서 발생하는 로그를 기반으로 데이터를 분석하여 서비스거부공격 탐지모델을 설명하였다.

■ 중심어 : | 인공지능 | 머신러닝 | 서비스거부공격 | 보안관제 | 서비스모델 |

**Abstract**

In this thesis, we will break away from the classic DDoS response system for large-scale denial-of-service attacks that develop day by day, and effectively endure intelligent denial-of-service attacks by utilizing artificial intelligence-based technology, one of the core technologies of the 4th revolution. A possible service model development plan was proposed. That is, a method to detect denial of service attacks and minimize damage through machine learning artificial intelligence learning targeting a large amount of data collected from multiple security devices and web servers was proposed. In particular, the development of a model for using artificial intelligence technology is to detect a Western service attack by focusing on the fact that when a service denial attack occurs while repeating a certain traffic change and transmitting data in a stable flow, a different pattern of data flow is shown. Artificial intelligence technology was used. When a denial of service attack occurs, a deviation between the probability-based actual traffic and the predicted value occurs, so it is possible to respond by judging as aggressiveness data. In this paper, a service denial attack detection model was explained by analyzing data based on logs generated from security equipment or servers.

■ keyword : | Artificial Intelligence | Machine Learning | Denial of Service Attack | Security Control | Service Model |

접수일자 : 2020년 12월 01일
수정일자 : 2021년 01월 04일
심사완료일 : 2021년 01월 04일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

# I. 서론

## 1. 연구의 배경 및 목적

사이버공간에서 서비스거부공격은 악의적 트래픽을 생산하고 이를 공격대상으로 전송하여 서비스의 가용성을 방해하는 행위를 말한다.

오늘날의 서비스거부공격은 누구나 행할 수 있는 환경이다. 즉, 구글링을 통해 손쉽게 서비스거부 관련 툴을 다운 받아 활용도 가능하다. 최근에는 전 세계의 PC를 대상으로 수많은 PC 좀비화를 통해 특정 사이트의 서비스를 방해하는 공격 형태로 진화하고 있다.

과거의 서비스거부공격은 국제표준기구(ISO)에서 표준화된 네트워크 구조를 제시한 기본 모델인 OSI 7계층 중 2계층(데이터링크계층) 부터 4계층(전송계층)을 악용한 공격이 대 다수였지만, 최근에는 계층7(응용계층)의 서비스거부공격이 다수를 점유되고 있다고 한다[1]. 그러나 서비스거부 대응시스템들은 2계층과 4계층의 트래픽 임계값 기반의 탐지구조로 되어 있어 계층7을 악용하는 공격에 대해 한계성을 보이고 있다.

본 논문은 이와 같이 심각한 서비스거부공격 대응하기 위해 인공지능을 활용한 탐지방안을 다루었다. 즉, 설치된 정보시스템, 보안시스템 로그를 활용해서 인공지능 기반 서비스모델 개발로 공격IP 추출을 하는데 목적을 두고 있다.

## 2. 연구의 내용 및 범위

서비스거부공격은 사이버위협 중 대단히 강력할 뿐만 아니라 사회와 비즈니스면에서 혼란을 일으킬 만큼 파급효과가 매우 크다. 이러한 공격기술은 지속적인 증가와 더불어 지능화, 고도화 되고 있다. 보안  업무측면에서도 수시로 발생하며 공격기법도 진화되고 있다. 기존의 공격기법이 네트워크 트래픽을 폭주시켜 업무를 마비 시켰다면, 최근에는 DNS(Domain Name Service), NTP(Nnetwork Time Protocol)서비스 등을 이용한 형태로 공격이 진화되고 있다. 이러한 사이버 공격에 적극적인 대응을 위해 보안전문가와 같은 추가적인 인적투자가 필요하다라고 한다. 하지만 비용적 측면에서 현실적 한계와 다양한 서비스거부공격 대응 보안솔루션의 한계로 현장 상황에 맞는 대응에 많은 어려움이 있는 실정이다.

본 논문에서는 이를 해결하기 위한 대안으로 서버나 보안장비로부터 발생하는 로그를 활용하여 인공지능기반의 서비스거부공격 대응방안 모델을 제안하였다. 제안된 모델을 통해 서비스거부공격으로부터 이상 징후를 확인 할 수 있다.

논문의 구성을 요약하면 제 2장에 인공지능 기반 서비스거부공격 대응 필요성 및 활용방안을 정리하였다. 이를 위해 서비스거부공격유형 분석과 인공지능 기술을 활용한 머신러닝 및 전처리방안에 대해서 살펴보았다. 제 3장에서는 인공지능 기반 서비스 모델 개발 방안을 제안하였으며, 서비스 모델의 알고리즘 동향과 개발방법에 대해서 정리를 하였다. 제 4장에서는 제안한 인공지능기반 서비스 모델에 적용된 알고리즘의 이론적 배경과 서비스 모델의 구현방안에 대해 설명을 하였다. 마지막으로 제 5장은 서비스모델 개발 방안에 대해 연구 결과를 정리하였고, 인공지능을 활용한 서비스거부공격 대응에 대해 깊이 있는 연구가 더 필요한 부분을 기술하였다.

# II. 인공지능 기반 서비스거부 대응 필요성 및 활용방안

## 1. 서비스거부 대응 체계

사이버공격으로부터의 기존 서비스거부공격 대응체계는 다른 공격 유형들과 달리 사전예방 활동이 무엇보다 중요했다. 기존 서비스거부공격의 연구는 완벽한 방어에 어려움이 있기 때문에 대부분의 공격은 예방활동을 통해 감내하는 부분으로 피해를 최소화하려 했다. 서비스거부공격 대응측면에서 보면 공격으로 확인된 트래픽에 대해 패킷캡처를 통해 공격트래픽을 수집하여 서비스거부공격의 패턴을 빠르게 분석하고, 이러한 분석결과로부터 도출된 방어정책을 방화벽, 침입방지시스템, DDoS 대응시스템 등에 반영하여 피해를 최소화하려했다. 이를 통해 상시 대응방안을 강구하여 이에

상응하는 정책개발 등의 활동을 수행하는등, 이와 더불어 서비스거부공격 대응 모의훈련 등을 통해서 대응능력을 강화했다[2].

사이버공격으로부터의 서비스거부공격은 'Ping Flooding', 'SYN Flooding', 'Session Flooding'과 같은 'Flooding'계열이 주요 공격수단이었지만, 최근의 서비스거부공격은 'Get Flooding', 'DNS', 'Chargen', 'NTP Reflect', 'Slowloris', 'RUDY Attack'과 같이 다양한 형태의 서버자원의 고갈을 노리는 형태로 진화되고 있다. 기존 서비스거부 대응장비는 초당 히트수를 측정하여 공격자 IP주소로부터 트래픽을 차단시키거나, 인입된 패킷에 대해서만 일정시간 퇴치를 하는 방식으로 대응하였다. 그러나 정상적인 접근 형태와 같이 동일한 방법으로 공격하는 기법들이 나날이 증가하고, 다량의 데이터와 혼재되어 들어오는 등의 요인으로 인해 서비스의 중단이 일어나서야 서비스거부공격을 받았는지 인지하는 경우가 일반적이다.[3]

## 2. 인공지능 서비스거부 대응 체계

인공지능기반의 서비스거부 대응체계 설계는 보안전문가의 경험과 기술, 그리고 보호하려는 영역의 IT인프라 환경에서 발생한 데이터 특성 정의가 무엇보다 중요하다. 이들을 설계에 반영하기 위해 현재의 보안장비에서 발생하는 로그의 특성을 충분히 숙지하고 이를 인공지능기술로 처리한 후에 그 결과로부터 비정상 데이터를 구분하여 대응이 가능토록 해야 한다. 이러한 대응체제 설계에서 고려할 사항을 정리하면 다음과 같다.

첫째, 서비스거부 보안전문가가 보호영역에 설치된 보안제품들의 대응상태와 DDoS 대응시스템, 침입방지시스템, 방화벽, WAF, 서버보안 등에서 발생되는 원시데이터들이 인공지능에서 어떻게 사용될 것인가에 대해 파악해야 한다. 여기서 중요한 점은 시스템로그까지 수집영역을 확대해서 융합분석이 가능토록 해야 한다. 이는 다양한 형태의 서비스거부공격에 대한 시나리오 기반의 인공지능 대응 환경을 구성하기 위해서이다.

둘째, 보안장비에서 발생하는 로그와 시스템에서 발생하는 로그들에 대한 데이터 수집을 통해서 서비스거부공격의 유형을 분류하고, 인공지능에서 정탐률에 대한 수치를 제시함으로써 차단과 탐지를 구분하여 대응의 수위를 결정할 수 있도록 해야 한다.

셋째, 오탐율을 줄이기 위해서는 서비스거부에 대해 데이터의 전처리를 통해 과정에 대한 프로세스를 사전 준비해야 한다. 마지막으로, 지도학습을 통해서 서비스 지도 학습에 대해서는 데이터의 변화에 대해 비정상행위 구별이 가능토록 한다.

이러한 내용을 토대로 현장에 적용하기 위해서는 인공지능 모델러와 보안전문가 서비스거부의 모의테스트 환경을 구성할 필요가 있다. 이때, 서비스공격용 패킷을 발생시킨 후에 나타나는 현상을 분석해야 한다. 그 결과로 데이터 거부공격에 대한 유형의 특성이 파악되어 한다.

**표 1. 인공지능 서비스거부 대응 체계 목표**

| 구분 | 목표 |
|---|---|
| 모델 | ■ 프로세스가 반영된 모델 개발<br>■ 내・ 외부 영역 구별 반영 |
| 플랫폼 | ■ 지도학습,비지도학습, 다양한 학습방식<br>■ 서비스거부 특성의 최적화 반영 |
| 사용자 환경 | ■ 인공지능 결과에 대한 재 학습 가능<br>■ 이상징후 중심 서비스거부 위험도에 구분 가능 |

## 3. 인공지능 데이터 수집방안

인공지능에서 활용할 데이터를 수집하기 위해서는 보안장비 또는 웹로그와 같이 실시간으로 생성되는 로그나 접근이력 등의 데이터를 수집해야 한다. 이러한 행위기반의 로그 데이터는 보안전문가의 노하우를 기반으로 한 특성을 추출함으로써 인공지능에서 신뢰도 있는 학습 및 판단을 위한 자료로 쓰일 수 있다. 인공지능의 데이터를 수집하기 위해서는 대용량의 데이터를 저장할 수 있는 저장 공간과 데이터의 성격에 따라 구분이 되어야 전처리 단계에서 데이터 처리를 오류 없이 효율적으로 수행 할 수 있다. 또한 인공지능에서 처리하기 위한 원시 데이터는 이기종의 보안장비나 서버 등에서 발생하는 로그에 대해 인공지능 수집시스템과 인공지능 수집 저장소를 보유하고, 데이터의 정합성을 유지해야 한다.

인공지능처리를 위한 데이터 수집을 위해서는 [그림

1]에서 보듯이 타 시스템에서 데이터를 제공 받을 수 있는 오픈 API(Application Programming Interface)방식의 서비스 제공이 필요하다. 이를 통해 수집저장소는 실시간으로 원본로그의 정합성을 유지하고, 대량의 데이터를 수집 및 처리에 안정성을 보장해 주어야 한다.

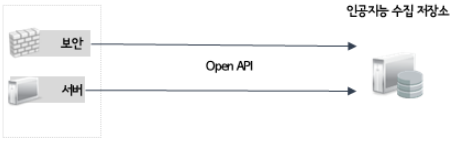


**그림 1. 데이터 수집 방안**

### 4. 인공지능 데이터 전처리 방안

인공지능이 다양한 형태의 데이터를 빠르고 정확한 처리를 위해서는 데이터 전처리과정이 필요하다고 한다[4]. 데이터 속성의 내용이나 데이터의 필드마다 데이터의 분산요소가 맞지 않는다면 인공지능의 판단 정확성을 보장하지 못하는 경우가 발생한다. 이를 위해서 데이터의 스케일링(Scaling)기법을 사용하여 데이터의 가용성을 보장하는 전처리 기법을 사용해야 한다. 데이터의 값이 일관성이 벗어난 값으로 입력을 받아들인다면 학습과정이 잘못된 예측과 다른 이해할 수 없는 출력으로 결과를 낼 수 있다. 특히 KNN(K-Nearest Neighbors)과 같은 머신러닝 기반 알고리즘이 데이터의 속성들 중 오차가 큰 값에 대해 최적화가 필요한 경우가 많다. 이를 위해 최소값과 최대값의 변화되는 스케일을 통해 정해진 값에 대해 효과적으로 사용이 가능하다.

## Ⅲ. 인공지능 기반 서비스거부공격 대응을 위한 서비스 모델 개발 방안

### 1. 서비스 모델 개요

많은 논문에서는 각각의 데이터 셋을 대상으로 여러 알고리즘을 적용하여 서비스거부공격을 탐지하는 모델 알고리즘을 제시한다. 데이터 전처리 방법은 논문에서 짧게 언급되고 있고, 중요 특성에 대한 설명은 부족하다. 중요 특성 추출과 그에 적합한 알고리즘 선별이 모형 성능에 크게 영향을 미친다. 여기서 중요한 점은 서비스거부공격의 특성상 다수 데이터 또는 로그를 대상으로 모델이 적용이 되기 때문에 허수값에 대한 대책을 가지고 모델개발을 수행해야 할 것이다. 이에 다수의 데이터를 대상으로 보안장비 로그로부터 공격 데이터의 분류 할 수 있는 방법에 대해 서비스 모델 개발방안을 제시하였다.

### 2. 서비스 모델의 알고리즘 동향

인공지능기술에서 기계학습과 심화학습을 활용하여 서비스거부공격 대응을 위한 서비스 모델 개발을 위해 탐지 및 예측 모형 알고리즘은 계속 발전하고 있다.[5]

예측 모형에 사용된 대표적인 알고리즘을 보면 'Support Vector Machine', 'Random Forest', 'Decision Tree', 'Long Term Short Memory', 'CNN'이 있으며, 여러 알고리즘을 혼합하여 사용하는 'PCA-RNN', 'PCA-SVM'등이 있다.

이러한 알고리즘을 활용한 모델생성 측면에서 보면 'Packet /Pcap(tcpdump)'데이터를 통해 공개된 패킷 데이터를 수집 후에 그들의 특성을 기반으로 모델 학습에 사용할 유용한 데이터를 추출한다. 추출한 데이터는 모델 학습에 적합한 형태로 변환한 후에 생성한 데이터 셋을 기반으로 학습을 진행한다.

또한 알고리즘 측면에서 보면 'Pcap(tcpdump)'데이터에서 전처리를 한 후에 특성을 추출하고, 학습 형태로 변환된 데이터 셋과 페이로드 데이터에서 다시 전처리하여 특성을 추출하는 형태로 이들의 특징을 어떻게 유용한 특징 데이터인지 판별하는 것이 매우 중요한 요소로 보고 있다고 한다.[6] 서비스모델의 알고리즘 동향에서 각각의 데이터 셋을 대상으로 여러 알고리즘을 서비스거부공격을 탐지하는 최적의 모델 알고리즘의 선택이 매우 중요하다.

### 3. 서비스 모델 설계 원칙

서비스 거부 공격은 다량의 접속 및 시간차 공격으로

진행이 되기 때문에 탐지 로그의 정탐, 오탐을 확인하기 위해서는 개별 로그마다 보안전문가가 여러 보안장비의 로그 이력을 살펴보아야 하므로 많은 시간과 자원이 낭비된다. 서비스 거부 공격의 보안장비의 로그 데이터를 비지도 학습인 클러스터링 방법을 활용하여 분석이 필요한 공격자의 활동을 주기적으로 주시해야 한다.

보안장비에서는 서비스 거부 공격의 유형으로 확인된 로그와 화이트 리스트 기반의 내부 데이터의 유형을 필터링 후 공격자의 활동에 대해서 리스트를 선정한다. 이를 토대로 해서 분석 대상 공격자의 활동에 대해 보호 영역의 보안장비 데이터에서 일정 시간 주기로 파생변수를 생성하고 비지도 학습을 수행한다. 여기서 중요한 것은 서비스거부공격의 대응 프로세스 반영을 위해 태스크 반복 주기 및 구간 결정이 매우 중요한 포인트이다.

### 4. 서비스 모델 개발 방법

서비스거부공격의 서비스 모델을 구현하기 위해서 방화벽 보안 로그 데이터에서 수집된 필드 추출한다. 방화벽에서 수집된 필드는 '발생시간', '출발지IP주소', '목적지IP주소', '출발지포트', '목적지포트', '발생수', '프로토콜', '패킷수', '패킷사이즈', 등을 로그 데이터의 레코드들을 수집할 수 있다. 방화벽 로그데이터를 30분단위로 데이터를 추출함으로써 데이터의 정합성을 높힐 수 있다. 이런 경우 장비간의 로그 기록 지연을 고려하여 종료 시점에서 5분을 중복허용하고, 35분 단위로 데이터셋을 생성하여 'K-means Clustering'알고리즘을 사용하여 특성들 간의 군집화를 통해 평소 트래픽과 다른 트래픽이 발생한 경우 군집화를 통해 이상징후 확인이 가능하다.

## Ⅳ. 인공지능을 토한 서비스거부공격 대응 기법 검증

### 1. 알고리즘의 이론적 배경

비 지도학습 모델은 복잡한 데이터에서 특정한 패턴을 인식하거나 유사한 데이터끼리 군집화하는 등의 목적으로 사용된다. 그러나 데이터에 사전 정의된 라벨이 없으면 지도학습과 같은 방식의 정확도 지표를 도출하기는 어렵다. 이러한 이유로 생성된 비지도 학습 모델의 활용이 비즈니스 목적에 적합한가에 대한 검증은 매우 중요하다. 비지도 학습 중 차원축소는 '재구성 오류'를 활용하여 평가 가능하며 군집 모델의 경우 일부라도 데이터 라벨 값을 알고 있는지 등의 상황에 따라 여러 종류의 평가 알고리즘을 선택하여 활용할 수 있다고 한다[7]. 따라서 비지도 학습 모델 평가를 위한 기준이 될 수 있는 사전 라벨링 데이터를 만들기보다는 일정기간의 로그 데이터에 대한 비지도 학습 모델의 분석 결과가 비즈니스 목적에 적합하다 판단된다.

### 2. 서비스모델의 구현방안

수집된 데이터를 대상으로 비지도학습의 일종인 클러스터를 사용하여 데이터가 가지고 있는 특성을 그룹핑 한다. 이어서 출발지 IP주소와 목적지 IP주소의 데이터를 기준으로 생성한 파생변수들을 중요하게 다뤄져야하는 특징(feature)으로 설정하고 클러스터링을 수행한다. 이와 같은 과정을 [표 1]과 같다.[8]

**표 1. 클러스터링 수행**

```
start = time.time()
kmeans = KMeansClutering()
feature =
['count','time_diff_sec','access_intv','access_per_sec','unique_src_port_cnt','tcp_flag','duration_std','duration_mean','unique_dstn_ip_cnt','action_val','domestic','private','overseas',]
preprocess_1_1 = rt[feature].copy()
preprocess_1_1.fillna(0,inplace=True)
k=7
rt_df,score=kmeans._fit_clustering(k,preprocess_1_1)
preprocess_1_result = pd.concat([rt,preprocess_1_1, rt_df],axis=1)
```

이를 통해 정상그룹과 이상 그룹을 구별, 이상행위가 보이는 패턴의 데이터를 찾아서 서비스거부공격의 형태를 구별할 수 있다고 한다. 이때 모델의 정확도를 높일 수 있는 방법으로 'K-means Clustering' 알고리즘을 사용하면 정의된 군집에서 개수를 찾을 수 있다. 이러한 과정은 [표 2]와 같다.

**표 2. K-means**

```
k=3
scaler = StandardScaler()
node2 = KMeans(n_clusters=k, algorithm='auto')
pipeline = make_pipeline(scaler, model2)
pipeline.fit(feature)

total_df = total.df.apend(feature)

kmeans_s = pd.DateFrame(pipeline.predict(feature)
kmeans_s_columns = [kmeans_s']

r=pd.concat([df_ip2[['source_ip', 'destination_ip]], kmeans_sj,
axis=1]
```

최적의 군집화는 다음과 같이 찾을 수 있다. 첫째 군집 중앙은 해당 군집에 속하는 모든 점의 산술 평균이다. 둘째 각 점은 다른 군의 중앙보다 자신이 속한 군집의 중앙에 더 가깝다. 여기서 주의 해야할 점은 K-Mmeans 알고리즘은 군집의 개수를 명시적으로 지정해야 한다. 'Inertia Value'의 값은 군집화가 된 후의 응집도를 나타내며 해당 값이 작을수록 응집도가 높게 군집화가 되었다는 의미이다. 군집화의 개수를 설정하기 위해 'Inertia Value'를 기준으로 최적의 군집 개수를 판단하고, 서비스거부공격모델에서 사용되는 군집의 개수는 아래의 로직으로 결정을 한다.

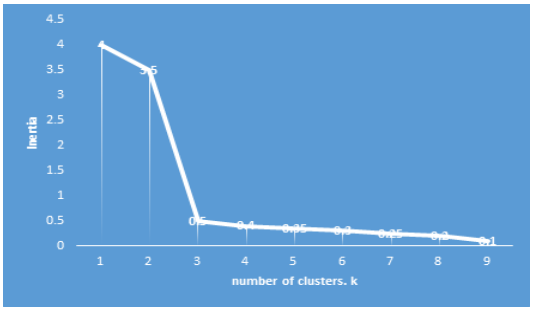


**그림 3. 서비스 모델 개발 절차**

위 데이터에서는 클러스터 K 개수가 3이상 증가하여도 군집의 응집도에 크게 영향을 주지 않기 때문에 군집의 개수를 3으로 사용하였다. 관측치가 적은 군집의 데이터를 추출하여 군집화된 데이터를 시각적으로 표현하기 위해서 t-SNE를 사용하여고 차원을 축소, [그림 4]에서 보듯이 같이 시각화로 DDoS공격이나, SCAN 공격에서 사용되는 공격 IP를 찾을 수 있다.

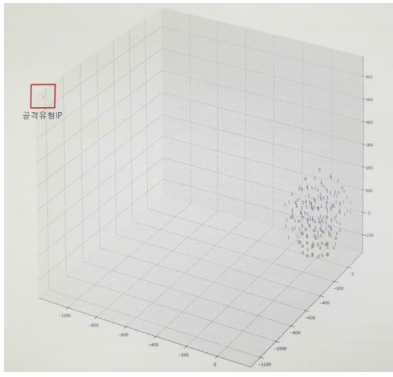

**그림 4. 로그 데이터 군집화**

## V. 결론

사이버위협으로부터 서비스거부공격의 위험은 상시 노출되어 있고, 이를 대응하기 위해 막대한 보안장비와 인력을 요구하게 된다, 이러한 보안위협으로부터 피로도를 줄이기 위해 수집부터 전처리과정등, 이를 효과적으로 처리하기 위한 인공지능 기반의 서비스 모델방안을 제안 하였다. 논문에서 제시한 서비스거부공격 데이터군집화를 통한 대응방안과 같이 다양한 형태의 모델들이 개발이 된다면, 보안장비에 의존하는 형태에서 4차혁명시대의 핵심인 인공지능을 활용한 사이버위협으로부터 정보자원의 서비스 안정성을 보장이 가능할 것이다 그러나 향후, 본 논문에서는 논의 되지 못했던 인공지능이 데이터를 처리하기 위한 전처리과정에 대한 추가 연구가 필요하며, 군집화를 통한 모델링외에 다른 관점에서 바라보는 인공지능 모델에 대한 추가적 연구가 필요하다.

## 참 고 문 헌

[1] Johnson kh Tanmay De "An Approach of DDoS Attack Detection Using Classifiers," National Insitue of Technology Durgapur India, pp.429-437, 2015.

[2] 백나은, 신재환, 장진수, 장재우, "Snort를 이용한 비

정형 네트워크 공격패턴 탐지를 수행하는 Spark 기반 네트워크 로그 분석 시스템," 한국콘텐츠학회논문지, 제18권, 제4호, pp.48-59, 2018.
[3] Jiangtao Pei, "A DDoS Attack Detection Method Based on Machine Learning" JOURNAL OF PHYSICS: CONFERENCE SERIES, 제1237권, 제3호, 2019.
[4] Thuy T.T Nguyen, Grenville Armitage, "A Survey of Techiniques for Internet Traffic Classification using Machine Learning," IEEE Communications Surveys & Tutorials, pp.56-76, 2008.
[5] 오영택, "인공지능 기술기반의 통합보안관제 서비스모델 개발방안," 한국콘텐츠학회논문지, 제19권, 제1호, pp.108-116, 2019.
[6] Nigel Williams Sebastian Zander, "A Preliminary Performance Comparsion of Five Machine Learning Alogrithms for Pracitical IP Traffic Flow Classification," ACM SIGCOMM Computer Communication Review, pp.5-16, 2006.
[7] 최동열, 안은영 "빅데이터를 이용한 자동 이슈 분석 시스템," 한국콘텐츠학회논문지, 제20권, 제2호, pp.240-247, 2020.
[8] Rojaiina Priyadarshini and Rabindra Kumar Barik, "A deep learning based intelligent framework to mitigare DDoS attack in fog environment," Some(KIIT University, Bhubaneswar, India), 2019.

## 저 자 소 개

**김 동 맹(Dong-Maeong Kim)** 정회원

■ 2012년 2월 : 건국대학교 컴퓨터공학과(공학석사)
■ 2019년 3월 ~ 현재 : LG히다찌 정보보안전문가

〈관심분야〉 : 정보보호, 인공지능, 보안컨설팅

**조 인 준(In-June Jo)** 정회원

■ 1982년 2월 : 전남대학교 계산통계학과 졸업
■ 1985년 2월 : 전남대학교 전자계산학과 석사
■ 1999년 2월 : 아주대학교 컴퓨터공학과 박사
■ 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
■ 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 전산조직응용