J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

국방분야 인공지능과 블록체인 융합방안 연구

The study of Defense Artificial Intelligence and Block-chain Convergence

김 세 용1* 권 혁 진[1] 최 민 우2
Seyong Kim Hyukjin Kwon Minwoo Choi

요 약

본 연구는 인공지능의 국방 분야 활용 시 데이터 위·변조 방지를 위한 블록체인 기술의 적용방안을 연구 하는데 목적이 있다. 인공지능은 빅 데이터를 다양한 기계학습 방법론을 적용하여 군집화하거나 분류하여 예측하는 기술이며 미국을 비롯한 군사 강대국은 기술의 완성단계에 이르렀다. 만약 데이터를 기반으로 하는 인공지능의 데이터 위·변조가 발생한다면 데이터의 처리과정이 완벽하더라도 잘못된 결과를 도출할 것이며 이는 가장 큰 적의 위험요소가 될 수 있고 데이터의 위·변조는 해킹이라는 형태로 너무나 쉽게 가능하다. 만약 무기화된 인공지능이 사용하는 데이터가 북한으로부터 해킹되어 조작되어 진다면 예상치 못한 곳의 공격이 발생할 수도 있다. 따라서 인공지능의 사용을 위해서는 데이터의 위·변조를 방지하는 기술이 반드시 필요하다. 데이터의 위·변조 방지는 해수함수로 암호화된 데이터를 연결된 컴퓨터에 분산 저장하여 한 대의 컴퓨터가 해킹되더라도 연결된 컴퓨터의 과반 이상이 동의하지 않는 한 데이터가 손상되지 않는 기술인 블록체인을 적용함으로써 문제를 해결할 수 있을 것으로 기대한다.

☞ 주제어 : 인공지능, 블록체인, 해쉬함수, 빅데이터

ABSTRACT

The purpose of this study is to study how to apply block-chain technology to prevent data forgery and alteration in the defense sector of AI(Artificial intelligence). AI is a technology for predicting big data by clustering or classifying it by applying various machine learning methodologies, and military powers including the U.S. have reached the completion stage of technology. If data-based AI's data forgery and modulation occurs, the processing process of the data, even if it is perfect, could be the biggest enemy risk factor, and the falsification and modification of the data can be too easy in the form of hacking. Unexpected attacks could occur if data used by weaponized AI is hacked and manipulated by North Korea. Therefore, a technology that prevents data from being falsified and altered is essential for the use of AI. It is expected that data forgery prevention will solve the problem by applying block-chain, a technology that does not damage data, unless more than half of the connected computers agree, even if a single computer is hacked by a distributed storage of encrypted data as a function of seawater.

☞ keyword : AI, Block-Chain, Hash function, Big-Data

1. 서 론

1.1. 연구배경

블록체인과 인공지능은 전 세계적으로 기술 혁신을 주도하고 있으며, 두 기술 모두 우리의 개인 데이터 뿐만 아니라 비즈니스의 미래에도 깊은 영향을 미치고 있다. 두 기술의 융합은 우리 국방에서 큰 시너지 효과를 얻을 수 있을 것이다. 제 4차 산업혁명의 핵심기술 중 하나인 드론(drone)은 군사 분야뿐만 아니라 민간분야에서도 그 활용도와 가치가 매우 높은 기술이며 이미 널리 사용되고 있다.[1] 그러나 드론은 무선통신방식을 사용한다는 점에서 해킹에 매우 취약하여 보안대책이 필요하다. 특히, 대량의 인명피해가 발생할 수 있는 군사 분야에서의 활용은 매우 신중해야 한다. 미래의 전장 환경은 드론뿐만 아니라 다양한 무기체계에 인공지능 기법이 적용되어 활용일 될 예정인데 치명적 자율살상무기(LAWS : Lethal Autonomous Weapons)에서의 사용함에 있어서 데이터의 위변조가 없도록 하는 보안 적용이 대두되고 있는 실정이다. 치명적인 결과를 초래할 인공지능에 사용할 데이터가 신뢰할 수 없는 데이터가 들어온다면 그 역효과를 매우 클 것이다. 인공지능의 기술은 날로 발전하여 거짓 데

1 Information Planning Bureau, Ministry of National Defense, Seoul-si, 04383, Korea
2 Combat Development Analysis Center, Training and Doctrine Commander, Daejeon-si, 34059, Korea
* Corresponding author (seyong58@naver.com)
[Received 20 November 2019, Reviewed 25 November 2019(R2 18 December 2019), Accepted 08 January 2020]

이터를 생산하기도 하며, 진짜처럼 조작을 하는 기술들이 지속적으로 발전하고 있다.

국방분야 인공지능 적용 및 활용을 위해서 데이터의 신뢰성과 무결성 보장을 위한 연구와 개발이 지속되고 있으며 궁극적으로 데이터의 위변조가 불가능 하도록 노력하고 있다. 그 방법의 하나로 블록체인 기술이 대두되고 있다. 인공지능에서 활용할 데이터에 블록체인 기술을 적용함으로써 보안을 강조하기 위한 내·외부 노력들이 진행 중에 있으며 특히 국방 분야는 데이터보안이 중요하기 때문에 블록체인에 대한 관심도는 갈수록 증대되고 있으나 관심과 기대만큼 연구와 개발 등이 활발하게 진행되고 있지는 않다. 본 연구를 통해서 인공지능과 블록체인 기술을 융합하는 방안과 국방적용의 필요성에 대한 연구가 필요한 실정이다.

1.2. 연구목적

제 4차 산업혁명과 더불어서 국방부는 국방개혁 2.0 추진을 위해 많은 노력을 기울이고 있다. 국방개혁 2.0의 핵심동력으로 AI(인공지능), Big-data(빅데이터), Cloud(클라우드)를 기반으로 추진 중에 있으며, 이를 추진하기 위한 조직으로 육군에 인공지능 연구발전처, 빅데이터 분석센터, 드론봇 추진단 등을 신설하여 운영 중에 있다. 관련 기술 접목을 위한 산학계 전문가들과의 컨퍼런스 자문 등을 통해 지속적으로 발전시켜나가고 있지만 정작 가장 중요한 보안 분야에 대해서는 큰 발전이 없었다. 초지능-초연결-초융합을 강조 하고는 있지만 보안문제를 해결하기 위한 솔루션 적용이나 장비부착 등으로 오히려 역효과가 나오면서 많은 난관에 봉착된 상태이다.

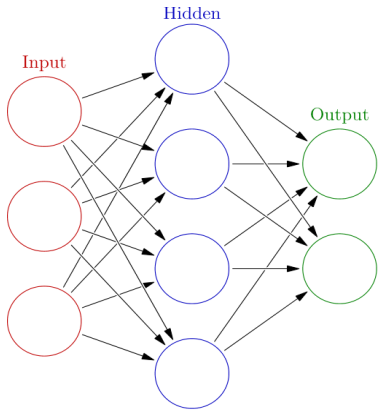
본 연구에서는 이러한 여러 가지 보안 이슈를 해결하기 위한 방법으로 블록체인 기술을 인공지능에 융합하여 국방에서 활용방안에 대하여 알아보고자 한다. 특히 국방분야에서 인공지능을 적용 시 발생할 수 있는 적 위협 시나리오를 데이터 위 · 변조의 형태로 제시하고 데이터 위 · 변조가 인공지능의 예측시스템에 오류를 일으킬 수 있으며 데이터의 위 · 변조를 방지할 수 있는 기술 및 적용방안을 중심으로 연구하였다.

2. 이론적 배경 및 선행연구

2.1. 인공지능

인공지능 기술을 세상에 각인시킨 사건이 바로 2017년 3월 구글의 알파고와 이세돌 9단의 바둑 대국이다. 이 사건으로 인해 딥-러닝(Deep Learning)과 기계학습(Machine Learning)에 대해 관심이 높아졌다. 인공지능을 이해하기 위해서는 딥-러닝과 기계학습에 대해 먼저 살펴 볼 필요가 있다.

인간의 학습은 뇌를 통해 이루어진다. 예를 들어 눈을 통해 받아들인 시각정보가 뉴런을 통해 뇌로 전달되고 뇌는 받아들인 정보를 분석하여 판단하는 과정을 거치며 어떠한 행위의 형태로 표현된다. 이때 여러 개의 뉴런이 연결되면서 복잡한 연산 등을 수행하게 되는데 이와 같은 두뇌의 정보 처리 과정을 모방해서 만든 알고리즘이 바로 인공 신경망(Artificial Neural Network, ANN)이다. 가장 대표되는 응용 분야는 문서, 사진, 동영상 등에서 어떠한 물체를 구분해야 할 때 그 물체의 특징을 확인하고 분석 및 조합하여 자동으로 해당 물체를 검출한다. 인공신경망은 뇌 속의 방대한 뉴런들이 서로 복잡하게 연결된 것과 같이 노드들이 연결되어 있으며. 아래 그림 1에서 각 원 모양의 노드는 인공 뉴런을 나타내고 화살표는 하나의 뉴런의 출력에서 다른 하나의 뉴런으로의 입력을 나타낸다.[2]



(그림 1) 인공신경망의 구조
(Figure 1) The structure of artificial neural network

이러한 인공지능의 장점은 첫째, 감정이 없기 때문에 완전히 논리적이고 오류가 없는 합리적인 결정을 한다. 둘째, 기계는 지치지 않고 위험한 환경에서도 작업할 수 있다. 이를 통해 우주 탐사 또는 광업과 같은 위험한 작업을 수행할 수 있다. 셋째, 데이터 분석을 통해 인공지능을 신뢰하는 것은 회사가 할 수 있는 최선의 결정이다. 인공지능은 구조화되지 않은 데이터를 쉽게 계산할 수 있으

며 데이터를 분석할 때 정확성을 보장하면서 실시간으로 결과를 얻을 수 있다.

2.1.1. 기계학습 및 딥-러닝

인공지능이 다시한번 주목을 받으면서 기계학습(머신러닝)과 딥-러닝 기술이 많이 활용되고 있다. 인공신경망과 같이 데이터를 기반으로 데이터를 평가하고 처리하는 알고리즘을 연구하는 분야를 기계학습이라고 한다. 여기서 주목할 점은 빅 데이터의 등장으로 방대한 양의 데이터를 신속하게 처리하고 정확성 또한 높아지는 효과를 볼 수 있었다. 인공신경망에 빅 데이터를 결합한 것을 우리는 딥-러닝이라고 정의한다. 따라서 딥-러닝은 머신러닝의 한 종류라고 할 수 있다.

인공지능은 데이터를 가공하고 처리하여 딥-러닝을 통해 컴퓨터가 인간보다 빠르고 정확한 예측을 하는 과정으로 요약할 수 있으며, 데이터 종류와 양, 품질에 따라 인공지능이 예측하는 결과가 달라지게 되므로 데이터의 신뢰성이 반드시 확보되어야 한다.

2.1.2. 국방분야 인공지능 활용

미(美) 국방부는 2018.6월 미 국방부 산하에 JAIC(Joint Artificial Intelligence Center, 합동인공지능 센터)를 창설하여 운영 중에 있으며 2019년 미 국방부 AI 전략(DOD AI Strategy)를 발표하여 5개 핵심 분야를 추진 중에 있다. 특히 Maven Project는 구글의 인공지능 전문가들의 기술지원을 받아 군사작전(IS격퇴작전)에 투입되면서 그 효과를 인증 받았다.[3]

한(韓) 국방부도 정보화기획관실에 인공지능정책담당관과 육군의 AI 연구발전처 등의 조직과 전문인력을 보강하여 임무수행 중에 있으며 여러 가지 프로젝트를 통해 국방분야에 적용시키고 있다. 장병 건강검진 결과와 X-RAY 촬영결과를 활용하여 질병을 예측하는 시스템을 구축하였으며, 육군은 과학화 경계시스템에 엣지 컴퓨팅 기술을 적용하여 지능화 경계시스템을 구축하고 있다. 군 장비의 가동률 향상과 수리/정비비용을 절약하기 위해 머신러닝 기반의 군 장비/수리부속 예측모형을 개발하여 활용 중에 있으며 국방 AI 추진전략을 수립하여 단계적으로 추진 중에 있다.[4][1]

1 발표자 학술대회 발표자료 참고

2.2. 블록체인

블록체인이란 여러 대의 컴퓨터에 정보를 복제해 저장하는 분산형 데이터 저장기술로, 다수에 의해 기록을 검증해 해킹 등 위변조 방지가 가능하다. 블록체인은 저장하고자 하는 데이터가 해쉬함수를 통해 암호화되어 '블록'이라고 하는 저장 공간에 저장되며, 저장된 데이터(블록)을 P2P[2] 방식을 통해 서로 연결된 네트워크상의 컴퓨터에 분산 저장하여 참여자의 합의가 이루어지지 않는 한 누구라도 임의로 수정할 수 없고 네트워크에 참여하는 누구라도 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위·변조 방지 기술이다. 이처럼 블록체인은 암호화된 데이터를 네트워크에 참여한 컴퓨터에 분산 저장하는 기술의 한 형태로, 한PC의 데이터가 변경을 시도하더라도 전체의 합의가 이루어지지 않으면 변경이 제한되어 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안 되었다.[5] 이러한 블록체인의 장점은 첫째, 분산되어 있고 중앙장치 없이 데이터를 공유할 수 있다. 이를 통해 블록체인에서의 거래는 중앙통제와 독립적으로 검증하고 처리가 가능하다. 둘째, 분산된 특성으로 인해 내구성이 뛰어나고 일관성이 있다. 공격에 취약한 중심점(중앙점)이 없기 때문에 시스템에 대한 악의적인 공격에 대처하기 용이하다. 셋째, 블록체인 기술이 제공하는 정보, 타임라인 및 신뢰성 등은 모두 정확하다.

2.2.1. 데이터 저장 및 보호

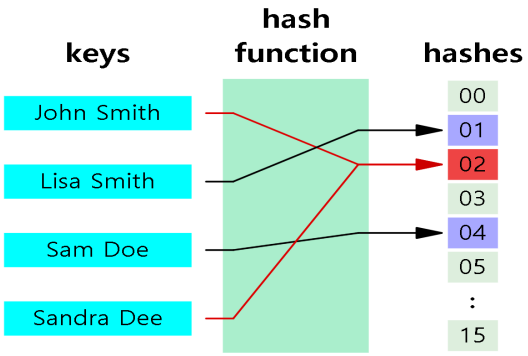
블록체인에서 데이터는 어떠한 형태로 저장되며 보호되는지에 대해 가장 대표적인 비트코인을 통해서 알아보기 위해서는 블록이라는 개념을 알아야 한다. 블록은 유효한 거래의 정보 묶음이라고 표현할 수 있다. 블록은 데이터이고 거래에 참여하는 모든 컴퓨터에 동일하게 저장된다. 비트코인의 블록 하나에는 평균 약 1,800개의 거래정보가 포함될 수 있으며, 블록 하나의 물리적 크기는 평균 0.98Mbyte이다. 또한, 이러한 거래정보를 그림 2와 같은 해시함수를 통해 16개의 숫자와 문자 혼합의 형태로 변환 후 모든 노드의 컴퓨터에 저장하게 되며 PoW작업[3] 방식을 통해 작업이 완료되면 저장된 값은 위·변조가 불가능하게 된다.[6]

2 P2P(Peer to Peer) : 인터넷에서 개인과 개인이 직접 연결되어 파일을 공유하는 것

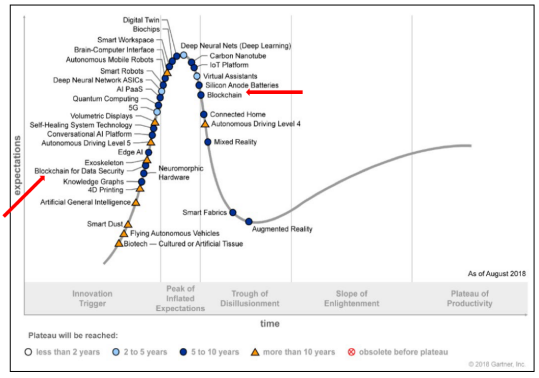
3 PoW(Proof-of-Work, 작업 증명) : 네트워크에서 일정 시간 또는 비용을 들여 수행된 컴퓨터 연산 작업을 신뢰하기 위해 참여 당사자 간에 간단히 검증하는 방식

만약 해킹을 통해 데이터(거래내역)를 변조하게 되면 해시 값이 바뀌게 되고 이미 여러 대 (비트코인 기준 만 여대)에 분산 저장된 동일 데이터와 해시 값을 비교하게 되면 변조 여부를 확인할 수 있다. 해시 값은 점 하나만 찍히더라도 16개의 모든 값이 바뀌므로 위·변조를 쉽게 식별할 수 있다.

2018년 가트너는 그림 3과 같이 블록체인 기술에 대한 동향을 분석하였다. 최초로 등장한 블록체인 기술은 비트코인을 기반으로 한 가상화폐의 등장으로 급성장했다가 현재는 퇴색해 가고 있는 기술로 분류되고 있지만 블록체인 기반의 데이터 보안기술은 최신기술로 떠오르고 있으며, 이 분야의 기술발전과 다양한 분야에서의 활용성이 급성장할 것으로 예상이 된다.



(그림 2) 해시함수의 예
(Figure 2) Example of Hash Function



(그림 3) 최신기술에 대한 하이퍼 사이클 분석결과(가트너, 2018)
(Figure 3) Gartner's own research on emerging technologies plotted along the Hype Cycle(2018)

2.2.2. 국방분야 블록체인

블록체인 기술은 역사가 오래되지 않아서 민간분야에서는 활발하게 이루어지고 있지만 국방 분야에서는 아직 걸음마 단계이다. 국방 분야에서 전술적 활용을 위한 블록체인 기술의 범위를 이해하려면 작전상황의 가시성, 데이터 무결성, 적층 제조, 보고, 운영 계약 및 물류 추정과 관련된 문제에 대한 블록체인 솔루션의 잠재력을 면밀히 조사해야만 한다. 블록체인 기술은 전장에서 장병의 안전 및 건강관리 문제 등을 지원하고, 보안 및 효율성 향상을 위한 데이터 공유 플랫폼을 구축하며, 공급망을 추적하여 문제 발생을 더 잘 예방하고 온도에 민감한 의약품 및 식품과 같은 상품의 추적을 개선 할 수 있다.

미군은 블록체인 기술을 다방면에 적용하기 위해서 미 국방고등기술국(DARPA)등 에서 연구를 추진 중에 있다. 전술 데이터 관리의 가치와 위험이 증가함에 따라 미 육군은 블록체인을 정보 기술 아키텍처 및 정보 기술 기업 현대화에 구현하는 것을 고려하고 있다. 안전한 환경에서 블록체인은 각 계획 수준과 모든 공급 등급에 군 적용 가능성이 있다. 특히 3D 프린팅을 활용한 적층가공(additive manufacturing)의 디지털 데이터 공급망에 블록체인을 적용하고 있으며, 2018 국방수법권(NDAA)'의 섹션 1646에서 사이버 공격과 방어를 위한 블록체인 기술 적용의 잠재성에 대한 브리핑을 통해 블록체인 적용을 추진 중에 있음을 확인하였다. 또한 미 육군의 우주 및 지상 통신국(S&T CD)은 통신 데이터의 위반 및 사이버 보안 문제를 확인하기 위해 블록체인을 활용하고 있다. 잘 알다시피 작전에 신기술 사용을 늘리면 데이터 흐름 수도 증가한다. 미 육군은 지상 및 위성 네트워크를 통한 데이터 흐름이 신뢰할 수 있도록 하려고 한다. S&T CD는 사용자 인증 및 신뢰 정보 공유와 같은 프로세스에서 머신러닝 및 블록체인을 활용할 계획이다. 이 계획은 단절되고 간헐적이며 제한된 대역폭 환경에 적합한 블록체인 합의 알고리즘을 갖추는 것이다. 인증 서비스는 머신러닝, 사용자 / 시스템 데이터 및 네트워크 위협 기록 및 상태를 활용하여 시스템 또는 네트워크 내의 각 사용자에 대한 신뢰 측정을 개발할 예정이다.

한국군도 블록체인의 군 적용을 위해 지속적으로 연구를 진행 중에 있으며, 국방과학연구소에서 2018년에 '블록체인 기술의 군내 도입방안연구'를 진행하였으며 군사분야에서 블록체인 적용가능 분야로 군수물자/수송, 문서/기록관리, 이동형 전투무선망 전장정보관리 사업 등을 선정하였다. 본 연구결과로 블록체인을 군사적으로 적용

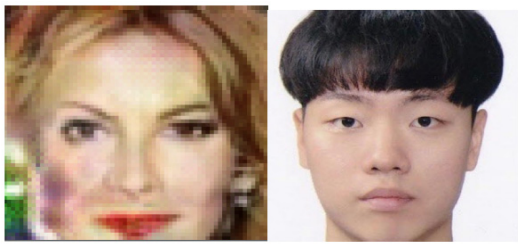
함에 따른 핵심 기대효과는 데이터의 무결성임을 강조하고 있고, 이를 통해 데이터의 품질과 신뢰성을 보장할 수 있다고 하였다.[7]

국방부는 블록체인의 군사적 활용을 신속히 적용하기 위해 관련분야 사업을 지속적으로 발굴하고 있으며, 방위사업청에서는 무기체계 계약 시스템에 블록체인 적용을 위한 ISP(Information Strategy Planning : 정보화전략계획) 수립사업을 진행 중에 있고, 국방부 법무관리관실 주도하에 군사정보체계에 블록체인을 적용하기 위한 연구를 진행 중에 있지만 아직까지 기술을 개발하여 적용하는 사례가 없다.

2.3 인공지능과 블록체인 융합

인공지능과 블록체인 기술의 융합에 대한 연구도 최근에 들어서야 활발하게 이루어지고 있지만 아직 많은 연구보고서나 실증연구 등이 많지는 않다. 최근 들어서 인공지능에서 블록체인을 적용함으로써 보안을 강조하기 위한 많은 연구가 시작되고 있다. Ziq iChen(2018)은 블록체인 상에서 운행되는 AI 분산형 AI 자율화 시스템 연구를 통하여 블록체인을 AI 적용가능성을 증명하였다.[8] F Corea(2017)은 AI와 블록체인의 융합에 대한 연구를 통해 시너지 효과를 분석[9]하였으며, Tshilidzi Marwala and Bo Xing University 에서는 블록체인과 인공지능 연구를 통해 두 기술의 융합을 통한 보안강화 방안을 연구하였다.[10] 인공지능과 블록체인의 융합을 통해 개발된 사례로 스마트 계약 테스트를 향상시키기 위해 만들어진 Singularity.Net이 있으며, 제조사인 Nahame은 블록체인 기술과 인공지능을 통합하여 회사가 감사를 원활하게 할 수 있도록 지원했다. P2P 렌터카 회사는 블록체인 기술을 기반으로 자가용 자동차를 생산할 계획도 있다. 국내에서는 블록체인기반 선거시스템에 AI 본인인증을 위한 방안을 실증연구 하였다. 이를 통해 20 ~ 30대의 투표율 감소를 해결하기 위한 방안으로 스마트폰으로 AI 기술을 적용한 본인인증을 통해 블록체인기술이 적용된 선거시스템을 통한 투표방안을 제시하였는데 그림 4와 같이 거짓데이터와 실제데이터를 활용하여 실증분석 하였다.[11]

인공지능과 블록체인의 융합의 접점은 데이터보호, 보안보장, 신뢰성, IT 인프라의 절약과 비용 효율성, 유연한 AI 구현 등을 들 수 있다.[12] 특히 인공지능은 주로 데이터에 의존하고 있으며 이러한 데이터를 활용 머신러닝(또는 딥러닝)을 통해 스스로를 발전시켜나가는 만큼 국방 분야 AI 적용에서도 민감하고 비밀스러운 데이터를 위해 보호된 분산형 인공지능 시스템을 구축하여 활용하여야 한다.



(a) Fake Data (b) Real Data

(그림 4) 인공지능에 사용된 데이터

(Figure 4) Data Used for Artificial Intelligence

3. 국방분야 인공지능 적용 취약점

3.1. 데이터 위변조 위험성

인공지능 로봇의 위험성을 직시하듯 미군은 '인간 통제력을' 절대 놓아선 안 된다는 입장으로 전장 상태를 판단하는 건 인공지능에 맡기되 마지막 공격 스위치는 인간의 몫으로 남겨뒀다. 그렇다면 왜 인공지능 로봇이 위험할까? 간단하게 표현하면 데이터의 오류이다. 즉, 목표로 하는 인물 또는 물체가 존재한다고 가정할 때 인공지능 로봇은 그림 5와 같이 딥-러닝을 통해 미리 목표에 대한 학습을 하고 실시간으로 탐지 및 탐색을 통해 들어오는 많은 정보를 가공 및 처리하여 자신의 사전정보와 데이터가 일치하는지 판단할 것이다. 만약 데이터의 처리와 인공지능이 정보를 판단하는 과정이 완벽하다면 데이터의 오류는 인공지능이 정보를 판단 및 예측하는데 잘못된 값을 도출하게 될 것이다.

현재 및 미래의 전장에서 국방의 자원들은 다양한 정보통신기술과 통신수단을 활용하여 서로 유기적인 융합을 통해 이루어 질 것이다. 다양한 네트워크를 사용한다는 것은 해킹으로부터 자유로 울 수 없으며 이미 사용되어 지고 있는 기술들이 해킹으로부터 높은 위협을 받고 있다. 특히, 사물인터넷(IoT : Internet of Things)은 서비스를 이용하기 위해서는 인프라(네트워크)에 연결해야 한다. 일반 가정의 경우 유무선 공유기가 이런 인프라에 해당한다. 해커가 공유기에 접근할 수 있다면 공유기에 연결된 각종 사물인터넷 기기에 접근하는 것은 물론, 여기서 발생한 정보를 탈취하는 것도 가능하다. 즉 일종의 도

(그림 5) 딥-러닝을 통한 학습과정
(Figure 5) Training process through Deep-Learning

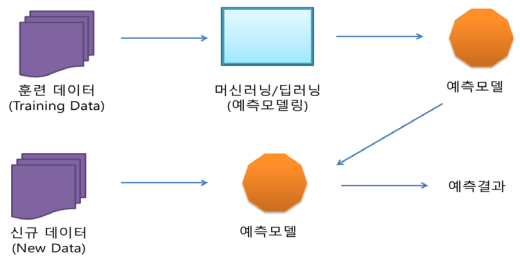
청이 가능한 셈이다. 인공지능 역시 이러한 해킹으로부터 자유로울 수 없기 때문에 딥-러닝 학습 간에 올바른 데이터의 보호가 필요하다.

3.2. 적 위협 시나리오

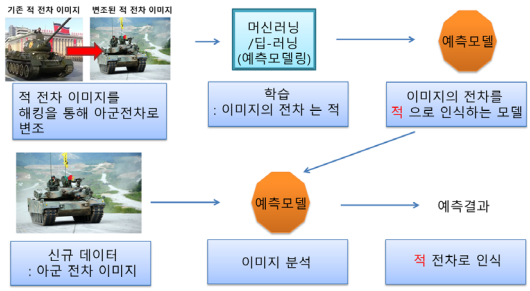
적의 위협 시나리오는 해킹이라는 수단을 통해 여러 가지 방법적인 부분이 있지만 본 연구에서는 인공지능의 기계학습을 방해하기 위한 데이터의 위·변조의 시나리오를 가지고 문제점을 분석하고 해결책을 제시해 보고자 한다.

딥러닝과 같은 머신러닝은 빅 데이터를 활용해 모델의 정확도와 성능을 높인다. 데이터가 많으면 많을수록 학습된 모델이 더 정확해 지지만 지나치게 많으면 학습 과정에서 과적합(over-fitting)이 발생하여 잘못된 모델을 학습할 수 있다. 또한, 잘못된 데이터를 학습하게 되면 당연히 잘못된 모델이 만들어지게 된다. 따라서 우리는 궁극적인 인공지능 로봇을 이용하기 위해서는 딥러닝 단계에서부터 올바른 데이터와 적당량의 데이터를 유지하는 것이 매우 중요하다. 딥러닝의 기본이 되는 것은 무엇인가? 바로 데이터이다. 딥러닝간 이용되는 데이터는 어떤 형태로든 생산되고, 저장되어 있을 것이고 통신망을 통해 연결되어 있다. 따라서 해킹으로부터 매우 위험하며 해킹을 통해 데이터가 손실 또는 조작되어 진다면 딥러닝으로부터 얻어진 예측모델은 잘못된 모델이 될 것이고 이는 인공지능이 잘못된 예측결과를 도출 하는데 영향을 줄 것이다.[13] 아래 그림 6은 훈련 데이터(Training Data)로부터 딥러닝 학습을 통해 만들어진 예측모델이 사용되는 과정이다.

위 과정에서 데이터의 위·변조가 일어나면 예측결과는 다르게 나올 것이다. 그림 7은 기존의 훈련 데이터 중 하나인 적 전차의 이미지를 아군 또는 동맹군의 전차 이



(그림 6) 인공지능을 통한 예측 과정
(Figure 6) Prediction Process through Announcement



(그림 7) 훈련 데이터 위·변조 과정
(Figure 7) Training data forgery and alteration process

미지로 위·변조시 아군전차를 적전차로 예측하도록 인공지능을 기만하는 과정이다.

여기서 보호해야 할 데이터는 훈련 데이터이다. 훈련 데이터를 보호할 수 있는 방법에는 무엇이 있을까? 중앙서버에 폐쇄적으로 보관하면 데이터를 보호할 수 있을까? 그렇다면 지금 이 시간에도 변화하고 보완되는 수많은 데이터들을 어떻게 중앙서버로 옮길 수 있을 것인가? 이 문제를 해결하기 위해서 비트코인으로 세상에 알려진 블록체인 기술을 제시한다.

4. 국방분야 인공지능 및 블록체인 융합방안

4.1. 블록체인 적용시 고려사항

국방 분야 인공지능 적용시 보안문제를 해결하기 위해 블록체인을 적용하는데 고려해야할 사항이 있다. 국방 분야의 데이터는 단순한 텍스트뿐만 아니라 영상, 음성, 신호 등 다양한 형태의 데이터가 존재하는데 앞서 3장에서 설명한 비트코인 형태의 블록체인으로는 이러한 데이터를 처리할 수 없는 구조적 제한사항이 있다. 텍스트 이외의 데이터에는 해쉬 함수를 적용할 수 없는 문제점이 있

었으나 최근에 이러한 문제를 해결하기 위한 새로운 블록체인 기술인 프라이빗 블록체인이 개발됨에 따라 영상 및 이미지를 블록체인에 암호화하여 저장/전송하는 기술을 활용할 수 있게 되었다.

또한 군에서 사용하는 데이터는 비밀자료가 많기 때문에 공개형 블록체인을 적용할 경우 굳이 공개될 필요가 없는 데이터를 공개할 수 있는 문제가 발생한다. 이를 위해 블록체인의 또 다른 기술인 프라이빗 블록체인을 적용한 구체적인 방안을 제시하고자 한다.

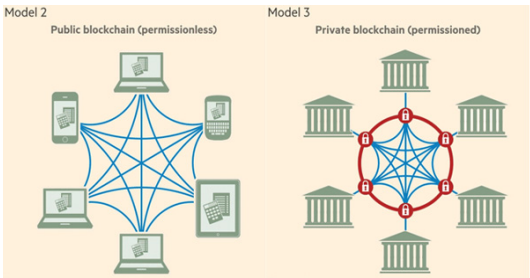
4.2. 프라이빗 블록체인

폐쇄형 블록체인이라고도 불리는 프라이빗 블록체인은 기관에서 특수하게 만든 블록체인이다. 이 네트워크에 들어가기 위해서는 네트워크상에서 만든 인증방식을 통해서 검증된 사람만이 프라이빗 블록체인에 참여할 수 있으며 차이점은 그림 8과 표 1이 같다.[14]

프라이빗 블록체인은 네트워크에 참여하기 위해서는 승인을 받아야하기 때문에 데이터 블록화 또한 승인된 PC만 가능하다. 따라서 외부의 해커나 악의적인 참여자가 프라이빗 블록체인 네트워크상에 참여 또는 데이터 변조가 불가능하다. 또한, 합의 알고리즘도 참여자 중 권한을 가진 사람이 기관의 합의 알고리즘 과정을 거친다. 소수 참여자의 권한을 통해서만 거래가 검증되고 처리되기 때문에 이 네트워크에 참여하지 못하는 사람들은 어떤 블록이 형성되는지 볼 수 있는 방법이 없다.

4.3 국방분야 적용모델(안)

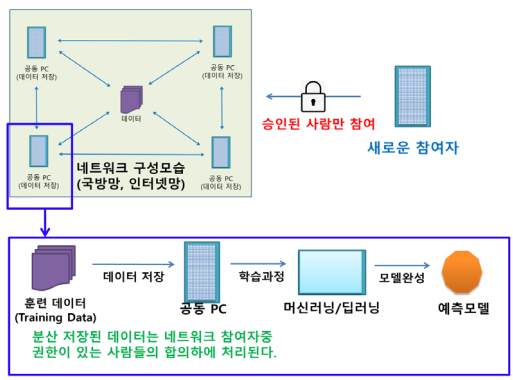
국방분야 인공지능과 블록체인 기술 융합을 통해 데이터의 신뢰성 확보와 안정적인 임무수행여건 보장을 위해 그림 9와 같이 국방 적용 모델 안을 제시하였다.



(그림 8) 퍼블릭 Vs. 프라이빗 블록체인
(Figure 8) Public Vs. Private block-chain

(표 1) 퍼블릭 블록체인과 프라이빗 블록체인의 차이점
(Table 1) Difference between public blockchain and private blockchain

구 분	퍼블릭 블록체인	프라이빗 블록체인
열람/보관 거래승인	누구나 제한 없이 참여가능	필요에 따라 임의로 제한
Consesus (합의문제)	PoW, PoS[4]	BTF[5], PoS
접근/열람	누구나	인가된 기관
사례	비트코인, 이더리움 등	R, Hyperledger 등
장점	높은 안정성, 신뢰성, 투명성, 익명성	정보공유 범위설정가능, 효율성, 확장성
단점	금융 서비스 적용시 느린 속도	신뢰를 바탕으로 한 연결로 기술적 보안성 보장이 제한
활용분야	해외송금, 크라우드 펀딩, 자산 및 정보기록	결재시스템, 신원·문서인증, 무역금융, 스마트계약 등



(그림 9) 국방분야 AI-블록체인 적용모델(안)
(Figure 9) Defense AI-Blockchain Application Model

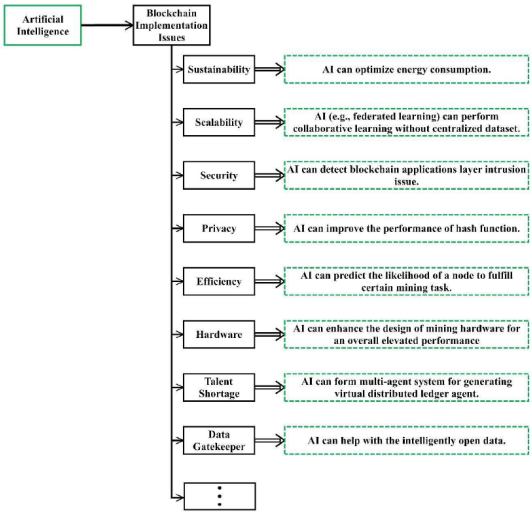
국방분야 인공지능에 사용한 데이터는 클라우드 기반의 주 저장소와 분산저장소에 저장을 하고 사전에 승인된 인원만 접근하도록 통제한다. 접근이 필요한 인원에

4 PoS(Proof of Stake, 지분 증명) : 지분 증명(PoS)은 작업 증명(PoW) 알고리즘의 문제점을 해결하기 위해 도입

5 BFT(Byzantine Fault Tolerance, 비잔틴 장애 허용) : 악의적인 노드가 분산 시스템에 참여한 상황에서도 전체 시스템은 신뢰도 있는 서비스를 제공할 수 있다는 것을 보장

대한 모든 권한은 관리자만 보유하여 엄밀히 통제하고 프라이빗 블록체인망을 구축하여 훈련데이터를 관리한다. 연구의 목적인 해킹 및 데이터 위·변조 상황을 가정해 보면 네트워크에 참여 하거나 데이터가 저장된 PC로 공격을 하게 될 것이다. 그러나 네트워크에 참여하기 위한 승인권한을 얻기가 불가능하고 네트워크에 참여하더라도 블록으로 지정된 데이터를 위·변조가 불가능하기 때문에 안전하게 데이터를 보호 할 수 있다. 이를 구현하기 위해서는 블록체인 기술뿐만 아니라 관련제도와 정책, 기반체계 등의 정립이 필요하다. 또한 다 부처 R&D 사업을 통하여 관련기술의 성숙도를 높이고 이후에 국방에 적용하는 방안을 통해 점차적으로 확산시키는 방법을 통해 관련기술을 확보 및 발전시켜 나가야 한다.

인공지능과 블록체인 기술의 융합은 그림 10과 같이 다양한 시너지 효과를 얻을 수 있다. 지속유지 가능성(에너지소비를 최적화), 확장성, 보안성, 효율성, 공유데이터 관리 등의 시너지 효과를 얻을 수 있으므로 국방 분야에서도 지속적으로 인공지능과 블록체인 기술 융합을 통한 적용을 확산시켜 나가야한다.



(그림 10) AI-블록체인 융합의 시너지 효과
(Figure 10) Synergy of AI-Blockchain Convergence

5. 결 론

제4차 산업은 군의 전투 모습을 획기적으로 변화시킬 것이 틀림없으며, 특히 인공지능 기술을 어떻게 사용하느냐에 따라 군사 강대국으로 도약할 수 있다. 그러나 인공지능은 데이터의 위·변조에 따라 공격대상이 변형될 수 있는 무서운 기술이기도 하다. 따라서 인공지능의 가장 기본인 데이터 보호가 기술도입에 필수적으로 선행되어야 한다. 이를 위해 국방 분야 인공지능과 프라이빗 블록체인 융합을 통해 저장된 데이터가 위·변조가 불가능하도록 하고 데이터 보호와 보안 문제를 해결함으로써 국방 분야 인공지능의 안정성을 확보해 나가야 할 것이다. 특히 국방 분야의 인공지능은 살상 무기에 많이 적용되고 있음을 감안할 때 이 부분은 반드시 지켜야 할 사항임에 틀림없다. 4차 산업혁명의 물결 속에 핵심동력인 인공지능의 안정성과 완전성 유지를 위한 추동력으로 블록체인 기술 적용은 정보보호와 보안문제를 해결해 줄 수 있는 핵심기술이므로 국방 분야 적용을 위해 지속적으로 발전시켜나가야 할 것이다.

본 연구는 이론적 내용과 가상의 시나리오를 바탕으로 국방 분야에 블록체인을 적용한 인공지능 구현을 위한 방안을 큰 틀에서의 아키텍쳐와 방향성을 제시한 점에 큰 의의를 가지고 있다. 관련 내용을 바탕으로 실제 모형을 구축하여 효과성에 대한 입증을 하지 못하였지만 이론적으로 충분히 검증된 내용을 바탕으로 모형(안)을 제시 함 으로써 국방의 적용 가능성에 대하여 이론적으로 접근해 보았다. 추후에는 관련된 모형을 바탕으로 모형의 타당성과 구현 가능성 등을 판단하여 실증분석이 필요하며, 불확실한 전장상황을 가정하여 다양한 상황에서 블록체인과 인공지능 기술을 효과적으로 활용하기 위한 설계를 다시 해 볼 필요가 있다. 현재 연구가 진행 중인 지능형 과학화 경계시스템 사업과 연계하여 프라이빗 블록체인을 적용하여 실증연구 방향을 구상 중에 있으며 소규모 네트워크에서의 가능성을 검증하고 추후 확산방향에 대해서는 지속적인 연구개발이 필요할 것이다.

국방 분야는 일반적인 큰 사회의 축소판과 비슷하면서도 국방이라는 특수성을 가진 약간 더 복잡한 상황에 놓여 있다. 또한 최첨단 기술을 가장 먼저 적용하고 활용해 볼 수 있는 훌륭한 테스트 베드를 보유하고 있다. 아직 시작 단계인 블록체인과 인공지능의 융합방안에 대하여 지속적인 연구와 개발이 필요하며 특히 데이터의 품질과 신뢰성이 중요한 국방에서의 연구개발은 더욱 중요하다.

국방개혁 2.0 추진과 4차 산업혁명, 그리고 국방 혁신(Military Innovation)을 달성하기 위하여 신기술 개발에 대한 아낌없는 투자와 과감한 사업추진을 통해 국방에 신속히 적용할 수 있도록 지속적인 노력이 필요하다.

참고문헌(Reference)

[1] Jae Hyung Kim, 10,000 Drones Overhead… "Saudi Terror" Is It Another?[inside&insight], Dong-A Economy internet news, 2019.9.20. http://www.donga.com/news/article/all/20190920/97489362/1

[2] Sungmin Rue, "BigData Effects on Artificial Intelligence" Korean Institute of Information Technology, Vol 14, No 1, PP. 29-34, 2016. http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06696245

[3] DoD, Summary of the 2018 DoD AI Strategy, 2019.2. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[4] Seyong Kim And 3 others. "Estimation time for mobilization of wartime troops using big data." Proceedings of the Korean Institute of IT Service Conference, 2019 http://scholar.dkyobobook.co.kr/searchDetail.laf?barcode=4010027236595

[5] kwang hoon Kim, "Understanding and Application of Blockchain Technology", Korean Institute Of Industrial Engineering magazine, Vol 25, No 1, PP. 13-19, 2018. http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07415872

[6] Don Tapscott "Blockchain revolution", 2017. https://doi.org/10.1515/ngs-2017-0002

[7] Ahn Jae Hong, ."Blockchain Defense Application Plan." Proceedings of the Korean Institute of IT Service Conference, PP. 196-206, 2018. http://scholar.dkyobobook.co.kr/searchDetail.laf?barcode=4010026888108

[8] Ziqi Chen And 3 others, "AI on Blockchain - The Decentralized AI Autonomic System", Cotex laboratory, 2018. https://www.cortexlabs.ai/Cortex_AI_on_Blockchain_EN.pdf

[9] F. Corea. The convergence of AI and Blockchain. https://medium.com/@Francesco_AI/the-convergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc, 2017.

[10] Block-chain and Artificial Intelligence Tshilidzi Marwala and Bo Xing University of Johannesburg Auckland Park Republic of South Africa, 2018. https://arxiv.org/ftp/arxiv/papers/1802/1802.04451.pdf

[11] Jaejin Lee and 3 others, "Block Chain based Election System by Artificial Intelligence Authentication", Journal of the Institute of Electronics and Information Engineers 56(4), 2019.4, 37-43(7 pages). https://doi.org/10.5573/ieie.2019.56.4.37

[12] https://espeoblockchain.com/blog/decentralized-ai-benefits/

[13] Sohee Park, Daesun Choi "AI Security Issues", Journal of the Korea Institute of Information Security and Cryptology, Vol 27, No 3, pp. 27-32, 2017. http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07192188

[14] Kyung-Hyune Rhee, Siwan Noh. "A Study on the Analysis and Solutions of the Blockchain Security Issues". Journal of Internet Computing and Services (JICS), vol. 20, pp.1-11, 2019. http://dx.doi.org/ 10.7472/jksii.2019.20.4.01

◐ 저 자 소 개 ◑

김 세 용 (Seyong Kim)
2009년 1월 국방대학교 운영분석 석사
2014년 12월 국방부 국방통계 담당
2019년 현재 충남대학교 경영학부 운영관리/MIS 박사과정
현재 국방부 정보화기획관실 국방 빅데이터/인공지능정책담당
관심분야 : 빅데이터, 인공지능, 클라우드, M&S, 통계학, 마케팅
email : seyong58@naver.com

권 혁 진(Hyukjin Kwon)
1989년 성균관대학교 산업공학(공학사)
1991년 성균관대학교 산업공학(공학석사)
2000년 성균관대학교 산업공학(공학박사)
1991년~2017년 KIDA
2017년~현재 국방부 정보화기획관
관심분야 : SW공학, 정보화평가, AI, BigData, IoT
email : khjsjy2001@daum.net

최 민 우 (Minwoo Choi)
2008년 금오공과대학교 기계공학부(공학사)
2008년 육군소위임관
2019년 국방대학교 국방과학학과 운영분석(공학석사)
2019년~현재 육군 교육사령부
관심분야 : 데이터분석, 빅데이터, 인공지능, etc.
E-mail : cmw3818@gmail.com