한국정보전자통신기술학회논문지(jkiiect)'21-6, Vol.14 No.3
논문 21-14-03-201 http://dx.doi.org/10.17661/jkiiect.2021.14.3.201

딥러닝 형상관리를 위한 블록체인 시스템 설계

배수환*, 신용태**

Design for Deep Learning Configuration Management System using Block Chain

Su-Hwan Bae*, Yong-Tae Shin**

요 약 머신러닝의 한 종류인 딥러닝은 각 학습 과정을 진행할 때, 가중치를 변경하면서 학습을 수행한다. 딥러닝을 수행할때 대표적으로 사용되는 Tensor Flow나 Keras의 경우 학습이 종료된 결과를 그래프 형태로 제공한다. 이에 과다 학습으로 인한 퇴화 현상 또는 가중치의 잘못된 설정으로 인해 학습 결과에 오류가 발생하는 경우, 해당 학습 결과를 폐기해야한다. 이에 기존 기술은 학습 결과를 롤백하는 기능을 제공하고 있지만, 롤백 기능은 최대 5회 이내의 결과로 제한된다. 또한, 딥러닝의 모든 과정을 기록하고 있는 것이 아니기 때문에 값을 추적하기 어렵다. 이를 해결하기 위해 MLOps의 개념을 적용한 기술이 존재하지만. 해당 기술에서는 이전 시점으로 롤백하는 기능을 제공하지 않는다. 본 논문에서는 기존 기술의 문제점을 해결하기 위해 학습 과정의 중간 값을 블록체인으로 관리하여 학습 중간 과정을 기록하고, 오류가 발생할 경우 롤백할 수 있는 시스템을 구성한다. 블록체인의 기능 수행을 위해서 딥러닝 과정 및 학습 결과 롤백은 Smart Contract를 작성하여 동작하도록 설계하였다. 성능평가는 기존의 딥러닝 방식의 롤백 기능을 평가하였을 때, 제안방식은 100%의 복구율을 가지는 것에 비교하여 기존 기법에서는 6회 이후에 복구율이 감소되어 50회일 때 10%까지 감소하는 것을 확인하였다. 또한, 이더리움 블록체인의 Smart Contract를 사용할 때, 블록 1회 생성 시 157만원의 금액이 지속적으로 소모되는 것을 확인하였다.

Abstract Deep learning, a type of machine learning, performs learning while changing the weights as it progresses through each learning process. Tensor Flow and Keras provide the results of the end of the learning in graph form. Thus, If an error occurs, the result must be discarded. Consequently, existing technologies provide a function to roll back learning results, but the rollback function is limited to results up to five times. Moreover, they applied the concept of MLOps to track the deep learning process, but no rollback capability is provided. In this paper, we construct a system that manages the intermediate value of the learning process by blockchain to record the intermediate learning process and can rollback in the event of an error. To perform the functions of blockchain, the deep learning process and the rollback of learning results are designed to work by writing Smart Contracts. Performance evaluation shows that, when evaluating the rollback function of the existing deep learning method, the proposed method has a 100% recovery rate, compared to the existing technique, which reduces the recovery rate after 6 times, down to 10% when 50 times. In addition, when using Smart Contract in Ethereum blockchain, it is confirmed that 1.57 million won is continuously consumed per block creation.

Key Words : BlockChain, Configuration Management System, Deep Learning, Ethereum, Tensor Flow

"This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2020-0-01602) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation)"

*Dept. of Computer, Soongsil University
**Corresponding Author : Dept. of Computer Science, Soongsil University (shin@ssu.ac.kr)

Received June 16, 2021 Revised June 17, 2021 Accepted June 21, 2021

1. 서론

머신러닝의 한 종류인 딥러닝은 각 학습 과정을 진행할 때, 가중치를 변경하면서 학습을 수행한다. 딥러닝을 수행할때 대표적으로 사용되는 Tensor Flow나 Keras의 경우 학습이 종료된 결과를 그래프 형태로 제공한다. 이에 과다학습으로 인한 퇴화 현상 또는 가중치의 잘못된 설정으로 인해 학습 결과에 오류가 발생하는 경우, 해당 학습 결과를 폐기해야한다. 기존 기술에서도 5회 이내의 값으로 롤백을 하거나, MLOps를 적용하여 중간 값을 관리하는 기능이 제공되지만, 완벽하게 학습 결과를 복구하거나, 이력을 관리해주는 기능 제공이 부족하다. 이를 해결하기 위해 딥러닝 형상관리를 위한 시스템에 대한 연구를 진행하였고[1], 본 논문에서는 기존 연구의 주제에 대한 실질적인 블록구성과 합의방식, 세부 동작 절차에 대하여 진행한 연구결과에 대하여 기술한다.

본 논문의 구성은 2장에서 관련연구로 블록체인과 딥러닝에 대하여 설명하고, 기존의 방식에서의 문제점을 서술하였다. 3장에서는 제안하는 기술의 구조와 블록 구성, 동작 절차에 대한 내용을 서술하였다. 4장에서는 제안 시스템의 성능평가로 이더리움을 사용했을 때 발생하는 비용대비 절약되는 금액을 계산하였으며, 기존 방식 대비 복구성능에 대하여 평가하였다. 마지막으로 결론에서는 본 연구의 결론과 향후 연구 진행방향에 대하여 서술한다.

2. 관련 연구

본 장에서는 제안하는 시스템의 기반의 되는 딥러닝, 블록체인의 기술과 이를 활용한 기존 기술들에 대하여 설명한다.

2.1 블록체인

블록체인은 기존의 폐쇄적인 보안방식의 매커니즘과는 다르게, 네트워크 참여자의 데이터 공유를 통해 데이터의 위변조를 방지하는 기술이다. 공격자가 데이터를 위변조하여도 네트워크에 참여하는 다른 참여자들의 데이터와 비교하였을 때, 다수가 소유한 데이터와 상이한 점이 있다면 변조된 데이터가 인정받지 못한는 형태를 가진다.

블록체인을 구성하는 방식은 네트워크 형태에 따라 Public 네트워크와 Private 네트워크로 구분된다. Public 네트워크는 제한없이 블록체인 네트워크에 참여 가능하며, 블록체인에서 제공하는 기능을 사용할 수 있다. Private 네트워크는 허가된 참여자만이 블록체인의 구성원으로 참여할 수 있으며, 제한된 기능을 제공받아 사용할 수 있다. 두 네트워크 형태의 특징은 아래의 [표 1]과 같다[2][3][4].

표 1. 블록체인 네트워크의 특징 비교
Table 1. Compare of BlockChain Network's Feature

	Public Block chain	Private Block chain
Read Permission	Don't Care	Authenticated User
Authentication and Commit	Don't Care	Authenticated User
Create Transaction	Don't Care	Authenticated User
Authorization	Not use	Use
Consensus	PoW	PoW, PBFT
Example	Bitcoin, Ethereum	Hpyer Ledger Fabric

블록을 생성하기 위한 합의 방식으로는 Public 네트워크에서는 주로 해시 알고리즘을 활용하여 블록을 생성하는 PoW(Proof-of-Work)를 사용한다. Private Network에서는 PoW을 사용할 수 있으며 참여자들 간의 데이터 교환을 통한 합의를 도출하는 PBFT(Practical Byzantine Fault Tolerance)[5][6] 방식을 사용한다.

2.2 딥러닝

딥러닝은 머신러닝 알고리즘의 한 종류로 기존의 단일 신경망(Neural Network)을 여러 층으로 쌓아 중첩시킨 형태를 가진다. 딥러닝의 신경망 구조는 다음의 그림 1과 같은 형태로 구성되며 이를 깊은 신경망 이라고 한다.

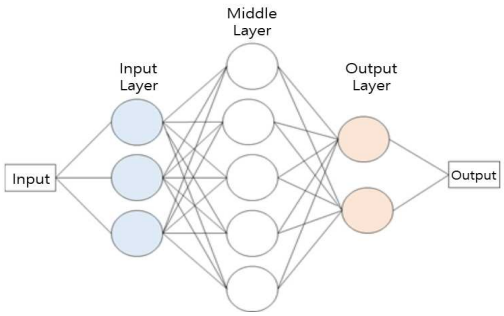

그림 1. 딥러닝 신경망 구조
Fig 1. Structure of Deep Learning Neural Network

딥러닝은 기존의 방식과는 다르게 특징량을 추출하는 방식에 차이가 있다. 기존 방식에서는 사람이 내부의 특징을 지정해주고 이를 학습하는 것과 다르게 기계가 자동으로 특징을 추출하여 학습할 수 있다[7]. 이를 위해 사용하는 것이 깊은 신경망으로, 3개 이상의 신경망을 합쳐놓은 형태를 가진다.

깊은 신경망에서 각 입력에서는 가중치라는 매개변수를 사용하여 학습 데이터의 변화를 주며 학습을 수행한다. 이때 학습 과정에서 초과학습이 발생하거나 가중치 변화로 인한 학습 결과의 오류가 발생할 수 있는데, 기존의 방식에서 오류가 발생하는 경우 학습한 상태를 폐기해야 한다. 이를 해결하기 위해 Tensor Flow와 Keras에서는 스냅샷 방식을 사용하여 가장 최근 수행되었던 5단계 이전까지의 결과로 롤백이 가능하지만, 딥러닝 과정 전체의 이력관리는 불가능하다[8].

3. 제안하는 시스템 설계

본 장에서는 제안하는 시스템의 구성, 블록 생성 시 절차, 롤백 절차에 대하여 설명한다.

3.1 시스템 구조

제안 하는 시스템은 크게 딥러닝을 수행하는 서버와 참여하는 노드들로 구성된다. 아래의 그림 2와 표 2는 이를 나타낸 그림과 각 구성요소에 대한 설명이다.

제안하는 시스템에서 합의 방식은 PoW를 사용한 합의를 진행한다. PoW의 경우 네트워크 참여자들 모두가 자원을 사용해야한다는 단점이 존재하지만, PBFT와는 다르게 특정 리더의 역할을 하는 사람이 주도적으로 데이터를 생성하고 전달하지 않기 때문에, 외부로부터 리더의 공격에 더 유연하게 대응이 가능하다. 또한, 기존의 연구에서 PBFT를 사용하는 Hyperledger Fabric의 경우, 블록 1개를 생성할 때 헤더에서 발생하는 데이터 때문에 블록 하나 당 200MByte에 가까운 용량이 필요로 하다[9]. 이 때문에 오래동안 지속하는 서비스를 위해서는 PoW를 사용하는 합의 방식을 사용하는 것으로 시스템을 설계하였다.

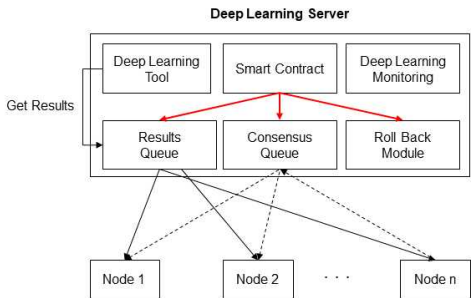

그림 2. 제안하는 시스템 구조
Fig. 2. Structure of Proposed System

표 2. 시스템 구성 요소
Table 2. Entity of System

Classification	Name	Discription
Deep Learning Server	Deep Learning Tool	Performing Deep learing
	Smart Contract	Use for block creation and results rollback
	Result Queue	Stores deep learning intermediate value
	Consensus Queue	Stores consensus process for nodes
	Roll Back Module	Rollback to previous deep learning processes
	Deep Learning Monitoring	Deep learning history management
User Node	Node	Making decision about block creation, consensus, rollback

3.2 블록생성 절차

제안하는 시스템에서 블록 생성은 아래의 그림 3과 같은 형태로 첫 번째 절차를 수행한다.

블록생성 시 첫 번째 절차에서 딥러닝 서버에서 학습을 수행하는 Deep Learning Tool은 학습하면서 발생하는 중간 결과값인 가중치, 정화도, 오차율에 대한 정보를 Results Queue에 보관한다. 이때, Smart Contract가 실행되어, Results Queue내부의 값을 블록체인 네트워크의 참여하고 있는 노드들에게 Broadcast로 전송한다.

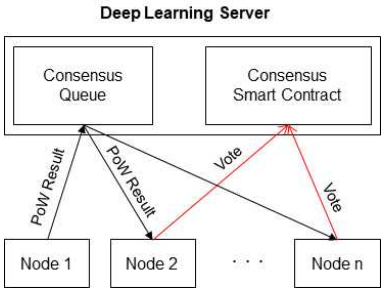

그림 3. 블록 생성 시 첫 번째 절차
Fig. 3. First procedure when creating a block

이때 블록은 아래의 그림 4의 내용과 같이 구성되며, 노드로 전송된 데이터들은 PoW를 사용한 합의 과정을 거치게되는데, SHA-256 해시 알고리즘을 사용한다. 이후 두 번째 절차인 그림 5와 같이 가장 처음 블록의 Nonce를 찾은 노드가 Deep Learning Server의 Consensus Queue로 블록의 해시 값과 Nonce를 전달하고, 이를 다른 노드들이 전달받아 검증작업을 수행한다. 이후 Consensus Smart Contract의 동작을 통해 각 노드의 검증 결과를 전달 받고, 51% 이상의 동의가 있는 경우 해당 블록을 체인에 등록한다.

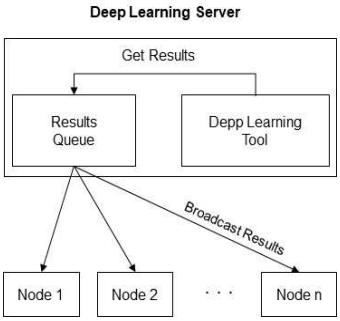

그림 5. 블록 생성 시 두 번째 절차
Fig. 5. Second procedure when creating a block

3.3 딥러닝 학습 결과 롤백기능 설계

제안하는 시스템에서 딥러닝 학습 결과의 롤백기능은 딥러닝 학습 결과가 오류가 발생하였을 때, 수행된다. 각 학습 단계에서 블록체인에 학습 정확도, 학습 오차율, 학습 가중치를 포함하고 있는데, 학습 결과에 오류가 있는 경우, 블록의 내용을 확인하여 이전 시점 중, 가장 높은 정확도를 가지는 상태의 가중치를 가져와 해당 지점으로 복구한다. 해당 기능은 Smart Contract을 사용하여 Roll Back Module에 작업을 요청하는 것으로 수행된다. Smart Contract가 실행되면, 각 노드들은 자신의 블록체인의 내용을 확인하고 복구할 지점을 선택하여 Roll Back Moule에 전달한다. Roll Back Module은 블록체인 네트워크의 모든 노드에게 롤백할 지점에 대한 정보를 수집한 후, 해당 지점으로 롤백을 수행한다. 아래의 그림 6은 롤백을 수행했을 때 블록체인의 변화를 나타낸 그림이다.

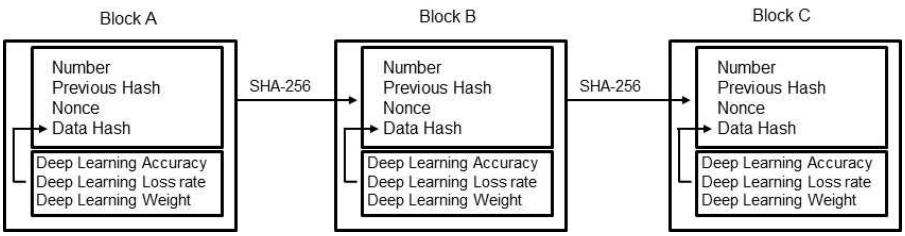

그림 4 블록의 구성
Fig. 4 Contents of Block

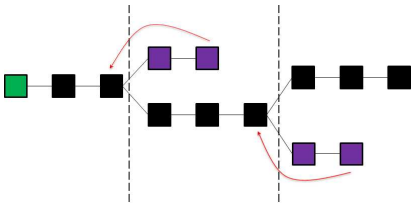

그림 6. 딥러닝 결과의 롤백 기능
Fig. 6. Rollback of Deep learning results

4. 성능평가

본 장에서는 제안하는 기법의 성능평가를 위해 기이더리움 플랫폼의 Smart Contract를 사용하여 서비스를 제공하는 경우 발생하는 비용을 계산하여, 제안하는 시스템에서 절감 가능한 비용에 대해 평가한다. 또한, 기존 딥러닝 롤백 기능과 제안 기술의 롤백 기능의 복구 성능에 대하여 평가한다.

4.1 기존 블록체인의 서비스 비용분석

기존의 PoW를 사용하며 Smart Contract를 통해 세부적인 기능을 제공하는 블록체인 플랫폼은 이더리움이다. 하지만, 이더리움은 Smart Contract를 사용할때, 아래 표 4와 같은 수수료 개념의 Gas가 사용된다.

표 4. 이더리움의 명령어 당 Gas 사용량
Table 4. Gas usage per instruction in Ethereum

Operation	Gas	Description
ADD/SUB	3	Arithmetic operation
MUL/DIV	5	
POP	2	Stack operation
PUSH	3	
BALANCE	400	Get balance of an account
CREATE	32,000	Create a new account using CREATE

제안하는 시스템의 노드가 100개라고 가정하였을 때, 시스템에서 처음 노드가 등록될 때 사용되는 Create 명령어는 100회가 필요하다. 이후 매번 블록을 생성할 때, Results Queue의 딥러닝 결과 값을 확인하기 위해 사용되는 Balance 명령어는 1회, 이를 100개의 노드에게 전달하기 위해 PUSH 명령어가 100회 사용된다. PoW의 수행을 위해 SHA-256 알고리즘을 각 노드당 10회씩 수행한다고 가정한다면, ADD와 MUL을 65,536회 수행한다. 이후 이를 Consensus Queue로 전달하기 위해 PUSH 명령어가 1회, 참여 노드가 블록 생성 결과 확인을 위해 99번의 POP 명령어가 수행된다.

아래의 표 5에서 확인할 수 있듯 고정적으로 사용되는 Gas의 양이 320M개 소모되며, 블록을 생성할 때 마다 약 525,000개의 Gas가 소모되는 것을 확인 가능하다.

표 5. 제안 기술의 명령어 사용량
Table 5. Gas usage per instruction in Ethereum

Operation	Gas	Description
POP	198	Amount per Block creation
PUSH	303	
ADD	19.6M	
MUL	32.7M	
BALANCE	400	Get balance of Results Queue
CREATE	320M	100 account required

실제 사용되는 비용 계산을 위해 2021년 6월 기준으로 1 이더리움(Eth)의 가격은 300만원이며, 1 Eth 당 100M의 Gas로 계산한 결과는 다음과 같다.

$$3.2 * Eth = 9{,}600{,}000\ KRW \quad (1)$$
$$0.525 * Eth = 1{,}575{,}500\ KRW \quad (2)$$

(1)은 초기 네트워크를 생성할 때 사용되는 비용이며, (2)는 블록을 생성할 때 마다 사용되는 비용이다. 만약 1번의 딥러닝을 수행할 때 10번의 사이클로 학습시킨다고 가정하면, 최종 사용 금액은 25,355,000원의 비용이 소모된다. 이를 장기적으로 사용한다면, 서비스를 제공하는데 소요되는 비용이 기하급수적으로 늘기 때문에, 이더리움 플랫폼을 사용하는 것은 어려움이 존재한다. 제안하는 시스템에서는 Smart Contract를 사용하는데 수수료가 사용되지 않기 때문에 서비스 제공에 필요한 비용이 절약된다.

4.2 딥러닝 롤백 성능 분석

기존 딥러닝 솔루션인 Tensor Flow와 Keras에서 제공하는 롤백 기능은 스냅샷을 기록하여 해당 지점으로 복구하는 기능을 사용한다. 또한 MLOps를 사용하는 경우에는 결과 값을 롤백하는 것이 아닌 모델 자체를 재배포하는 방식을 사용하기 때문에, 학습 결과를 보존하지 못한다는 단점이 존재한다.

이에 본 절에서는 Tensor Flow와 Keras의 딥러닝 결과를 롤백하는 기능과 본 시스템의 롤백 기능의 성능을 비교한다.

Tensor Flow와 Keras의 롤백 기능은 가장 최근의 5번째의 결과 값 까지만 복구가 가능하다. 롤백 가능 여부를 $D_{rollback}$ 복구 대상지점이 되는 곳을 D_{target} 현재 학습된 마지막 지점을 D_{end}의 파라메터로 설정하고 표현하면 (1)과 같이 구분된다.

$$D_{rollback} = \begin{cases} D_{target} \geq D_{end} - 5, & Available \\ D_{target} < D_{end} - 5, & Unavailable \end{cases} \quad (1)$$

(1)의 방식으로 구분하여 복구율을 계산하여 그래프로 나타내면 아래의 그림 7과 같이 나타난다.

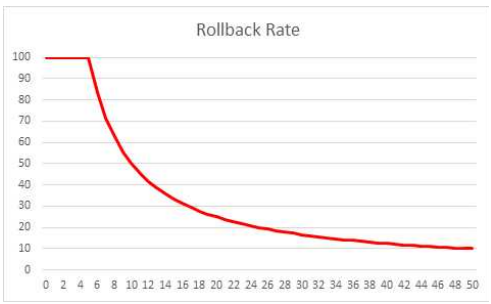

그림 7. Tensor Flow와 Keras의 복구율
Fig. 7. Recovery rate of Tensor Flow&Keras

반면에 제안하는 기법의 경우에는 블록체인을 활용하여 모든 구간에 대한 정보를 블록에 보관하고 있기 때문에, 복구 지점에 대한 제약이 존재하지 않는다.

5. 결 론

본 논문에서는 딥러닝을 수행하면서 학습 중간에 발생하는 값들을 블록체인에 저장하고, 학습 결과에 오류가 발생하는 경우 롤백 작업을 수행하여 딥러닝의 형상관리를 제공하는 시스템을 제안하였다.

제안하는 시스템에서는 기존의 Tensor Flow와 Keras에서 제공하는 스냅샷을 사용하는 방식보다 더 오래된 학습 결과로의 롤백을 수행가능하며, MLOps에서 제공하는 학습 중간 결과 값을 저장하는 기능을 제공한다.

제안기법의 서비스 비용적인 측면을 100개의 노드가 있는 환경의 시나리오로 비교한 결과 처음 블록체인을 생성할 때 960만원의 비용과 블록 생성 시 157만원의 비용이 소모되는 것을 확인하였다. 또한 과 기존의 Tensor Flow, Keras의 롤백 기능을 사용할 때 복구율을 계산한 결과, 초기 5회에는 100%의 복구가 가능하였으나, 6회 이후의 블록 복구 기능은 $\frac{n-5}{n}$만큼 계속하여 감소되어, 50회일 때 10% 수준의 복구율을 가지는 것을 확인하였다. 위의 두 가지 비교를 통해 제안하는 시스템의 우수성에 대하여 평가를 수행하였다.

향후 해당 시스템을 배포하여 실제 환경에서의 테스트를 진행하고, 고도화시켜 딥러닝을 수행하는 환경에서 사용할 수 있도록 연구할 계획이다.

REFERENCES

[1] S. H. Bae, H. J. Lee, Y. T. Shin. “A Study on Deep learing Configuration Managemen t System using Block chain”, Journal of 2021 KIPS, vol 28. pp234-237, 2021

[2] S. Nakamoto. “Bitcoin: A Peer-to-Pe er Electronic Cash System”, 2009

[3] V. Buterin. “Ethereum White Paper: A Next Gerneration Smart Contract & Decentra lized Application Platform”, 2014

[4] IBM. “An Introduction to Hyperledger”, 2018

[5] K. Driscoll et al. “Byzantine Falut Tolera nce, from Theory to Reality”, “Computer safy, Realiabili

ty, and Security. pp235-248, 2003
[6] M. Castro, B. Likov. “Practical Byzantine Fault Tol erance”. Third Symposium on Op erating Syste m Design and Implementation. 1999.
[7] K.Hikodukue. “Python NI YORU SCARPING & KI KAIGAKUSHU TECHNIQUE”, WIKIBO OKS. 2019
[8] TensorFlow. “TensorFlow Guide, Save Model, Che ck Point”. last modified Mar 22. 2021. “https:// www.tensorflow.org/guid e/checkpoint”
[9] J. S. Bong. “A Personal Health Information Sharin g Platform based on Hyperledger Fabric Blockc hain”. Ph.D. diss. University of Soongsil. 2019

저자약력

배 수 환(Su-Hwan Bae) **[정회원]**

- 2016.03 - 2018.02, 숭실대학교 일반대학원 융합소프트웨어학과 석사
- 2018.03 - 현재, 숭실대학교 일반대학원 컴퓨터학과 박사과정

〈관심분야〉 블록체인, 인공지능, 컴퓨터 통신, 정보보호,

신 용 태(Yong-Tae Shin) **[정회원]**

- 1991 - 1994, University of Iowa 컴퓨터학과 공학 박사
- 1995.03 - 현재, 숭실대학교 컴퓨터학부 교수

〈관심분야〉 컴퓨터네트워크, 분산 컴퓨팅, 인터넷 프로토콜, 초고속통신망, 전자상거래 기술