Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.99

사이버공격 융합 동향 분석을 위한 딥러닝 기반 보안 취약점 분석 자동화 메커니즘*

김 진 수,[1†] 박 남 제[2‡]
[1,2]제주대학교 (대학원생, 교수)

Deep Learning-Based Automation Cyber Attack Convergence Trend Analysis Mechanism for Deep Learning-Based Security Vulnerability Analysis*

Jinsu Kim,[1†] Namje Park[2‡]
[1,2]Jeju National University (Graduate student, Professor)

요 약

다양한 기술들이 하나로 융합되어 새로운 기술로 변화되고 있는 현재의 기술사회에서 사회의 변화에 발맞추듯 새로운 사이버공격들이 만들어지고 있다. 특히, 다양한 공격들이 하나로 융합됨으로 인해 기존의 보안 체계만으로 시스템을 보호하는데 어려움이 발생하고 있다. 이와 같은 사이버공격에 대응하기 위해 많은 정보가 생성되고 있다. 하지만, 무분별하게 발생하는 취약점 정보는 관리자에게 불필요한 정보를 제공하여 혼란을 유도할 수 있다. 따라서 본 논문에서는 딥러닝 기반의 언어 학습 모델을 이용하여 문서를 학습하고, 취약점 정보를 추출하여 MITRE ATT&CK 프레임워크에 따라 분류함으로써 관리자에게 구분화된 취약점 정보를 제공하여 새로이 발생하고 있는 사이버공격 융합 기술의 분석을 보조하는 메커니즘을 제안한다.

ABSTRACT

In the current technological society, where various technologies are converged into one and being transformed into new technologies, new cyber attacks are being made just as they keep pace with the changes in society. In particular, due to the convergence of various attacks into one, it is difficult to protect the system with only the existing security system. A lot of information is being generated to respond to such cyber attacks. However, recklessly generated vulnerability information can induce confusion by providing unnecessary information to administrators. Therefore, this paper proposes a mechanism to assist in the analysis of emerging cyberattack convergence technologies by providing differentiated vulnerability information to managers by learning documents using deep learning-based language learning models, extracting vulnerability information and classifying them according to the MITRE ATT&CK framework.

Keywords: MITRE ATT&CK, Cyber Attack, Attack Convergence, Vulnerability, MachineLearning

I. 서 론

기술의 발전은 점차 고도화되고 있으며, 기존에는 서로 다른 기술로만 인식되어 오던 기술들이 하나로 융합되어 새로운 기술로 발전하고 있다. 이 변화는 근래에 들어 보다 빠른 속도로 진행되고 있으며, 미래의 사회상을 바꾸는 원동력으로 적용될 수 있다 [1-3]. 특히 기술 간의 융합은 기존 기술의 한계를

Received(12. 21. 2021), Modified(01. 17. 2022), Accepted(01. 20. 2022)
* 본 논문은 2021년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 2019년 대한민국교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A04083374)
† 주저자, kimjinsu@jejunu.ac.kr
‡ 교신저자, namjepark@jejunu.ac.kr(Corresponding author)

벗어나 새로운 방향성을 제시할 수 있다는 점에서 많은 연구가 요구된다.

하지만 기술 간의 융합은 새로운 개념의 기술을 발생시킬 수 있으나, 기존과 다른 방향성을 가지는 시스템은 기존의 보안취약점뿐만 아니라 추가적인 보안취약점이 발생할 수 있다는 문제를 포함한다[4-6]. 특히 다양한 기술들이 융합함에 따라 세분화되는 기술들은 기존의 취약점 분석 체계만으로 적용하는 데 한계를 가질 수 있다[7-9]. 이와 같은 한계에 대응하기 위해 미래에 발생할 수 있는 융합기술에 대한 보안 취약점을 자동으로 분석하는 것은 유행성이 높은 공격 기술들의 취약점을 정리하여 연구의 방향성을 설정하거나, 집중적인 보안성 강화가 요구되는 기술을 설정하여 투자하여 비용대비 효과성을 높이는 등의 다양한 분야에 적용할 수 있다[10-12].

본 논문에서는 사이버 융합 공격 기술의 동향 분석을 위해 사이버 공격에 대한 취약점 정보를 가지는 문서를 수집하고, 문서상의 취약점 정보를 자동적으로 추출하여 MITRE ATT&CK 프레임워크에 대입하여 구조화된 취약점 정보를 제공하는 보안 취약점 분석 메커니즘을 제안한다.

II. 관련 연구 동향 분석

2.1 MITRE ATT&CK

MITRE의 ATT&CK 프레임워크는 조직에 위험을 초래할 수 있는 공격 기술과 공격의 피해를 최소화하기 위한 탐지 및 완화 기술의 범위가 방대해짐에 따라 단일 조직에 대한 공격 유형을 분석하고 대응하기에 한계점이 발생하였으며, 이와 같은 문제를 타개하기 위해 개발된 프레임워크이다[13].

MITRE의 ATT&CK 프레임워크는 Adversarial Tactics, Techniques, and Common Knowledge의 약자로 공격자의 전술과 기술들에 대하여 탐지를 수행하는 지식 기반 위협 탐지 모델이다. ATT&CK 프레임워크는 크게 Matrix, Tactics, Techniques의 세 가지로 구분된다. Matrix는 공격 기술을 정리한 Tactic와 Techniques의 전반적인 개념과 관계를 의미한다[14-16]. Matrix는 Enterprise, Mobile, ICS로 구분되며, 각각의 Matrix는 각 분야에서 발생한 각종 서비스를 대상으로 한 주제로 상세히 분류된다[16-18]. Tactics는 공격 대상에 따라 행동하는 공격자의 목적을 정의하는 것으로, 정보탐색, 실행, 지속성과 같이 공격자가 공격 대상으로 하는 목적을 중점으로 분류한다[19,20]. Techniques는 Tactics를 수행하기 위해 사용할 수 있는 방안을 정리한 것으로, 공격 기술에 의한 피해 결과를 명시한다.

2.2 지도학습(Supervised Learning)

일반적으로 머신러닝은 주어진 입력값의 목표값을 설정하고, 목표값에 인접하는 것을 목적으로 하는 지도학습과 학습데이터의 특징을 학습하여 별도의 입력된 목표값 없이 학습 모델 스스로 학습을 수행하는 비지도학습(Unsupervised Learning), 특정 환경에서 학습의 수행 결과 발생하는 보상에 기반하여 학습을 수행하는 강화학습(Reinforcement Learning)으로 구분할 수 있다[21-23].

지도학습은 다시 분류(Classification)와 회귀(Regression)의 두 가지 모델로 구분된다. 분류 모델은 입력된 데이터를 사전에 정의된 범주에 따라 분류를 수행하는 모델이다. 회귀 모델은 현재 가지고 있는 데이터를 활용하여 연속되는 값의 예측을 수행하는 모델을 의미한다[24-26].

본 논문에서는 지도학습 기반의 분류 모델을 이용하여 취약점 정보를 학습하고, MITRE ATT&CK 프레임워크에 맞춰 보안취약점을 분류함으로써 자동화된 분석 메커니즘을 제안함에 목적을 가진다. 분류의 과정은 ATT&CK 프레임워크라는 명확한 지표를 가지고 수행하므로 명확한 목표값을 설정할 수 있는 지도학습 기반의 학습 모델을 구축하였다.

2.3 딥러닝 기반 언어 학습 모델 동향 분석

딥러닝을 기반으로 하는 언어 학습 모델 초기에는 입출력을 시퀀스 단위로 처리하는 RNN(Recurrent Neural Network) 모델에서 시작되었으며, 최근에는 Transformer 기반의 모델로 변화하고 있다.

Ashish 외 7명의 연구[27]에서는 RNN 구조적 한계에 따른 기울기 소실 문제와 크기가 일정하지 않은 정보를 고정된 크기의 벡터로 압축함에 따라 정보 손실이 발생하는 문제를 가지는 seq2seq 모델을 보완하기 위해 어탠션(Attention)을 적용하였다. 해당 연구에서는 기존 seq2seq 모델의 인코더-디코더 방식을 유지하되, 인코더와 디코더를 어탠션으로 구성하는 Transformer 방식을 제안하였으며, 제안

모델을 적용하여 WMT(Workshop on statistical Machine Translation) 2014의 영어-독일어 번역 부분에서 28.4 BLEU을 달성하며 효과성을 입증하였다.

언어 학습 모델 중 NLP(Natural Language Processing) 분야에서는 사전에 학습된 언어 모델을 생성하고, 이를 베이스로 다른 분야에서 사용하는 언어를 추가적으로 학습함으로써 성능을 향상시키는 방향으로 발전하고 있다. Jacob 외 3명의 연구[28]는 언어의 문맥에는 양방향성이 존재하며, 학습 과정에서도 양방향 학습이 요구됨을 주장하며 새로운 구조의 언어 학습 모델을 제안하였다. 해당 연구에서 제안된 학습 모델은 BERT(Bidirectional Encoder Representations from Transformers) 모델이라 불리며, 위키피디아의 25억여 개의 단어와 BookCorpus의 8억여 개의 단어와 같이 별도의 레이블링이 진행되지 않은 텍스트 정보를 사전에 학습한 언어 모델로 많은 NLP 기반의 작업에서 높은 성능을 보이며 효과성을 입증하였다.

Yinhan 외 9명의 연구[29]에서는 기존의 BERT 모델의 성능 향상을 위해 새로운 언어 학습 모델 RoBERTa(Robustly Optimized BERT Pretraining Approach)를 제안하였다. 제안된 RoBERTa 학습 모델은 BERT 모델의 하이퍼파라미터와 학습 데이터의 사이즈를 조절하여 BERT의 성능을 향상시킨 모델이다. BERT 모델에서 언어를 학습하는 과정에서 단계마다 다른 위치에 존재하는 언어를 마스킹하는 Dynamic masking, 다양한 방식의 입력 데이터를 통해 가장 높은 성능 수준을 보이는 구성을 확인하는 Input format, 기존의 데이터 규모보다 큰 규모의 사용을 통해 성능을 향상한 Large batch의 3가지 주요한 개선사항을 적용하여 효과를 입증하였다.

III. 제안 메커니즘

3.1 소단원 작성 기법

본 논문에서는 사이버공격 융합 기술 동향를 분석하기 위한 머신러닝 기반의 보안 취약점 자동화 분석 메커니즘을 제안한다. 제안하는 메커니즘은 MITRE의 ATT&CK에 속하는 Tactics와 Techniques을 분석하고, 각각의 키워드를 추출한 뒤, 입력으로 사용되는 보안 문서 키워드 판별을 위한 지표로 사용한다. 입력된 보안 문서는 사이버 공격과 관련된 키워드를 추출하고, Tactics와 Techniques를 기반으로 유효한 키워드를 이용해 분류를 수행한다. 최종적으로 보안 문서상에 존재하는 보안취약점을 MITRE ATT&CK의 Matrix 구조에 맞춰 정리함으로써 단계화된 보안취약점 정보를 분석한다. Fig.1.은 제안하는 메커니즘에 대한 전반적인 흐름을 보이는 개념도이다.

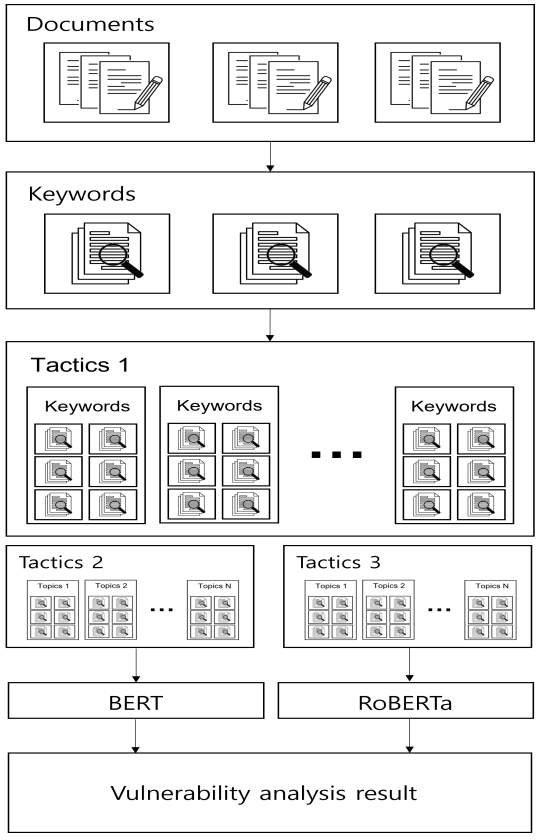

Fig. 1. Proposal Mechanism Conceptual Diagram

제안 메커니즘은 사전에 MITRE ATT&CK의 Tactics와 Techniques의 키워드 분석 및 분류하여 지식베이스를 구성하고, 이를 바탕으로 언어 학습 모델인 BERT와 RoBERTa를 적용하여 입력되는 문서상에 존재하는 보안취약점을 분류하는 것을 목적으로 한다. 따라서 기존의 보안 문서 분석을 통해 키워드를 추출하고, 의미가 불분명하거나, 의미가 없는 전치사 등을 제거하는 전처리 과정을 수행하였다. 이후, 각각의 키워드를 지식베이스 상의 키워드와 매칭하여 보안취약점 분류모델의 학습데이터를 구성하였

다. 제안 메커니즘은 지식베이스 학습 데이터 구축 단계, 보안취약점 자동화 분류 단계로 구분한다.

3.2 지식베이스 학습 데이터 구축 단계

지식베이스 학습 데이터 구축 단계는 보안 취약점의 자동 분석을 위해 먼저 목표를 생성하는 단계를 의미한다. 해당 단계에서는 MITRE ATT&CK 프레임워크의 Tactics 및 Techniques의 주요한 문장을 추출하고, 학습 데이터와 학습 데이터 간의 관계 설정을 수행한다. 학습 데이터는 STIX(Structed Threat Information eXpression) 2.0을 기반으로 사이버 위협체계를 적용하여 Attack Pattern, Threat Actor, Identity(Environment), Vulnerability, Tool의 5개의 SDO(STIX Domain Objects)와 SRO(STIX Relationship Object)를 사용하였다.

Table 1.은 SDO에 대한 내용을 설명하는 것이다.

Fig. 2.는 제안 메커니즘에서 SDO와 SRO에 대해 설계한 내용을 보이는 것이다. SRO의 관계는 Attack Patten의 Technique에 해당하는 SDO의 메인 노드를 1 depth, 메인 노드에 대한 주요한 키워드를 하위로 하여 2 depth의 관계를 설정하였다. 또한 Technique에 직접적인 관계를 가지는 키워드를 1 depth의 위치로 설정하여 각 SDO에 대한 키워드를 Technique의 키워드로 학습하는 것을 방지하였다. 초기 학습 데이터 구축을 위해 전문가 세미나를 통하여 MITRE ATT&CK의 Tactics와 Techniques 및 관련 문서의 키워드를 Techniques로 구분하여 키워드를 추출하여 지식베이스를 구축하였다. 지식베이스는 14개의 Tactics와 91개의 Technique, 각 Technique에 속하는 SDO와 키워드로 구성하였다.

Table 1. STIX-based SDOs

SDO	Explanation
Attack Pattern	About TTP (Tactic, Technique, Procedure)
Threat Actor	Name of hacker group/related group (nickname), etc.
Environment	Default Service List by OS
Vulnerability	CVE Vulnerability Types
Tool	Hacking tool used to deploy TTP

각각의 SDO는 ATT&CK 프레임워크의 Technique에 속하는 공격 그룹 정보, 취약점 정보, 공격 환경 정보, 공격 도구 정보의 소항목으로 구성된다. 학습 데이터 설정 과정에서 키워드는 4개의 SDO의 소항목과 Technique에 대한 직접적 연관을 가지는 키워드로 분류하여 학습을 수행한다.

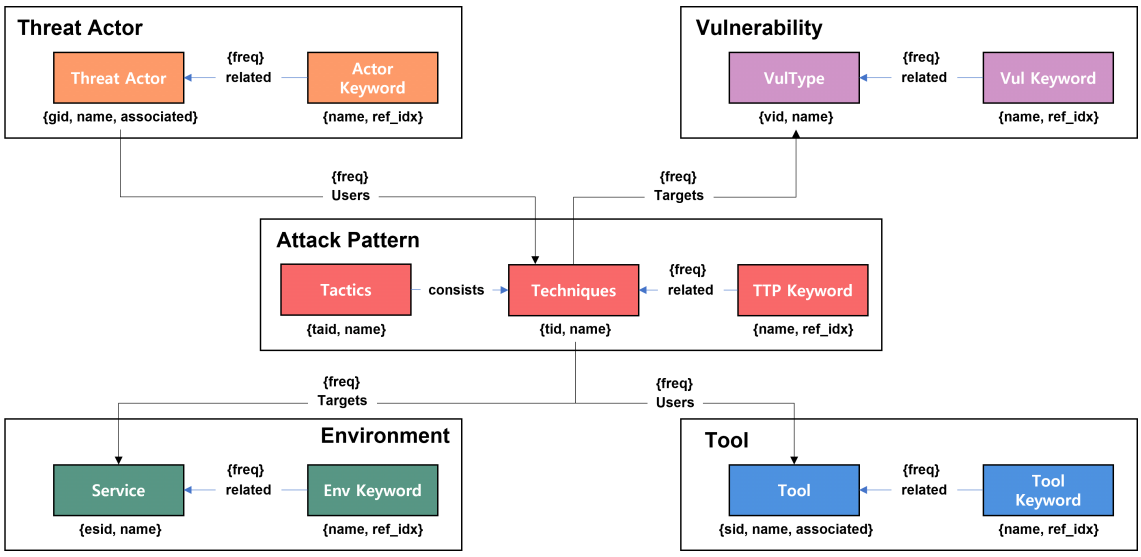

Fig. 2. Establishing the relationship between SDOs in the proposal mechanism

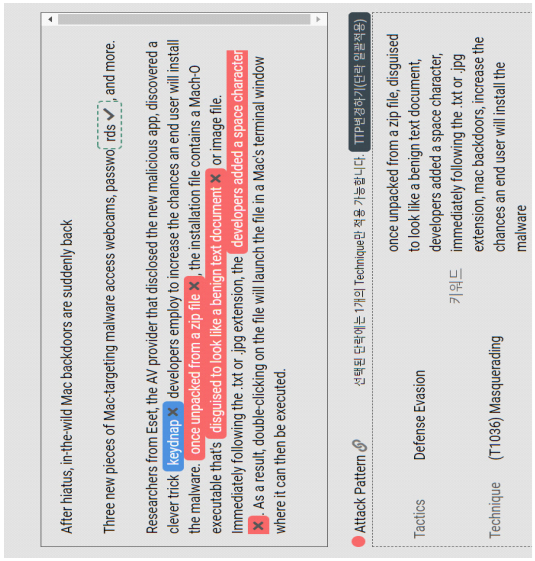

Fig. 3. Knowledge base building process

Fig.3.은 지식베이스 구축을 위해 문장 단위로 학습 데이터를 설정하는 과정을 보이는 것이다.

이와 같이 분류한 학습 데이터는 Fig.4.와 같이 정리되며, 문단 단위로 하나의 TTP가 지정되어 문단을 이루는 자연어 흐름 상에서 { } 기호 안의 구문이 attention 대상이 되며, { 키워드 | 클래스 }의 구조를 가진다.

TA0005	Defense Evas	T1036	Masquerading	After hiatus, in-the-wild Mac backdoors are suddenly back
TA0005	Defense Evas	T1036	Masquerading	Three new pieces of Mac-targeting malware access webcams, passwords, and more.
TA0005	Defense Evas	T1036	Masquerading	Researchers from Eset, the AV provider that disclosed the new malicious app, discovered a clever trick {keydnap|Keydnap} developers employ to increase the chances an end user will install the malware. {unpacked zip file|Masquerading}, the installation file contains a Mach-O executable that's {disguised look like benign text document|Masquerading} or image file. Immediately following the .txt or .jpg extension, the {developer added space character|Masquerading}. As a result, double-clicking on the file will launch the file in a Mac's terminal window where it can then be executed.

Fig. 4. Transformed training data

3.1 보안취약점 자동화 분류 단계

보안취약점 자동화 분류 단계에서는 기존에 구조화되지 않은 텍스트를 이용하여 언어를 학습한 BERT 모델과 RoBERTa 모델을 사용하여 학습을 수행하였으며, 이 과정에서 CTI(Cyber Threat Information)의 기술 문장 분류를 위한 파인 튜닝(Fine Tuning)을 수행한다. 파인 튜닝이란 기존에 학습이 수행된 모델을 기반으로 목적에 맞춰 업데이트하는 방법을 의미한다. 파인 튜닝 과정은 아래와 같이 수행된다.

① 학습용 데이터셋 정제 및 정규화
② 학습, 검증, 테스트 데이터셋 분리 train,Validation,Test
③ 데이터 토큰화(구글의 다국어 BERT 토크나이저 활용)
④ 데이터 패딩 및 어텐션 마스킹
⑤ 학습 입력, 마스크, 레이블 묶기(TensorDataset 활용)
⑥ 사전 학습된 BERT 모델 로드 (구글 다국어 BERT)
⑦ 옵티마이저 설정및 하이퍼파라미터 튜닝(Adam, learning rate 설정)
⑧ 스케줄러 생성(학습률 조절)
⑨ 모델의 그래디언트 초기화
⑩ Epoch 만큼 훈련 반복

파인 튜닝을 위한 파라미터는 아래와 같다.

```
model_name = 'BERT-base-uncased'
max_length = 100
optimizer = Adam(learning_rate=5e-05, e
                 psilon=1e-08,decay=0.01
                 , clipnorm=1.0)
```

학습 데이터셋의 길이는 100으로 설정하였으며, 학습률은 5e-05, 수치 안정을 위한 엡실론 상수 값은 1e-08, 소수에 대한 학습 감소율은 0.01로 설정하였다.

IV. 제안 메커니즘 결과 분석

본 논문에서 제안한 메커니즘은 BERT 모델과 RoBERTa 모델을 적용하여 자동화된 보안 취약점 분석을 제공하는 것을 목적으로 한다. 제안 메커니즘의 효과성 분석을 위해 정확도 검증을 수행하였으며, 그 결과는 Fig.5.와 같다.

총 3,589건의 데이터셋을 대상으로 2,872건의 학습을 수행하였으며, 719건의 데이터셋을 대상으로 취약점 분류를 수행하였다. 그 결과, 10회의 학습을 수행한 후 학습 훈련에 사용된 데이터에 대해 BERT와 roBERTa에서 각각 82.74%와 83.24%

	Learning Count	Ours (Train/test)
BERT	10 epochs	08274/0.7405
	100 epochs	0.9970/0.8069
RoBERTa	10 epochs	0.8324/0.7488
	100 epochs	0.9974/0.7686

Fig. 5. Proposal Mechanism Accuracy Verification

의 정확도를 보였으며, 학습 과정에서 사용되지 않은 데이터셋을 대상으로 취약점 분류를 수행한 결과 각각 74.05%와 74.88%의 정확도를 보였다.

학습 수행 횟수와 정확도의 관계성을 확인하기 위해 100회의 학습을 수행한 이후 정확도를 확인한 결과 학습 과정에서 사용되지 않은 데이터셋을 대상으로 각각 80.69%, 76.86%의 정확도를 보이며 학습 수행 횟수와 정확도가 비례함을 확인하였다.

또한, 학습 과정에서는 RoBERTa가 높은 정확도를 보임에도 불구하고, 실제 취약점을 분석하는 경우 BERT 모델이 보다 안정적이게 수행됨을 확인할 수 있다.

V. 결 론

근래에 들어서 다양한 기술들이 융합되며 보안취약점 또한 다양하게 발생하고 있다. 이는 보안취약점에 대한 다양한 보안 문서의 생성을 의미하며, 무분별하게 많은 정보가 발생할 수 있음을 의미한다. 구조화되지 않은 보안 문서를 담당자로 하여금 혼란을 유도할 수 있으며, 이는 전반적인 보안 체계의 약점으로 이어질 수 있다.

본 논문에서 제안하는 모델은 입력 문서에 존재하는 사이버공격과 관련된 키워드를 자동으로 추출하고, 이를 기반으로 문서상에 존재하는 공격 또는 보안 기법을 MITRE의 ATT&CK 프레임워크의 Tactics에 기반하여 분류함으로써 세분화된 공격 목적과 기법으로 정리하여 복잡한 공격에 적용된 기법을 분석하는 학습 모델로, 향후 발전하고 있는 사이버공격과 기술의 융합에 따라 복잡해지는 보안취약점을 분류하기 위해 많은 연구가 요구되는 분야이다.

향후, 언어학습 모델의 동향을 분석하여 추가적인 파라미터 도입을 통해 제안 메커니즘의 정확도를 높이는 연구의 수행이 요구된다.

References

[1] Jong-Seok Choe, Jong-Gyu Park and Ho-Won Kim, "Research on artificial intelligence and internet of things convergence security technology," *Information and Communications Magazine,* vol. 34, no. 3, pp. 65-73, Feb. 2017.

[2] J. Kim and N. Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing," *Personal and Ubiquitous Computing,* pp. 1 - 9, Aug. 2019.

[3] Gihyo Nam, "Convergence security technology trends and issues," *Weekly technology trend*, Institute for Information & communications Technology Promotion, pp. 1-9, Nov. 2014.

[4] Dou Kim, "Convergence security technology and patent trends," *Weekly technology trend*, Institute for Information & communications Technology Promotion, pp. 15-24, Jun. 2017.

[5] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, vol. 80, pp. 34517-34534, Mar. 2020.

[6] D. Lee, N. Park, G. Kim and S. Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment," *Peer-to-Peer Networking and Applications*, vol. 11, pp. 1299-1308, Mar. 2018.

[7] Gyeong-Hui Gwon, "Seoul Digital Forum 2004- Digital Convergence

Revolution: In Search of New Opportunities," *Digital Contents*, vol. 6, no. 133, pp. 72-80, Jun. 2004.

[8] Jinsu Kim, Sungwook Ryu and Namje Park, "Privacy-Enhanced Data Deduplication Computational Intelligence Technique for Secure Healthcare Applications," *Computers Materials Continua*, vol. 70, no. 2, pp. 4169-4184, Sep. 2021.

[9] Seong-Hoon Lee and Dong-Won Han, "Smart technology application status and future," *Korea Institute of Information Technology Magazine*, 9(2), pp.45-52, Aug. 2011.

[10] J. Kim, N. Park, G. Kim and S. Jin, " CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia," *Electronics, vol.* 8, no. 4, 412, Apr. 2019.

[11] Sung-Hee Jin, "A Case Study and Industry Demand Investigation on Technological Convergence Education Related to the 4th Industrial Revolution - Focused on Electronics, Software, and Automobile -," *Journal Of The Korea Contents Association*, 19(2), pp. 36-48, Feb. 2019.

[12] Eunjin Kim, Sun-Tae Kim and Jong-Suk Lee, "Exploratory research on future innovation convergence technology in the digital transformation era," *Proceedings of the Korean Institute of Information and Commucation Sciences Conference*, pp. 627-629, Jan. 2021.

[13] Otis Alexander, Misha Belisle and Jacob Steele, "MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy," *MITRE*, Mar. 2020.

[14] N. Park, Y. Sung, Y. Jeong, S. Shin and C. Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea," *International Conference on Computer and Information Science*, pp. 1-15, Jun. 2019.

[15] Roger Kwon, Travis Ashley, Jerry Castleberry, Penny Mckenzie and Sri Nikhil Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," *2020 Resilience Week*, Salt Lake City, UT, USA, Oct. 2020.

[16] D. Lee and N. Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance," *The Journal of Supercomputing*, vol. 73, pp. 1103-1118, Aug. 2016.

[17] Anna Georgiadou, Spiros Mouzakitis and Dimitris Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors*, vol. 21, no. 9, 3267, May. 2021.

[18] Sungwook Ryu, Jinsu Kim, Namje Park and Yongseok Seo, "Preemptive Prediction-Based Automated Cyberattack Framework Modeling," *Symmetry*, vol. 13, no. 5, 793, pp. 1-20, May. 2021.

[19] J. Kim and N. Park, "Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment," *Transactions on Emerging Telecommunications Technologies,* John Wiley & Sons, Inc. New York, NY, USA, Fub. 2021.

[20] Jeremy Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks," 2*020 IEEE International Conference on Smart Cloud (SmartCloud)*, Washington, DC,

USA, Nov. 2020.

[21] Jinsu Kim, Donghyeok Lee and Namje Park, "CCTV-RFID enabled multifactor authentication model for secure differential level video access control," *Multimedia Tools and Applications*, vol. 79, pp.23461-23481, Jun. 2020.

[22] Rich Caruana and Alexandru Niculescu-Mizil, "An empirical comparison of supervised learning algorithms," *Proceedings of the 23rd international conference on Machine learning*, pp. 161-168, Jun. 2006.

[23] Jinsu Kim and Namje Park, "Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments." *Applied Sciences*, vol. 10, no. 14, pp. 1-12, Jul. 2020.

[24] Youngsup Shin, Kyoungmin Kim Jemin Justin Lee and Kyungho Lee, "ART: Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity," 2021 World Automation Congress (WAC), Taipei, Taiwan, Oct. 2021.

[25] Bing Liu, "Supervised Learning," Web data mining, pp. 63-132, Apr. 2011.

[26] Jinsu Kim and Namje Park, "A Face Image Virtualization Mechanism for Privacy Intrusion Prevention in Healthcare Video Surveillance Systems," *Symmetry*, vol. 12, no. 6, pp.1-15, Jun. 2020.

[27] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez and Lukasz Kaiser and Illia Polosukhin, "Attention Is All You Need," *Computation and Language*, pp.1-15, Jun. 2017.

[28] Jacob Devlin, Ming-Wei Chang, Kenton Lee and Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," *Computation and Language*, pp. 1-16, May. 2019.

[29] Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer and Veselin Stoyanov, "RoBERTa: A Robustly Optimized BERT Pretraining Approach," *Computation and Language*, pp. 1-13, Jul. 2019.

〈저자소개〉

김 진 수 (Jinsu Kim) 학생회원
2019년 8월: 강원대학교 전자정보통신공학부 정보통신공학전공 석사
2019년 9월~현재: 제주대학교 융합정보보안학협동과정 박사과정
2019년 9월~현재: 제주대학교 사이버보안인재교육원 연구원
〈관심분야〉 클라우드, 지능형 영상감시 시스템, IoT 등

박 남 제 (Namje Park) 종신회원
2008년 2월: 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월~2008년 12월: ETRI 정보보호연구단 선임연구원
2009년 1월~2010년 8월: UCLA Post-Doc., ASU Research Scientist
2010년 9월~현재: 제주대학교 교육대학 초등컴퓨터교육전공 교수
2010년 9월~현재: 제주대학교 대학원 융합정보보안협동과정 교수
〈관심분야〉 정보교육, STEAM, 정보보호, 암호이론 등