

오토인코더 기반의 IoT 연계 처리를 통한 IoT 데이터 신뢰 기법

연용호¹, 정윤수^{2*}

¹목원대학교 소프트웨어교양학부 조교수, ²목원대학교 정보통신융합공학부 조교수

IoT data trust techniques based on auto-encoder through IoT-linked processing

Yong-Ho Yon¹, Yoon-Su Jeong^{2*}

¹Assistant Professor, Department of Software Liberal Art, Mokwon University

²Assistant Professor, Division of Information and Communication Convergence Engineering, Mokwon University

요 약 분산 환경에서 다양하게 사용되고 있는 IoT 장치는 의료·환경·교통·바이오·공공장소 등 사용 분야가 다양해지면 서 IoT 장치에서 송·수신되는 데이터의 중요도가 점점 증가하고 있다. 본 논문에서는 IoT 데이터의 신뢰성을 보장하기 위한 방법으로 수 많은 데이터들을 다양한 중요 속성별로 분류·처리하도록 오토인코더 기반의 IoT 연계 처리 기법을 제안한다. 제안 기법은 오토인코더 기반의 IoT 연계 처리를 위해서 IoT 데이터를 특성별로 블록체인으로 묶어 처리하 도록 IoT 데이터별로 상관관계 지수를 사용한다. 제안 기법은 IoT 데이터의 신뢰성을 보장하기 위해서 상관관계 지수 에 적용된 블록체인 기반의 n-계층 구조로 확장 운영한다. 또한, 제안 기법은 IoT 데이터의 상관관계 지수에 따라 IoT 수집 데이터에 가중치를 적용하여 IoT 데이터를 선택할 수 있을 뿐만 아니라 실시간으로 IoT 데이터의 무결성을 검증 하는 비용을 낮출 수 있다. 제안 기법은 n-계층 구조로 IoT 데이터를 확장할 수 있도록 IoT 데이터의 처리 비용을 유지한다.

주제어 : 사물인터넷, 오토인코더, 무결성, 데이터 연계, 블록체인

Abstract IoT devices, which are used in various ways in distributed environments, are becoming more important in data transmitted and received from IoT devices as fields of use such as medical, environment, transportation, bio, and public places are diversified. In this paper, as a method to ensure the reliability of IoT data, an autoencoder-based IoT-linked processing technique is proposed to classify and process numerous data by various important attributes. The proposed technique uses correlation indices for each IoT data so that IoT data is grouped and processed by blockchain by characteristics for IoT linkage processing based on autoencoder. The proposed technique expands and operates into a blockchain-based n-layer structure applied to the correlation index to ensure the reliability of IoT data. In addition, the proposed technique can not only select IoT data by applying weights to IoT collection data according to the correlation index of IoT data, but also reduce the cost of verifying the integrity of IoT data in real time. The proposed technique maintains the processing cost of IoT data so that IoT data can be expanded to an n-layer structure.

Key Words : Internet of Things, Autocoder, Integrity, Data Link, Blockchain

*Corresponding Author : Yoon-Su Jeong(bukmunro@mokwon.ac.kr)

Received September 11, 2021

Revised September 30, 2021

Accepted November 20, 2021

Published November 28, 2021

1. 서론

4차 산업혁명 시대가 대두된 이후 사물 인터넷(intelligence and Internet of Things, IoT) 기술이 사용되고 있는 분야는 다양해지고 있으며, 서로 다른 이기종의 IoT 장치가 서로 상호적으로 연결되는 ICT 환경이 구축됨으로써 IoT 기술은 다른 기술들에 비해 핵심 기술로써 중요한 역할을 수행하고 있다[1, 2].

IoT 환경에서는 데이터의 처리 속도 및 보안 문제점을 개선하기 위해서 실제 환경에서는 IoT 데이터를 실시간으로 수집하여 다른 IoT 장치에게 전달한 후 필요한 IoT 데이터만을 추출하는 과정에서 IoT 데이터의 신뢰성을 보장하는 연구들이 증가하고 있다.

최근에는 이기종의 IoT 장치들이 서로 연결 가능하기 때문에 IoT 장치 사이에서 송·수신되는 데이터가 기하급수적으로 증가하고 있으며, 제3자에게 노출되지 않도록 IoT 데이터에 인증과 암호를 사용하고 있다. 그러나, IoT 데이터에 보안 기능을 부여함으로써 서버의 부하 및 네트워크 트래픽의 증가를 야기하고 있어 이를 해결하기 위한 방안이 필요하게 되었다[3-5].

본 논문에서는 IoT 환경에서 IoT 데이터를 안전하게 추출될 수 있도록 오토인코더 기반의 로드 밸런스를 수행할 수 있는 IoT 데이터 신뢰 기법을 제안한다. 제안 기법은 로드밸런스 과정에서 비지도 방식으로 IoT 정보를 수집하고 학습하기 때문에 IoT 서명 정보 값을 임의의 랜덤값으로 생성하도록 하고 있으며, 다른 IoT 정보는 비트 형태로 보안 정보(SI, Security Information) 값만을 할당받아 처리한다. 이것은 IoT 장치 이외의 네트워크 구성 요소들의 부하를 낮추기 위해서이다. 또한, IoT 데이터는 블록체인이 되도록 n-계층 형태로 확장함으로써 네트워크 트래픽을 최소화한다. 제안 기법은 비대칭적으로 IoT 데이터를 처리하기 위해서 IoT 데이터별로 연계 정보를 사전 처리 함으로써 서버의 대역폭과 계산 비용을 낮추고 있다. 제안 기법은 오토인코더 기반의 로드 밸런싱 과정에서 IoT 장치간 데이터 연계를 유지하기 위해서 IoT 데이터를 이진 코드로 벡터화 함으로써 벡터화된 IoT 정보간 서로 직교하도록 그룹화한 후 각 정보의 가중치 확률을 이용하여 IoT 데이터를 제3자에게 노출시키지 않도록 n-계층 형태로 가중치를 추출한다.

이 논문의 구성은 다음과 같다. 2장은 오토인코더와 IoT 데이터 처리 연구들에 대해서 설명한다. 3장에서는 IoT 연계 처리의 효율성을 위한 오토인코더 기반의 IoT 데이터 신뢰기법을 제안하고, 4장에서는 실제 환경에서

수집된 IoT 트래픽 데이터 셋을 이용하여 성능 평가를 수행한다. 마지막으로 5장은 결론을 맺는다.

2. 관련연구

2.1 오토인코더

최근 딥러닝이 사회적으로 큰 이슈가 되면서 데이터 인코딩과 관련된 다양한 학습기법들이 연구되고 있다. 오토인코더(AutoEncoder)는 비지도(unsupervised) 방식으로 데이터를 훈련시키는 인공 신경망의 한 종류로써, 데이터를 먼저 인코딩 한 후 인코딩된 표현을 학습하여 입력 데이터와 가장 가깝게 생성하는 기법이다.

오토인코더는 그림 1처럼 W_h 로 정의되는 아핀 변환(affine transformation) 후 스퀴싱(squashing)을 거치는 인코더 과정을 통해 입력 x 가 맨 왼쪽부터 동작하여 중간 은닉층(hidden layer) h 를 형성한다. 형성된 은닉층의 결관은 다른 W_x 로 정의되는 아핀 변환 다음에 또 다른 스퀴싱이 나타나도록 디코더 과정을 통해 디코더의 대상이 되는 기본과정을 hidden 계층에 따라 반복적으로 수행한다.

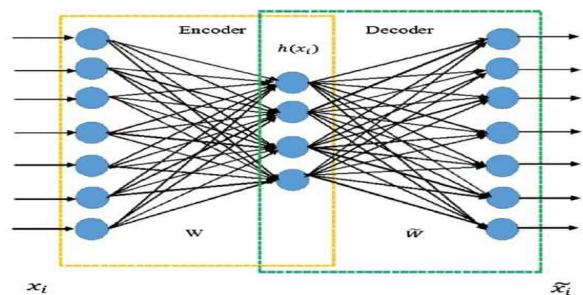


Fig. 1. Autoencoder Operation

Fig. 1의 과정을 방정식으로 나타내면 식 (1)~ 식 (2)처럼 표현이 가능하다.

$$h = f(W_h x + b_h) \quad (1)$$

$$\hat{x} = g(W_x h + b_x) \quad (2)$$

오토 인코더는 이상 감지, 이미지 노이즈 제거, 이미지 압축기 등과 같은 응용 분야에 많이 사용된다. 오토인코더에서 인코더는 압축기로 사용되고, 은닉 표현(코딩된 표현)은 특정 입력의 모든 정보를 전달하는 역할로 사용된다.

2.2 기존연구

IoT 장치가 다양한 환경에 사용되면서 IoT 사용 목적에 따라서 복잡한 네트워크 구조가 형성되는 분산 클라우드 환경은 IoT 장치에서 생성되는 데이터의 유형(공인 데이터셋 부족, 침입 경로 등)에 따라 IoT 데이터의 보안 문제가 다양하게 발생되고 있다.

네트워크 환경에서 발생하는 IoT 데이터 보안은 주로 IoT에서 생성한 공인 데이터 셋이 부족했기 때문에 발생되었다. 최근 딥러닝이 대두되면서 CICIDS2017[6], UNSW-15[7], N_BaloT[8], KDD99[9], NSL-KDD[10] 등에서 실시간으로 생성한 트래픽 데이터 셋을 사용하여 IoT 장치가 비정상적으로 동작하는지를 점검하고 프로토콜별로 성능 평가를 수행하고 있다.

IoT 장치에서 생성하는 데이터는 사용 용도 이외에 네트워크에서 생성하는 데이터 트래픽과 거의 차이점이 없다. IoT 장치에서 생성하는 데이터의 특징 정보들은 최근 인공지능(딥러닝) 기술을 이용하고 있다. 인공지능(딥러닝) 기술과 함께 IoT 데이터의 특징 정보를 추출하는 방식은 데이터 차원을 전처리 단계에서 줄이기 때문에 IoT 데이터의 정확도와 처리 효율을 향상시킨다[11,12].

IoT 데이터의 연계 처리와 관련된 많은 연구에서는 IoT 데이터의 손실 없이 IoT 데이터를 정확하게 선별하기 위해서 선형판별분석 대신 주성분 분석(PCA)을 주로 이용하고 있다. 이것은 주성분 분석이 IoT 데이터의 특징 정보 간 비선형 상관관계를 포착하지 않기 때문이다[13,14].

3. 오토인코더 기반의 IoT 정보 신뢰 향상 기법

3.1 네트워크

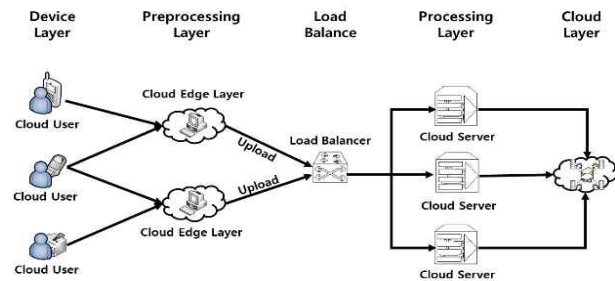


Fig. 2. System Layer of Overall Proposed Model

제안 기법은 그림 2처럼 IoT 데이터를 클라우드 환경에서 생성하기 때문에 IoT 데이터가 서버에 전달하기 전에 로드 밸런스를 수행한다. 그림 2의 구조처럼 로드밸런스 과정에서 비지도 방식으로 IoT 정보를 수집하여 학습하게 되면 학습된 정보들은 클라우드 계층에서 서버가 학습을 완료할 수 있도록 추가 파라미터를 업데이트하게 된다.

제안 기법은 Fig. 2처럼 시스템을 구성한 이유가 오토인코더를 통해 수 많은 IoT 데이터들을 서로 연계처리하기 위해서이다. Fig. 2의 구성 요소들은 IoT 서명 정보 값만을 임의의 랜덤값으로 생성하고 그 이외의 정보는 비트 형태로 보안 정보(SI, Security Information) 값만을 할당받아 처리한다. 그 이유는 네트워크 구성 요소 간 역할을 강화할 뿐만 아니라 서버 부하를 낮추기 위해서이다. 또한, 제안 기법은 IoT 데이터의 상관관계 지수를 사용하여 블록체인을 n-계층 구조로 확장함으로써 네트워크 트래픽 감소와 빠른 데이터 처리가 가능하다.

3.2 IoT 정보 연계

제안 기법은 IoT에서 생성한 데이터를 오토인코더 과정을 통해 비대칭 처리를 수행하여 IoT 데이터별 고유벡터의 쌍대비교 행렬인 d_{ij} 의 i 번째 벡터와 j 번째 벡터 사이의 연계 정보 R_{ij} 를 Fig. 3과 같이 구성한다.

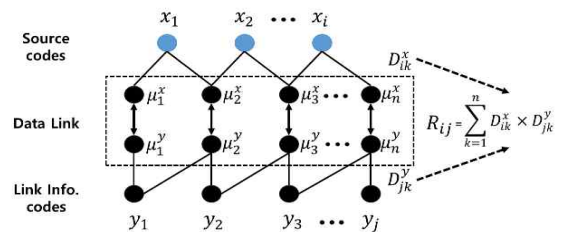


Fig. 3. IoT Data Link Information for Asymmetric Processing

제안 기법은 오토인코더 기반의 로드밸런싱을 수행하는 과정에서 인코딩된 IoT 데이터의 벡터 정보들을 사전 연계처리함으로써 서버의 대역폭과 계산 비용을 낮추는 효과를 얻는다. Fig. 3에서 IoT 데이터의 비대칭 처리에 적용되는 정보는 식 (1)과 같다.

$$R_{ij} = \sum_{i=1, k=1}^n D_{ik}^x \times D_{jk}^y \quad (1)$$

여기서, D_{ik}^x 는 i 번째 벡터와 k 번째 사전처리 계층 사이의 연계성을 의미하고, D_{jk}^y 는 j 번째 벡터와 k 번째 사전처리 계층 사이의 연계성을 의미한다.

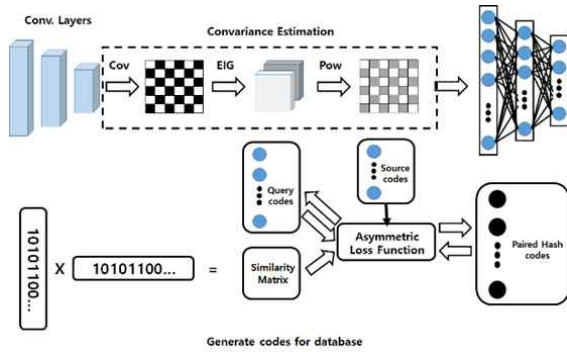


Fig. 4. Binary code vectorization of IoT information

제안 기법은 오토인코더 기반의 로드밸런싱 과정에서 IoT 데이터 연계를 유지하기 위해서 IoT 데이터를 그림 4처럼 이진 코드로 벡터화하기 때문에 IoT 데이터 간 비대칭 연계 처리를 수행한다. 그리고, 벡터화된 IoT 정보는 서로 직교하도록 비대칭적으로 그룹화한 후 각 정보의 가중치 확률을 이용한다. 이것은 IoT 데이터를 외부에 노출시키지 않도록 IoT 데이터의 가중치를 추출하기 때문이다.

3.3 비대칭 IoT 정보 처리

제안 기법은 다수의 IoT 장치로부터 서버로 송신되는 IoT 데이터의 특성에 따라 연계 처리하도록 트랜잭션을 다중 해쉬 체인 기반의 블록체인으로 식(2)처럼 묶는다. 제안 기법은 IoT 데이터의 가중치를 계층적으로 추출하기 때문에 제3자로부터 안정적으로 보호할 수 있도록 IoT 데이터를 해쉬 체인한다.

$$\sum_i \sum_j P_{ij}(IoT_i, IoT_j) \quad (2)$$

여기서, i 와 j 는 IoT 데이터의 인덱스를 의미하고, P_{ij} 는 쌍대비교 행렬을 이용한 IoT 데이터의 연계 지수 확률을 의미한다.

또한, 제안 기법은 비대칭적으로 그룹화하도록 식 (3)과 같은 확률 함수를 적용한다.

$$E(B_i^x) = - \sum_{i=1}^n \frac{1}{n} \log \frac{1}{n} = \log n \quad (3)$$

여기서, n 은 IoT 데이터의 수를 의미하고, i 는 IoT 데이터의 i 번째 연계 정보를 의미하고, x 는 비대칭 연계 정보의 그룹의 인덱스를 의미한다.

3.4 비대칭 IoT 처리 알고리즘

제안 기법은 비대칭적으로 그룹화하기 위해서 IoT 데이터별로 odd/even으로 replication 수에 따라 2개의 해쉬 값을 첫 번째와 마지막에 추가한다. Table 1은 IoT 데이터의 효율적 연계 처리를 위해서 IoT 데이터를 다중 해쉬 체인으로 묶어 블록 형태로 주기적으로 반복 생성하는 비대칭 IoT 처리 알고리즘을 보여주고 있다.

Table 1. IoT Information process algorithm

Input: IoT Information
Output : Generation IoT data using odd/even
<pre> 1: for every IoT data do 2: Generate the IoT data 3: If receive IoT Information from IoT Device 4: Store the IoT Information block 5: Generate random blocks in n-bit from using $R(0,1)^n$ 6: If Generate hash value for odd/even 7: Add to first and last of hash chains 8: Verification of integrity of IoT data 9: end if 10: else 11: Request IoT data from other IoT Devices 12: end if 13: end for </pre>

Table 1에서 IoT 정보를 주기적으로 갱신함으로써 IoT 데이터간 간섭을 최소화하기 위해서 IoT 정보는 odd/even에 따라 비교 분류한다. Table 1처럼 IoT 데이터 이외에 계산 집약적인 정보들은 모두 non-블록체인으로 처리하며, IoT 데이터 간 간섭을 최소화하도록 그룹으로 묶은 IoT 데이터들을 임의의 크기로 그룹핑한다.

4. 평가

4.1 실험 환경

시뮬레이션에서 사용할 데이터셋은 [12, 15] 에서 수집한 실제 트래픽 데이터셋을 사용하였으며, IoT 데이터의 특징 추출은 오토인코더 기반으로 추출하고 있다. 제안 기법에서 추출된 IoT 데이터의 분류는 다중 결정 트

리를 이용하였으며, 학습에 사용된 다중 클래스 알고리즘은 Random Forest 알고리즘을 사용하였다. 네트워크 망은 멀티 메쉬 망으로 구성하고, 아두이노 장비에서 IoT 데이터를 송·수신하도록 하였다.

시뮬레이션을 위한 파라미터는 다중 해쉬 체인으로 IoT 환경을 구성하였다. 네트워크 범위는 IoT 장치의 송수신 범위를 고려하여 50~100m 사이가 되도록 설정하였으며 서버와 IoT 장치의 대역폭은 10MHz / 5MHz으로 설정하였다. 블록체인과 관련된 설정 중 블록체인의 최대 크기에 대한 한계는 0.5~ 1Mbytes으로 설정하였다.

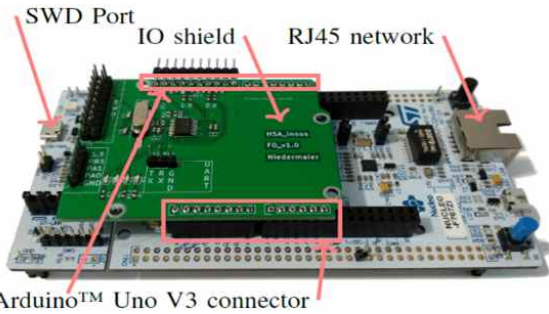


Fig. 5. IoT Device used in Performance Evaluation

4.2 성능평가

제안 기법은 식 (4) ~ 식 (7)을 이용하여 정확도, 정밀도 재현율 그리고 F1-score 등을 성능 평가 척도로 사용한다.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (7)$$

4.2.1 트래픽별 정확도

IoT 장치로부터 생성한 데이터를 서버로 전달하는 과정에서 여러 요인(자연요소, 네트워크 상황 등)에 의해 IoT 데이터의 무결성이 보장받지 못하는 경우가 발생된다. 제안 기법은 오토인코더 기반의 로드밸런싱을 이용하여 데이터의 무결성에 대한 정확도를 분석한 결과 Table 2와 같다. Table 2에서 제안 기법은 오토인코더 기반의 로드밸런싱을 사용하였을 지 않았을 때가 트래픽별로 평균 4.3% 향상되었다. 이 결과는 IoT 데이터 간 블록 체인으로 그룹으로 가중치를 부여하여 IoT 데이터 간 동기화를 수행하도록 IoT 데이터 오류율을 최소화하도록 유지하였기 때문이다.

또한, 제안 기법은 IoT 데이터를 클라우드 서버로 직접 전달하지 않고 IoT 데이터 간 트랜잭션의 누적 사용을 일정한 크기로 그룹 관리하도록 블럭 처리하기 때문에 IoT 장치에서 수집되는 데이터가 증가할수록 IoT 데이터의 무결성 정확도가 높게 나타났다.

4.2.2 IoT 데이터 연계 처리시간

제안 기법은 IoT 데이터를 처리하는 로드 밸런싱에서 IoT 데이터의 트래픽 별 블록체인을 연계하는 소요 시간을 오토인코더 훈련 시간과 데이터 재구성 시간으로 구분하여 처리시간을 분석한 결과는 Table 3와 같다.

Table 3처럼 로드밸런싱을 이용하여 블록체인을 연계하는 시간이 로드밸런싱을 이용하지 않는 블록체인 연계 시간보다 평균 7.5% 향상된 결과를 얻었다. 이 결과는 IoT 데이터를 서버에 저장되기 전 로드밸런싱을 통해 사전 처리 및 분석을 수행하였기 때문에 IoT 데이터간 상관 정보를 행렬로 표현하여 IoT 데이터의 중요 정보 산출이 향상된 결과이다. 물리적인 환경에 따라 IoT 데이터 처리 시간이 상이하게 나타날 수 있지만 IoT 장치와 서버 간 Hidden 레이어(25~100)에 따라 최대 12.9%의 처리 시간 차이가 나타났다.

Table 2. Accuracy according to type of IoT traffic

Method	Number of IoT															
	Http				Ftp				Syn				UDP			
	A	P	R	F	A	P	R	F	A	P	R	F	A	P	R	F
Load Balancing	98.612	97.831	97.652	98.996	97.528	96.981	98.021	97.374	98.021	98.328	97.827	98.654	97.686	97.543	96.687	96.754
Not Load Balancing	96.547	95.934	96.874	96.772	96.032	95.362	97.210	65.328	96.014	95.367	95.147	95.326	96.214	96.574	95.147	95.036

A: Accuracy, P: Precision, R: Recall, F: F1-Score

units : %

Table 3. Processing time according to type of IoT traffic

units : second

Method	Number of IoT							
	Http		Ftp		Syn		UDP	
	AET	DR	AET	DR	AET	DR	AET	DR
Load Balancing	36.980	5.647	32.254	4.022	34.114	4.699	27.324	3.658
Not Load Balancing	49.325	7.621	46.587	5.894	43.658	6.399	38.328	4.758

AET: AutoEncoder Training time(s)
DR: Data reconstruction time(s)

5. 결론

정보통신 기술이 4차산업 혁명 기술들과 융합되면서 IoT에서 처리되는 데이터의 활용도가 다양한 분야에서 활용되고 있다. 본 논문에서는 IoT 데이터를 안전하게 검증하기 위한 오토인코더 기반의 IoT 데이터 신뢰 기법을 제안하였다. 제안 기법은 로드밸런싱 과정에서 비지도 방식을 사용하여 IoT 서명 정보 값을 임의의 랜덤값으로 생성하기 때문에 네트워크 부하를 낮추고 있다. 또한, 제안 기법은 IoT 데이터별 고유벡터의 쌍대비교 행렬의 벡터 요소사이의 연계 정보를 사전처리하였다. 특히, IoT 데이터 연계를 유지하기 위해서 IoT 데이터를 이진 코드로 벡터화 함으로써 IoT 데이터를 제3자에게 노출시키지 않도록 IoT 데이터의 가중치를 추출하였다. 실험 평가 결과, 제안 기법은 오토인코더 기반의 로드밸런싱을 사용하였을 경우 트래픽별 정확도가 평균 4.3% 향상되었으며, 로드밸런싱을 이용하여 블록체인을 연계하는 시간은 평균 7.5% 향상되었다. 향후 연구에서는 기존 연구 결과를 이용하여 IoT 환경에서 수집되는 데이터셋의 신뢰도 검증 정확도를 향상시킬 수 있는 연구를 수행할 계획이다.

REFERENCES

- [1] A. Shahnaz, U. Qamar & A. Khalid, (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, 7, pp. 147782–147795.
- [2] S. Son, J. Y. Lee, M. H. Kim, S. J. Yu, A. K. Das & Y. H. Park, (2020). Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. *IEEE Access*, 8, 192177–192191.
- [3] X. Yang, X. Pei, M. Wang, T. Li & C. Wang, (2020). Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain. *IEEE Access*, 8, 144809–144822.
- [4] M. K. Choi, C. Y. Yeun & P. H. Seong, (2020). A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access*, 8, 118732–118740.
- [5] A. Majumdar & G. Mohan, (2020). Distributed Fractionalized Data Networks For Data Integrity. *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–3.
- [6] U. Imtiaz & H. M. Qusay, (2019). A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks. *Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference(CCNC)*, 1–6.
- [7] Machine Learning Repository. (2021). <https://archive.ics.uci.edu/ml/index.php>
- [8] K. Igor, S. Igor & B. Alexander. (2018). Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. *IEEE ACCESS*, 6, 72714–72723.
- [9] T. Mahbod, B. Ebrahim, L. Wei & A. G. Ali. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. *Proceedings of the 2009 IEEE symposium on computational intelligence in security and defence application*, 1–6.
- [10] NSL, <http://www.nsl.cs.unb.ca/NSL-KDD>.
- [11] H. Chae & S. H. Choi. (2014). Feature Selection for efficient Intrusion Detection using Attribute Ratio. *International Journal of Computers and Communications*, 8, 134–139.
- [12] Machine Learning Repository. (2021). <https://archive.ics.uci.edu/ml/datasets.php?format=&ask=&att=&area=&numAtt=greater100&numIns=&type=seq&sort=nameDown&view=list>.
- [13] B. Ravishankar, P. Kulkarni & M. V. Vishnudas, (2020). Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments. *Proceedings of the 2020 International conference on Mainstreaming Block chain Implementation (ICOMBI)*, 1–4.
- [14] P. Huang, K. Fan, H. Yang, K. Zhang, H. Li & Y. Yang, (2020). A Collaborative Auditing Blockchain for Trustworthy Data Integrity in Cloud Storage System. *IEEE Access*, 8, 94780–94794.
- [15] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo & Y. Elovici. (2017). *Detection of unauthorized iot devices using machine learning techniques*. preprint arXiv:1709.04647.

연 용 호(Yong-Ho Yon)

[정회원]



- 1988년 2월 : 충북대학교 수학과 학사
- 1990년 2월 : 충북대학교 수학과 석사
- 1997년 8월 : 충북대학교 수학과 박사
- 2011년 3월 ~ 현재 : 목원대학교 소프트웨어교양학부 조교수
- 관심분야 : 격자론, 수리논리, 합의대수
- E-Mail : yhyon@mokwon.ac.kr

정 윤 수(Yoon-Su Jeong)

[정회원]



- 1998년 2월 : 충북대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 유·무선 통신 보안, 정보보호, 바이오인포매틱, 헬스케어, 빅 데이터, 클라우드 컴퓨팅
- E-Mail : bukmunro@gmail.com