Journal of KIIT. Vol. 18, No. 11, pp. 109-121, Nov. 30, 2020, pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.11.109

포스트코로나 시대의 언택트 교육 환경을 대비한 블록체인 기반의 온라인 학습 플랫폼

이동혁*, 김상춘**, 박남제***

The Blockchain-based Online Learning Platform for the Untact Education Environment in the Post-COVID-19 Era

Donghyeok Lee*, Sangchoon Kim**, and Namje Park***

2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A04083374)

요 약

최근 전 세계적으로 코로나 사태를 겪으며 많은 변화를 겪고 있다. 과거와 같은 대면방식의 학습, 업무환경 등이 비대면으로 전환되는 추세이나, 너무도 급작스러운 변화에 따라 완벽한 대처를 하지 못하고 있다. 기존의 온라인 학습 시스템은 사전에 제작된 컨텐츠나 영상을 재생하는 방식으로 진행되어 교수자와 학습자 간 쌍방향 커뮤니케이션에 한계점이 있다. 이러한 문제에 따라 실시간 학습에 화상회의시스템을 활용하는 추세이나, 민감 학습정보 노출 등의 우려가 있으며, 부적절한 이용, 실시간 행동판단에 한계점이 있다. 본 논문에서는 블록체인 기반의 온라인 학습 플랫폼을 제안하였다. 제안한 기법은 빅데이터 분석을 통하여 학습자의 행동분석 및 부정학습 방지가 가능하며, 민감 학습정보 노출을 차단한다. 또한 블록체인을 활용하여 학습데이터에 대한 무결성을 유지하고 불법적인 조작을 원천적으로 차단하므로 안전한 온라인 학습 플랫폼을 구축할 수 있다.

Abstract

Recently, the global COVID-19 outbreak has undergone many changes. Learning, work, etc., which were conducted in a face-to-face manner, are shifting to non-face-to-face, but they are not able to fully cope with sudden changes. The existing online learning system is a method of playing pre-made content or video. Therefore, there is a limitation in interactive communication between instructor and learner. Using a video conferencing system for real-time learning has concerns such as exposure of sensitive learning information. In this paper, we proposed a blockchain-based online learning platform. The proposed technique can analyze learners' emotions and behaviors through big data analysis, and prevents exposure of sensitive learning information. In addition, it can maintain the integrity of academic data and establish a safe online learning platform.

Keywords
online learning, blockchain, privacy protection, untact education, online education

* 제주대학교 과학기술사회연구센터, 학술연구교수
- ORCID: https://orcid.org/0000-0001-7516-469X
** 강원대학교 정보통신공학전공 교수
- ORCID: https://orcid.org/0000-0001-9401-4232
*** 제주대학교 초등교육학과 교수(교신저자)
- ORCID https://orcid.org/0000-0003-4434-8933

· Received: Sep. 10, 2020, Revised: Nov. 24, 2020, Accepted: Nov. 27, 2020
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University,
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

최근 발생한 COVID-19 사태는 일상속의 수많은 부분들에 크게 영향을 미치고 있다. 특히, 초중고 뿐만 아니라 대학에도 비대면 원격교육이 권장되면서 언택트 교육환경은 이미 우리 생활속에 보편화 되어가고 있는 상황이다. 이미 원격교육을 위한 온라인 기반의 언택트 학습시스템의 도입이 활발하게 이루어지고 있으며, 포스트코로나 시대에 맞는 원격 학습에 대한 중요성은 날로 증가하고 있다. 현재 많은 학교에서 온라인 수업이 진행 중에 있거나 고려하고 있다[1]-[3]. 과거에도 일부 수업이 온라인으로 진행되거나 대체된 바 있으며, MOOC와 같이 온라인 공개수업이 진행된 바 있다. 그러나 과거 진행된 온라인 수업의 경우 대부분 미리 촬영한 영상을 재생하는 형식으로 진행되는 경우가 많다. 이러한 사전에 촬영된 영상 재생 기반 수업의 경우는 수업의 보조용도로써는 적절하나, 학생과 실시간 소통을 할 수 있다는 오프라인의 장점을 극복할 수 없다.

따라서, 언택트 교육환경은 이러한 과거의 온라인 교육 시스템과는 근본적으로 달리 생각해야 한다. 언택트 교육환경에서는 교수자와 학습자 상호간 실시간으로 교류가 가능해야 하며, 학습자의 반응과 참여도를 실시간으로 확인하여 학습 과정에 실시간으로 반영될 수 있어야 한다. 오프라인 수업의 경우는 교수자가 학습자의 학업상태를 실시간으로 확인 가능하여 이에 대한 적절한 실시간 대처가 가능하나, 온라인 학습의 경우 학습자의 학업상태 확인이 오프라인만큼 용이하지 않은 특성이 있으며 이러한 문제가 오프라인의 학습효과를 온라인으로는 따라잡기 어렵다는 인식을 가지게 한다.

COVID-19 사태 이후로 교육환경에 대한 오프라인에서 온라인으로의 변화가 너무 급작스럽게 찾아왔으며, 현재로서는 완벽하게 대응하지 못하고 있다. 따라서 온라인 수업이 부실하다는 우려와 인식이 커지고 있는 상황이며 이를 극복할 수 있는 언택트 환경에 맞는 온라인 교육 플랫폼에 대한 연구가 시급한 상황이다. 특히, 학습 과정에서 학습자의 학업상태 및 감정상태를 실시간으로 판단하여 교수자가 적절하게 대처할 수 있는 구조가 필요하다.

한편, 언택트 교육환경에서는 프라이버시 보호나 정보보안에 대한 대책이 필요하다. 학습자가 실시간으로 수업을 받는 과정에서 필요에 따라 시스템에 학습정보가 수집될 수 있다[4]. 학습자의 이름, 주소, 연락처 등 기본적인 신원정보 뿐만 아니라 학습과정에서의 부적절한 행위를 잡아내기 위한 영상분석 기술을 위해 의도치 않은 영상 수집이 필요할 수 있으며, 학습 집중도 파악을 위해 영상분석을 통하여 얼굴정보, 동작 등 학습자의 다양한 정보를 수집하여 분석할 수 있다. 이러한 영상정보 분석을 통하여 학습자가 부적절한 행위를 할 경우 적절한 조치를 취하게 될 수 있다. 학습자의 출결상황, 학습태도 등의 분석을 위해 영상감시가 필요하나, 이는 학습자의 개인 프라이버시를 침해할 수 있으며 이러한 정보가 해킹 등으로 외부에 노출될 경우 심각한 개인정보 노출로 이어질 수 있다[5]-[8].

한편, 불법적으로 학업 성취도를 임의로 조작하기 위한 목적으로 학습 참여 영상이나 채점 결과를 임의로 조작할 수도 있다. 특히, 공공 클라우드 환경에서는 이러한 문제가 더욱 심각하다. 클라우드 서비스 제공자 또는 제3자에 의해 학습자의 개인정보 및 민감 학습데이터가 노출될 수 있으며, 이 과정에서 개인정보의 침해로 이어질 수 있다[9]-[12]. 학습 시스템상에서 종단간 암호화를 적용한다 하더라도, 학습데이터의 조작은 감지하기 쉽지 않으며, 특히 내부자가 학습데이터를 임의로 조작한다면 학습자 개인 뿐 아니라 심각한 사회적 문제로 부각될 수 있다. 온라인 학습 시스템에서는 이러한 보안 문제가 항시 존재하고 있다[13]. 따라서 클라우드 기반의 언택트 교육 시스템 환경에는 이러한 보안 문제에 대한 대응책이 반드시 필요하다.

본 논문에서는 이러한 문제를 해결하기 위하여 블록체인 기반의 교육시스템을 제안한다. 블록체인은 데이터 조작을 근본적으로 방지할 수 있어 무결성에 대한 보장이 필요한 온라인 학습 시스템에 적합하다. 제안한 방식은 블록체인을 이용하여 학습정보에 대한 조작이 불가능하며, 블록체인에 학습자의 영상정보를 보관하여 학습데이터의 무결성을 보장할 수 있다. 또한, 학습자 얼굴정보의 마스킹이 가능하여 학습자의 프라이버시를 안전하게 보호할 수 있다는 장점이 있다.

II. 관련 연구

2.1 포스트코로나와 언택트 교육

2.1.1 언택트 시대에 따른 교육환경의 변화

온라인 교육은 공간에 제약을 받지 않는 편리함으로 많은 잠재력을 가지고 있으며, 언택트 시대에서 필수적인 요소가 되고 있다. 과거에도 온라인 교육은 이루어져 왔으며, 특히 사이버대학과 같은 온라인을 위주로 하는 시스템을 갖는 교육기관도 다수 존재하는 상황이다. 온라인 교육환경은 우리에게 낯설지 않으며, 현대인이라면 대다수가 학교 또는 직장에서 온라인 교육을 받은 경험이 있을 것이다.

그러나 포스트코로나 시대의 온라인 교육은 과거의 온라인 학습 시스템으로 해결하는데는 한계가 있다. 과거의 온라인 교육 시스템은 주로 보조적 학습 용도로 활용되어온 경우가 많다. 특히, 미리 제작해 놓은 영상이나 컨텐츠를 재생하는 방식의 온라인 교육이 많으며, 이러한 방식은 오프라인 교육과는 분명히 맥락을 달리한다.

오프라인 교육은 쌍방향 커뮤니케이션이 가능하다는 것이 주요 장점이다. 온라인 교육 환경에서는 이러한 쌍방향 커뮤니케이션에 한계가 있으며, 학습 이후에 퀴즈를 풀게 한다던가, Q/A를 통한 피드백 등으로 이러한 문제를 처리하였다. 그러나 이러한 방식은 온라인 교육의 쌍방향 커뮤니케이션 문제를 해결하는 데 한계가 있다.

이를 극복하기 위하여 ZOOM과 같은 실시간 회의 솔루션을 화상강의 플랫폼으로 이용하여 교육하는 것이 대세이다. 그러나 이는 원격회의 용도로는 매우 적합하나, 학습자의 학업상태를 체계적으로 관리하는 기능을 갖고 있지 않으므로 이러한 시스템을 별도로 구성되어야 한다는 문제가 있다. 또한, 세밀한 영상처리 및 보관이 필요하다. 교수자가 학습자의 학업상태를 원활하게 확인하려면 선명한 영상이 제공되어야 하며, 차후 부정방지를 위해 영상데이터를 저장하는 기능 또한 필요하다. 그리고 해당 영상이 공공클라우드 서버에 저장되어 발생할 수 있는 보안문제 또한 해결하여야 한다.

2.1.2 언택트 교육환경의 보안 위협

온라인 교육 시스템에서는 교수자와 학습자의 개인정보, 출결정보, 평가정보 등 민감 학습데이터를 취급하므로 반드시 보안을 고려하여야 한다. 특히 실시간 언택트 교육 환경에서의 보안 문제는 해결해야 할 사안이 더욱 많이 존재하나 이러한 실시간 언택트 교육 플랫폼의 보안 측면에 대한 부분은 아직까지 많은 논의가 이루어지지 않았다.

먼저, 실시간 언택트 화상 대면 수업을 위해 선명한 수준의 화질이 요구된다. 그러나 HD급 이상의 선명한 화질이 제공될 경우, 사용자의 홍채/지문 등 다양한 생체정보가 직접적으로 노출될 수 있다[14].

실시간 화상회의 솔루션은 영상이 클라우드 시스템을 통하여 전달되는 경우가 많으며, 이러한 클라우드 환경은 내부자 공격에 매우 취약하다. 또한 항시 해커의 공격이 발생할 수 있으며, 이 과정에서 학습자의 실시간 영상정보 및 민감 학습데이터가 노출될 수 있다. 포스트코로나 시대의 언택트 학습 시스템은 기존 오프라인에서의 모든 학습 데이터가 온라인으로 이전될 확률이 높으며, 온라인상에 노출될 수 있는 민감 학습 데이터가 더욱 많아질 수 있다. 따라서 학습자의 개인정보, 생체정보 및 민감 학습 데이터는 반드시 안전한 수단으로 보관할 필요가 있다.

학습자의 위치정보 노출 또한 프라이버시 문제가 될 수 있다. 학습자의 위치가 영상분석을 통해 노출될 수 있으며, 만약 불법적으로 학습 서버에 접근하는 해커 또는 악의를 가진 내부자는 모든 학습자에 대한 위치 파악이 가능하여 이러한 정보를 악용할 수 있다. 학습 마케팅 등의 기초자료로 수집될 수도 있으며, 최악의 경우 범죄를 위한 자료로 사용될 수 있어 학습자의 위치정보도 안전하게 보호해야 한다.

그리고 민감 학습 데이터인 학업성취도 정보는 반드시 안전하게 보호해야 한다. 악의를 가진 해커 또는 내부자가 성적정보를 임의로 수정할 경우, 사회적으로 큰 혼란에 빠지게 할 수 있다. 불법적인 학업성취도 조작이 발생 가능함에 따라 교육환경의 온라인 이전에 대한 불안감을 조성할 수 있어 학업성취도는 온라인 전환의 주요한 보호대상이 된다.

2.2 기존 온라인 교육 시스템 보안 기법

온라인 교육 시스템은 해커의 침입 위협, 내부자의 정보 접근이 가능하므로 보안에 대한 이슈가 꾸준히 제기되었다. May 등은 원격 온라인 교육 환경에서의 보안 문제와 개인정보보호 문제가 증가하고 있어 참가자의 개인정보를 강력하게 보호해야 함을 언급하였다[15]. 해당 연구에서는 학습자가 자신의 개인정보에 대한 노출에 대해 우려하고 있음을 지적하였으며, 학습 데이터를 안전하게 보호하는 것이 무엇보다 중요함을 강조하였다. 이를 위해 개인정보보호, 학습 리소스의 신뢰성, 원활한 액세스, 주소 및 위치 개인정보보호, 싱글사인온(SSO), 디지털 권한 관리(DRM) 등이 온라인 교육 시스템에서 중요한 요소임을 강조하였다. 또한 Luminita 등은 온라인 교육 플랫폼에 대해 접근제어, 기밀성, 무결성, 가용성, 부인 방지와 같은 기본 보안 측면을 충족해야 함을 강조하였으며, 온라인 교육 환경에서 영향을 미치는 취약점들을 언급한 바 있다[16]. Weippl 등은 학습 시스템 보안을 위해 고전적인 CIA(기밀성, 무결성 및 가용성) 접근방식을 기반으로 다른 모든 요구사항도 이러한 세가지 기본 속성으로 설명할 수 있다고 주장하였다[17]. Meghna 등은 온라인 교육 플랫폼의 보안 문제 및 취약성에 대해 평가하였으며, 현재의 이러닝 학습 환경에 대한 취약점과 결함을 발견하고 이러닝 보안을 위한 보안모델을 설계하였다[18].

Meghna는 그림 1과 같이 보안모델을 계층적인 관점에서 접근하였고, 계층상 최상위계층에 관리자를 배치하고, 학습 리소스에 대한 접근을 관리자 및 교수자에 의해 제어할 수 있도록 하였다. 이러한 방식을 통해 최상위계층에서 전단위 통제를 가능하게 하여 보안 위협을 방지하는 특징이 있다. 한편, Chuyang 등은 블록체인을 이용한 이러닝 기법을 제안하였다[19]. 해당 연구에서는 온라인 교육 생태계를 위해 퍼블릭 블록체인과 프라이빗 블록체인의 결합을 통한 이러닝 평가 및 인증을 위한 블록체인 시스템을 제안하였다.

Chuyang이 제안한 보안 모델은 그림 2에 나타나 있다. 이와 같이 온라인 교육에 블록체인을 적용한 기법은 개방적인 이러닝 환경 구축에 도움이 된다는 장점이 있다. 그러나 해당 연구는 학습데이터에 대한 블록체인 구성에 대한 내용이 핵심이며, 학습자를 어떻게 인증할 것인지, 혹은 학습자의 행동 및 반응을 어떻게 분석할 것인지에 대한 여부를 언급하지 않고 있다. 기존의 온라인 교육환경은 오프라인 환경의 보조수단이라는 인식이 강하였으나, 언택트 교육환경은 온라인이 중심이 되며, 현장감 있는 쌍방향 소통 학습을 위해서는 반드시 이러한 고려가 필요하다.

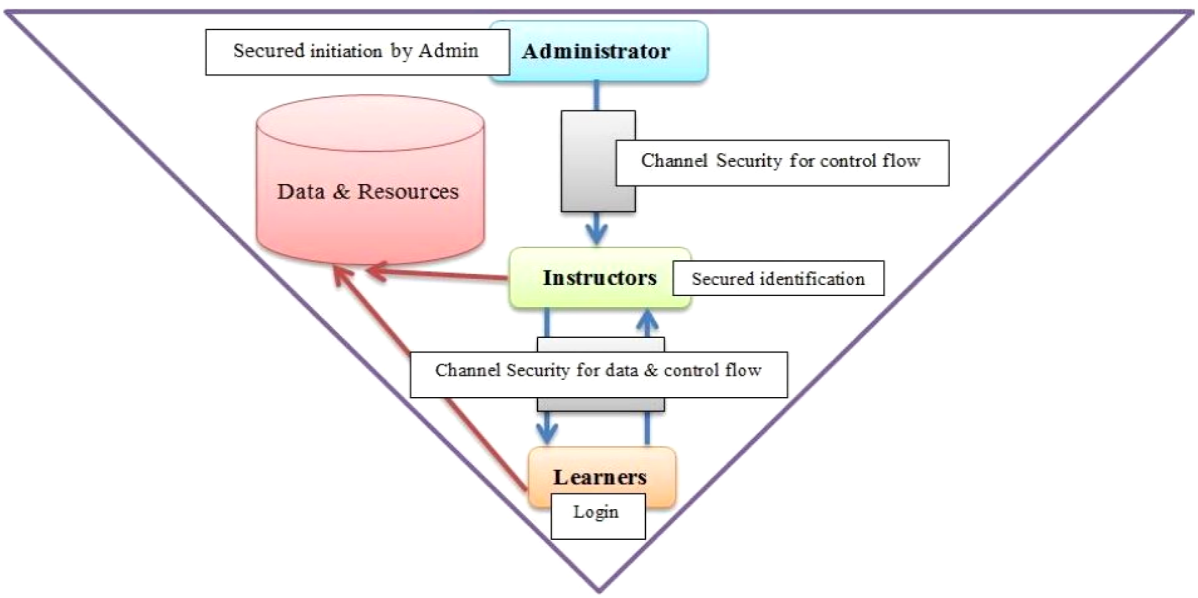

그림 1. Meghna의 이러닝 보안모델 [18]
Fig. 1. Meghna's e-learning security model [18]

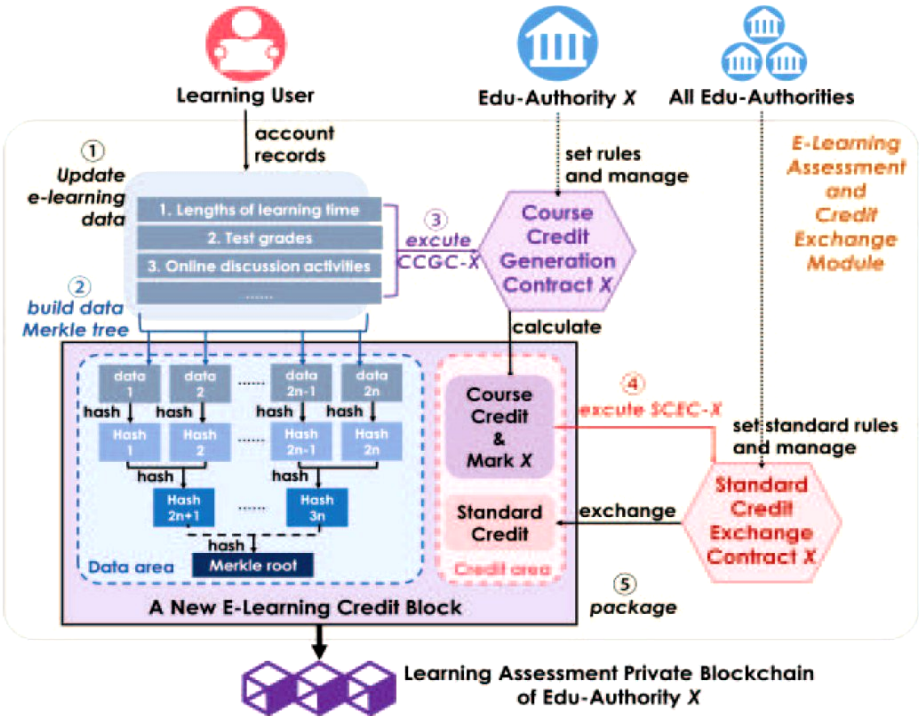

그림 2. Chuyang의 이러닝 보안모델 [19]
Fig. 2. Chuyang's e-learning security model [19]

현재까지 온라인 교육 시스템의 보안 위험성에 대해 많은 연구가 되어 왔으나, 주로 미리 촬영한 영상을 재생하는 기존 LMS(Learning Management System) 환경에서의 보안에 대한 연구에 초점이 맞춰져 있다. 이러한 방식으로는 쌍방향 의사소통이 필수적인 실시간 언택트 교육에 대한 보안 문제는 완벽하게 해결할 수 없다. 언택트 교육환경은 기존의 온라인 교육시스템과는 맥락을 달리한다. 교수자, 학습자, 콘텐츠, 평가 등 다양한 구성요소가 고려되어야 하며, 이러한 구성요소들이 안전하게 보호되어야 한다[20]-[29].

본 논문에서는 블록체인 기술을 이용한 안전한 온라인 교육 플랫폼을 제시하였다. 특히, 민감학습 데이터 조작 방지가 가능하고 영상 노출에 따른 프라이버시 보호 문제를 해결하였다.

III. 새로운 온라인 학습 플랫폼 제안

본 장에서는 먼저 언택트 환경에서의 온라인 교육 시스템 구축을 위한 고려사항을 살펴보고, 이를 반영한 새로운 온라인 학습 플랫폼을 제안한다.

3.1 언택트 학습 플랫폼의 고려사항

언택트 학습 플랫폼의 구축을 위해서는 다양한 고려사항이 필요하다. 본 절에서는 언택트 학습 플랫폼의 고려사항을 살펴본다.

3.1.1 실시간 행동분석

언택트 학습은 근본적으로 오프라인 학습에 비해 학습자의 행동이나 감정을 실시간으로 파악하기 어렵다. 실시간 화상회의 솔루션을 사용하여 학습자의 얼굴을 확인할 수는 있지만, 오프라인에서 대중과 직접 마주하는 것과는 차이가 존재할 수 밖에 없다. 따라서 언택트 학습이 원활이 이루어지려면 이러한 학습자의 실시간 행동분석이 필수적이다. 온라인 시스템의 장점을 살려 학습자 행동분석이 시스템적으로 자동화되어 수집 및 분석되고, 교수자에게 적절하게 전달되어야 하며, 교수자는 이를 실시간 확인하고 적절히 대응할 수 있어야 한다.

3.1.2 가용성 보장

언택트 학습시스템은 가용성이 보장되어야 한다. 가용성을 고려하지 않은 채 접속폭주 등으로 인하여 학습시스템을 통한 학습이 원활히 이루어지지 않는다면 학습자의 학습권 침해로 이어질 수 있다. 또한 온라인 교육에 기술적으로 문제가 발생할 경우 학생들의 학습공백이 발생할 수 있어 이러한 가용성 문제는 반드시 고려되어야 한다. 특히, 학습자의 장소, 지역에 구애받지 않고 가용성이 보장될 수 있어야 하며, 천재지변 등 부득이한 상황이 아닐 경우 가용성은 보장되어야 한다. 이를 위해 5G등 최신 네트워크 기술을 활용할 수 있어야 하며, 학습자의 장비에 대한 구애를 최소화하여야 한다.

3.1.3 학습데이터의 무결성 유지

학습데이터는 반드시 무결성을 유지해야 한다. 특히, 민감학습 데이터중 하나인 학업성취도 데이터는 반드시 무결성을 유지해야 하는 항목으로써, 학업성취도에 대한 조작이나 위해가 발생할 경우 사회적으로 큰 혼란을 가져오게 될 수 있다. 한번 저장된 학업성취도 데이터는 어떠한 일이 있어도 수정되어서는 안되며, 만약 부득이한 수정이 필요한 경우 적절한 사유와 로그를 남기고 추가적으로 데이터를 더하는 방식으로 저장해야 하며, 기존 저장된 학업성취도 데이터 또한 그대로 보존해야 한다.

3.1.4 학습 영상정보의 안전한 관리

실시간 학습 과정에서 학습자 및 교수자의 영상정보가 전달된다. 학습자의 학습태도, 행동분석, 출석 확인 등을 위하여 영상이 시스템에 수집될 필요가 있으며, 이러한 데이터는 직접적으로 학습자의 프라이버시 침해 원인이 될 수 있다. 특히, 학습 과정에서의 영상정보상에 학습자의 얼굴인식 정보나 홍채/지문 등 생체정보가 노출될 수 있으며 내부자 또는 해커 등 악의를 가진 자에 그대로 노출될 수 있어 영상정보에 대한 안전한 관리가 필요하다.

3.2 제안 방식 설계

제안하는 방식은 그림 3에 나타난 것과 같다. 해당 시스템은 LMS 서버 및 블록체인 서버, 학습자가 접속할 수 있는 클라이언트로 구성되어 있으며, 클라이언트는 PC 또는 모바일 환경이 될 수 있다. 교수자와 학습자는 LMS 서버를 통하여 수업을 할 수 있으며, 각 학습자는 그에 대응되는 블록체인을 가진다. 해당 블록체인에는 학습자의 얼굴정보, 영상 분석에 따른 행동 분석 정보, 접근 로그, 평가 정보를 담고 있다. 즉, 각 블록체인에는 학습자의 수업 과정에서의 학업정보가 기록되며, 한번 저장되면 블록체인의 특성상 변경이 불가능하다. 이러한 특성은 학습과정에서의 악의적인 성취도 조작을 방지하는데 매우 효과적이다. 그림상에서 학습자와 매핑되는 블록체인의 한 블록은 개념적인 부분이며, 실제 블록체인은 블록체인 서버에 저장된다. 블록체인이 담고 있는 데이터는 암호화되어 있으며, 외부인은 불법적으로 원본 데이터를 확인할 수 없다.

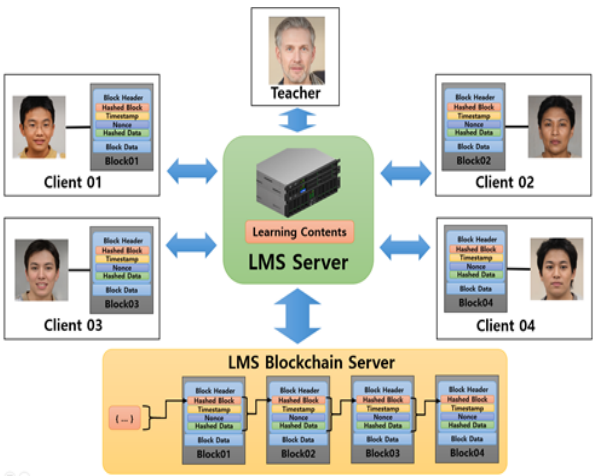

그림 3. 블록체인 기반 학습 시스템
Fig. 3. Blockchain-based learning system

블록체인에 저장되는 데이터의 유형은 그림 4와 같다. 블록체인의 데이터상에는 아래와 같은 4가지의 정보를 포함하고 있다.

a) 학습자의 신원 : 학습자의 신원 정보가 저장되며, 개인의 식별정보는 반드시 암호화되어야 한다.

b) 마스킹된 얼굴 데이터 : 원본 이미지를 저장하지 않고 마스킹 처리 후 저장한다. 얼굴 정보를 그대로 저장할 경우 프라이버시 노출이 발생할 수 있다. 따라서 프라이버시 보호를 위해 얼굴 영상에 대한 적절한 마스킹기법을 적용하여 저장한다.

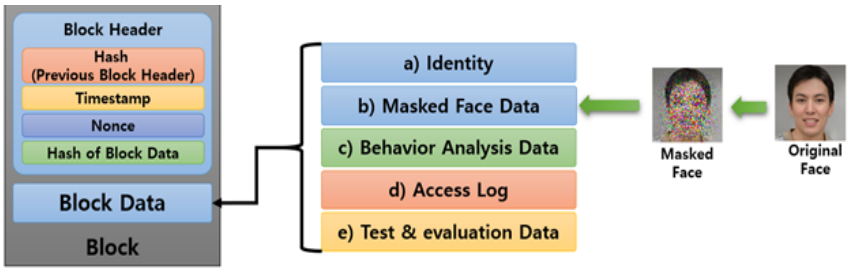

그림 4. 블록체인에 저장되는 데이터 유형
Fig. 4. Types of data stored in the blockchain

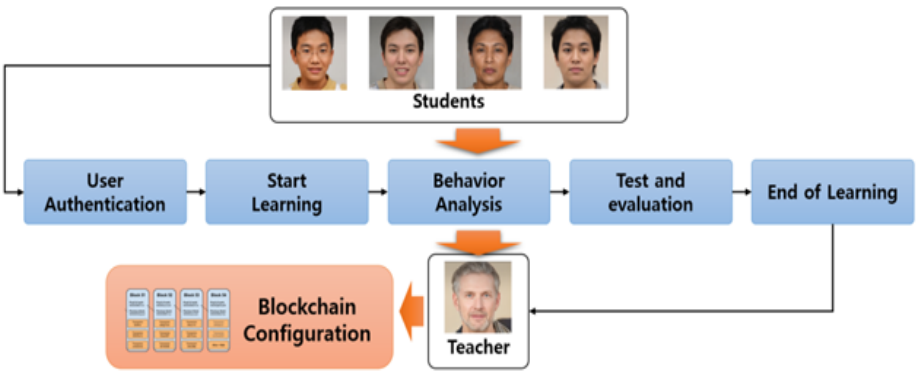

그림 5. 제안 방식의 수행 절차
Fig. 5. Procedure of the proposed method

c) 행동 분석 데이터 : 학습 과정에서의 행동을 분석한 결과를 저장한다. 행동 분석은 영상 분석을 통해 이루어지며, 부적절한 행동 방지 및 학습자의 집중도 등을 판단할 수 있다.

d) 접근 로그 : 학습자가 LMS 서버에 접근한 내역(학습 시작 및 종료)에 대한 로그를 저장한다.

e) 테스트 점수 데이터 : 테스트를 수행한 결과값을 저장한다. 테스트 결과는 민감한 개인정보이므로 암호화하여 보관해야 하며, 외부인에게 노출되어서는 안된다.

3.3 수행 절차

학습 내용의 블록체인 저장을 위해 진행되는 절차는 그림 5와 같다. 먼저 ID/Password 및 얼굴 안면인식을 통한 학습자 인증이 수행되고, 학습이 시작되면 LMS 시스템에서는 학습자의 실시간 행동분석을 수행한다. 학습자의 실시간 행동 분석은 빅데이터, 인공지능 등을 통해 다양한 감정 및 행동에 대한 파악이 이루어 질 수 있으며, 학습자의 행동 분석 내용은 실시간으로 교수자에게 전달된다. 교수자는 해당 데이터를 수업의 효율성을 높이기 위한 데이터로 활용할 수 있다.

학습이 이루어지고 난 후에는 평가가 수행되며, 학습에 대한 평가가 이루어지고 난 후 학습이 완료되면 교수자는 학습 종료를 승인한다. 이 시점에서 학습 데이터가 블록체인에 안전하게 저장되며, 해당 학습 데이터는 수정할 수 없게 된다.

블록체인에 저장된 데이터는 블록체인의 특성상 수정이 불가능하며, 만약 불가피하게 수정이 필요한 경우는 교수자가 사유를 등록하고 새로운 블록체인을 추가로 입력하여야 한다. 이 경우에도 기존 저장되었던 성적 데이터는 지워지지 않으며, 학업성취도 조회시에는 가장 최신에 업데이트된 데이터를 가져오는 것으로 최신 정보를 유지할 수 있다. 이와 같이 학업성취도는 조작이 불가능한 상태로 안전하게 저장 및 관리된다.

3.3.1 학습 시작 단계

학습 시작에 앞서, 로그인을 통하여 학습자가 정당한 사용자인지 여부를 확인하여야 한다. 제안한

방식에서는 사용자 인증을 위해 2-factor 인증을 수행한다. 인증을 위해 사용자의 ID/Password 인증과 얼굴 인식 인증이 요구되며, 얼굴인식이 정상적으로 되지 않는 경우 인증되지 않은 것으로 처리하는 것이 원칙이다. 이러한 방식으로 불법적인 대리 학습을 방지할 수 있다.

그러나 학습자의 안면인식 정보가 사전에 존재하지 않거나 특별히 허가를 득한 경우 학습자의 아이디만으로도 인증이 가능하며, 로그인 즉시 얼굴을 등록하여야 한다. 즉, 얼굴 인식을 위해 사전에 등록된 안면인식 정보가 필요하며, 이러한 얼굴인식 기반 인증은 본인이 아닌 다른 사람의 불법적인 접근을 할 수 없게 한다. 특히, 평가를 위한 시험을 치루는 과정에서는 더욱 얼굴 인식 기반 인증을 철저하게 수행하여 부정행위를 방지한다.

3.3.2 학습 진행 단계

기존의 학습 성취도 분석은 주로 사후평가에 집중되어 적시적인 교육환경을 제공하는 것이 어려운 편이다. 예를 들어 학습자가 수업에 얼마만큼 집중하는지에 대한 여부는 기존의 수업에서 판단하는 것이 쉽지 않았다. 제안하는 언택트 교육 시스템은 이러한 학습자의 행동을 얼굴인식을 통하여 실시간으로 분석해 준다는 측면에서 적시적인 교육환경을 제공할 수 있다. 학습이 진행되는 동안 영상 분석을 통하여 학습자의 행동을 파악한다. 학습자의 행동 분석을 통해 수업의 집중도를 판단할 수 있으며, 이러한 영상 분석은 시각적, 언어적 장벽을 극복할 수 있다는 장점이 있다. 만약 학습자가 적절하지 않은 행동을 취할 경우 경고성의 알람 등이 발생할 수 있다. 그리고 교수자는 학습자의 집중도를 실시간으로 확인하며 적절하게 대응할 수 있다. 만약 학습자의 집중도가 매우 저조할 경우, 교수자는 학습자의 주의를 집중시킬 수 있는 적절한 방안을 선택할 수 있어 효율적인 교육을 진행할 수 있다.

3.3.3 테스트 및 평가 단계

수업이 끝나면 적절한 온라인 테스트를 진행할 수 있다. 학습자의 평가 결과는 블록체인상에 기록되며, 블록체인은 무결성을 보장한다는 특징이 있어 데이터의 조작이 불가능하다. 이러한 방법을 통해 평가 결과에 대한 악의적인 조작을 원천적으로 차단할 수 있다. 한편, 학업성취도 등 평가 데이터는 학습자에게 민감한 개인정보로써 비밀리에 취급될 필요가 있다. 즉, 학업성취도 등 평가 데이터는 기밀성과 무결성을 동시에 유지할 필요가 있다. 따라서 블록체인에 저장 시 평가 결과는 반드시 암호화하여 저장해야 한다. 암호화 과정에서, 비밀키는 시스템 최고관리자 및 교수자만 알고 있어야 하며, 학습자를 포함한 다른 관계자는 어떠한 경우에도 암호화 키를 알 수 없도록 한다. 따라서 허가되지 않은 자는 학습 데이터에 원천적으로 접근할 수 없다.

3.3.4 학습종료 및 저장단계

전체 학습이 끝난 후 교수자의 승인에 의해 학습 블록체인이 구성된다. 이 시점에서 각 블록체인의 헤더 정보가 구성되고, 이를 포함한 모든 블록체인 데이터가 저장된다. 블록체인은 이전 블록의 헤더정보를 해쉬(Hash)처리한 값이 다음 헤더에 저장되는 특징이 있어 블록체인 헤더를 사전에 임의로 구성할 수 없다. 따라서 학습 종료 시점에서 교수자의 승인을 통해서만 블록체인이 구성될 수 있으며 학습자의 학습정보가 저장된 각 블록체인의 헤더가 체인화되어 블록체인 서버에 저장된다. 교수자의 승인을 통해 블록체인이 기록된 이후 학습에 대한 데이터는 수정할 수 없으며, 차후 수정이 필요시는 별도의 블록체인을 구성하여 추가로 저장하여야 한다.

Ⅳ. 제안기법 분석

4.1 안전성 측면

제안한 방식에 대하여 조작 방지, 학습데이터 보호, 부정사용 방지, 행동 분석, 프라이버시 보호 측면에서 안전성 분석을 수행한다.

4.1.1 불법 조작 방지

제안한 방식은 학습 이후에 교수자의 승인에 따라 모든 학습 데이터가 블록체인으로 저장된다. 이

러한 블록체인 방식을 적용함에 따라 근본적으로 데이터에 대한 조작이 불가능하다. 특히 불법적인 학업 성취도의 조작이 불가능하며, 접근 로그와 같은 사후 추적에 필요한 데이터를 남기고 있으므로 데이터의 조작이 원천적으로 불가능하다.

4.1.2 학습데이터 보호

악의를 가진 자에 불법적으로 학습데이터가 노출된다면 학습자 개인정보의 침해 소지가 될 수 있다. 본 논문에서는 학습데이터에 대한 보호를 위해 암호화를 적용한다. 특히, 테스트 및 평가 데이터에 대한 정보를 암호화하여 보관하므로 학업성취도 등 민감 학습 데이터를 안전하게 보관할 수 있다.

4.1.3 불법 인증 방지

기존의 인증 방식은 ID/Password 혹은 공인인증서와 같은 single-factor 인증을 수행하는 것이 일반적이다. 그러나, 언택트 환경의 온라인 교육에서는 이러한 방법은 적절하지 않다. 예를 들어, 한차례 인증과정을 거친 후 정작 학습을 다른사람으로 교체하여 진행하는 경우는 기존의 single-factor 인증기법으로는 감지가 불가능하다. 불법적인 학습환경 접근에 따른 적절하지 않은 테스트 환경이 조성될 수 있어 이러한 문제는 반드시 해결하여야 한다.

제안하는 방식에서는 2-factor 인증을 수행한다. ID/Password 방식과 얼굴영상 인식기반 인증을 동시에 수행함으로써 본인이 아닐 경우 정상적으로 학습을 진행할 수 없도록 하고 있다. 얼굴인식 기반의 2-factor 인증이 갖는 의미는 크며, 얼굴인식이 아닌 지문 등의 생체인식을 가정할 경우, 한번의 인식 과정을 거치면 결국 다른 부적절한 임의의 학습자로 교체가 가능하여 허점이 발생할 수 있다. 얼굴인식 기반의 2-factor 인증을 통해 학습 과정에서 정당한 사용자가 아닌 다른 사람이 학습을 진행하고자 할 경우, 정상적으로 인증이 되지 않으므로 불법적인 학습을 원천적으로 방지할 수 있다.

4.1.4 영상정보 보호

학습 과정에서 학습자의 얼굴영상을 수집하게 되며, 얼굴영상 수집은 정당한 학습자 여부를 판단하는 필수적인 요소이다. 이러한 얼굴 영상 수집은 프라이버시 측면에서 문제가 될 수 있다.

제안하는 논문에서는 안면인식을 통해 수집한 사용자의 얼굴이 블록체인에 보관 시 마스킹 처리되어 저장된다. 이 경우, 실제 얼굴 데이터는 저장되지 않으며 마스킹된 데이터만 저장되므로 학습자의 프라이버시를 보호할 수 있다.

4.2 효과성 측면

4.2.1 학습자 행동분석

학습자 영상정보 기반의 행동 분석을 통해 학습자가 부적절한 행동을 취할 경우 적절한 조치를 취할 수 있다. 영상정보는 빅데이터/인공지능을 통하여 학습자의 감정, 행동 패턴 등을 분석해 낼 수 있으며, 구체적으로 교수자에게 전달할 수 있다.

한편, 행동 분석을 통해 사용자의 집중도를 체크할 수 있으며, 이렇게 수집된 집중도 또한 교수자에게 전달된다. 교수자는 학습자의 집중도 정보를 수업에 활용하여 학습자의 집중도를 높이기 위한 다양한 방법을 실시할 수 있다.

4.2.2 가용성 측면

학습데이터를 적시에 가져오지 못할 경우 시스템의 가용성이 훼손될 수 있다. 본 논문에서 제안하는 방식은 학습데이터가 블록체인상에 저장된다. 블록체인은 다수의 노드에 데이터를 보관하므로 가용성에 있어 매우 효과적인 시스템이다. 즉, 제안하는 방식은 블록체인 방식의 특성에 따라 학습데이터의 가용성을 보장할 수 있으며, 저장되는 노드의 개수가 증가할수록 가용성을 더욱 확보할 수 있다.

4.3 기존 방식과의 비교

기존의 온라인 학습시스템 보안 기법은 주로 LMS 학습시스템 자체에 대한 보안 대책이 주요 관점인 측면이 있다. 그러나, 언택트 교육환경은 온라

인 학습에서 현실감 있는 학습환경과 원활한 피드백 등이 매우 중요하며, 학습자의 영상정보에 대한 적극적인 취급방법 또한 충분히 고려되어야 한다.

Meghna의 방식은 계층구조를 통하여 접근제어 측면에서의 장점이 있으나, 정당한 로그인 후 학습 과정에서 학습자를 임의로 교체하는 경우 등에서의 불법적인 학습 참여를 감지할 수 없다. 제안한 방식은 영상 얼굴인식을 통하여 정당한 학습자인지 여부를 감지할 수 있다. 학습자 본인이 아닌 경우에는 즉시 파악하여 적절한 조치가 가능하다. 또한, Meghna의 방식은 접근제어 측면에서의 보안 관점에서 접근하여 데이터 자체의 조작이나 변조에 대한 감지가 불가능하다. Chuyang의 방식 및 제안한 방식은 학습 데이터를 블록체인에 저장하므로 불법적인 조작을 할수 없어 이러한 불법적인 학습데이터 조작의 원천적인 방지가 가능하다. 한편, 학습자 행동분석의 경우 Meghna 및 Chuyang의 방식에서는 언급하고 있지 않으나, 제안한 방식에서는 학습 과정에서 학습자 행동분석 데이터를 활용하여 교수자에게 정보 제공이 가능하다. 아울러 기존 연구에서는 학습자 개인정보보호에 대한 내용을 고려하고 있지 않으나, 제안한 방식에서는 학습 데이터 암호화 및 영상 데이터 비식별화를 통하여 학습자의 프라이버시를 안전하게 보호할 수 있다. 표 1은 기존 방식과 제안 방식을 비교하고 있다.

표 1. 제안 방식 비교
Table 1. Comparison of proposed methods

Method	Prevent illegal authentication	Data security	Behavior analysis	Privacy protection
Meghna[18]	△	△	×	△
Chuyang[19]	△	○	×	×
Our Method	○	○	○	○

4.4 성능 측정

본 절에서는 성능 측정을 위해 단일 블록 생성에 소요되는 시간과 영상 비식별화를 포함한 블록생성 시간을 데이터 사이즈 단위로 비교하였다. 비식별화된 블록 생성을 위해서는 영상에 대한 비식별화를 먼저 수행하여야 하고, 이후 블록의 Merkle-Tree를 생성하여 블록체인상에 저장한다. 성능 측정 결과는 그림 6과 같다. 그림 6의 X축은 일반 블록 데이터 사이즈이며, Y축은 디스크 I/O 시간이다. 비식별화 방식, 성능 측정을 수행한 방식 및 성능 측정을 수행한 HW환경은 i7 4세대 CPU, 메모리 8G, 일반 HDD 1T용량의 환경이다. 그림 6의 결과 그래프는 왼쪽 Block Creation은 블록처리 시간을 의미하며, 오른쪽 Block Creation + De-identification은 블록처리 시간과 비식별화를 함께 처리한 시간을 의미한다. 측정 결과, 영상에 대한 비식별화를 수행함과 동시에 디스크 I/O 시간이 발생하여, 실질적으로 데이터 비식별화 수행 처리시간은 디스크 I/O 시간에 비례함을 알 수 있다.

그림 6의 결과를 통해, 데이터 사이즈가 증가할수록 처리시간이 지연되는 것을 확인할 수 있어 적절한 사이즈 이내의 데이터를 구성하는 것이 바람직하다. 또한 영상 비식별화 서버를 별도로 두는 경우 더욱 효율적인 학습 시스템을 구축할 수 있다.

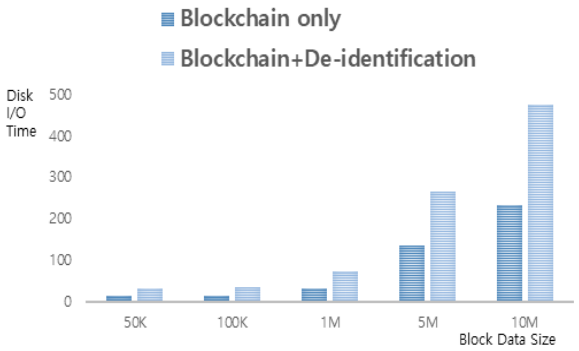

그림 6. 성능 측정
Fig. 6. Performance measurement

V. 결 론

포스트코로나 시대로 진입함에 따라, 언택트 교육 환경의 중요성은 더욱 커지고 있다. 현재 다양한 언택트 교육이 시도되고 있으나, 언택트 교육에 대한 보안 연구는 많이 진행되지 않고 있다. 그러나 온라인 환경에서 이루어지는 언택트 교육 시스템은 보안에 취약할 수 있으며, 다양한 사이버 공격이 발생할 수 있어 안전한 대책이 반드시 필요하다. 언택트 환경에서의 보안은 아무리 강조해도 지나치지 않으며, 학습 환경이 오프라인에서 온라인으로 전환

됨에 따라 반드시 고려해야 할 요소이다. 특히, 언택트 교육 환경에서는 기존의 온라인 학습 환경보다 더욱 많은 보안 위협 노출이 우려되는 상황이다. 온라인으로의 접근이 용이해짐에 따라 민감 학습데이터가 해커의 공격 또는 내부자의 정보 탈취 등 다양한 경로로 정보가 노출될 수 있다. 또한, 언택트 교육 환경은 학습자에 대한 프라이버시 노출이 발생할 수 있으며, 학습자 영상정보, 평가 및 학업 성취도 정보와 같은 다양한 정보가 노출될 수 있다.

본 논문에서는 블록체인을 이용한 안전한 언택트 교육 시스템을 제안하였다. 제안한 방법은 블록체인 내에 안면 마스킹 영상, 학습자의 행동 분석 데이터, 엑세스 로그, 테스트 및 평가 정보 등을 저장하고 있다. 블록체인은 그 자체로 강력한 무결성을 가지고 있으며, 학습데이터가 블록체인에 저장됨에 따라 해커의 인위적인 조작이 불가능하다.

제안한 방식의 장점으로, 빅데이터/인공지능 기반의 실시간 행동 분석을 통해 학습자의 감정상태 및 학습태도, 집중도를 파악하여 교수자에게 적절한 조치를 취하도록 유도할 수 있어 적시적 교육이 가능하다. 또한 학습자가 부적절한 행동을 취할 경우 교수자는 이에 대한 적절한 경고조치를 취할 수 있어 원활한 언택트 학습에 도움을 줄 수 있다. 오프라인과 온라인의 가장 큰 차이는 쌍방향 커뮤니케이션이며, 이러한 부분이 언택트 환경을 위한 온라인으로 전환되어도 원활하게 작동할 수 있어야 한다. 또한, 필요에 따라 정보기술의 장점을 활용하여 학습자 행동분석에 따른 적시적 교육, 블록체인을 이용한 민감 학습데이터 보안과 같은 측면에서는 오프라인의 교육환경에 비해 강점을 가질수도 있다.

코로나 사태의 진행에 따라, 언택트 교육 환경은 더욱 우리 생활에 점차 밀접해지게 될 것이다. 효과적인 교육환경 달성과 학습자의 프라이버시 보호를 위해 향후에도 언택트 교육 시스템에 대한 많은 연구가 시급히 진행되어야 할 것이다.

References

[1] Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, and Chul Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, Springer, pp. 1-15 Jun. 2018.

[2] C. J. Park and J. S. Hyun, "Factor Analysis of Visual Literacy Influencing Diagram Understanding and Drawing in Computer Science Education", Journal of Advanced Information Technology and Convergence, Vol. 9, No. 1, pp. 67-76, Jul. 2019.

[3] Jinsu Kim and Namje Park, "BlockChain Technology C3ore Principle Education of Elementary School Student Using Gamification", Journal of The Korean Association of Information Education, Vol. 23, No. 2, pp. 141-148. Apr. 2019.

[4] Donghyeok Lee and Namje Park, "CCTV Video Privacy Protection Scheme Based on Edge Blockchain", The Journal of Korean Institute of Information Technology, Vol. 17, No. 10, pp. 101-113, Oct. 2019.

[5] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", Electronics, Vol. 8, No. 7, 735, pp. 1-17, Jun. 2019.

[6] Kim Seung-Hee, "Risk Factors Identification and Priority Analysis of Bigdata Project", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 19, No. 2, pp. 25-40, Apr. 2019.

[7] Lee Yun-Min and Jin-Seob Shin, "Establishment of Monitoring System by Ubiquitous Computing", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 19, No. 1, pp. 127-132, Feb. 2019.

[8] Woo Yoseop, and Iksoo Kim. "Framework for Multimedia Service Using Multicast in CVCN Network", Journal of Advanced Information

Technology and Convergence, Vol. 9, No. 2, pp. 55-63, Dec. 2019.

[9] Donghyeok Lee and Namje Park, "Geocasting based synchronization of Almanac on the maritime cloud for distributed smart surveillance", Journal of Supercomputing, Vol. 73, No. 3, pp. 1113-1118, Aug. 2016.

[10] Donghyeok Lee and Namje Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance", Journal of the Korea Institute of Information Security & Cryptology, Vol. 28, No.2, pp. 417-428, Apr. 2018.

[11] Donghyeok Lee and Namje Park, "Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management", The Tansactions of The Korean Institute of Electrical Engineers, Vol. 6, No. 1, pp. 879-1888, Dec. 2017.

[12] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun 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, No. 6, pp. 1299-1308, Mar. 2018.

[13] Adil Jeghal, Lahcen Oughdir, and Hamid Tairi, "Politic of security, privacy and transparency in human learning systems", Education and Information Technologies, Vol. 21, No. 3, pp. 521-530, May 2016.

[14] 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. 891, Jun. 2020.

[15] Madeth May and Sébastien George, "Privacy Concerns in E-learning: Is UsingTracking System a Threat?", International Journal of Information and Education Technology, Vol. 1, No. 1, pp. 1-8, Apr. 2011.

[16] Defta Costinela Luminita, "Information security in E-learning Platforms", Procedia-Social and Behavioral Sciences, Vol. 15, pp. 2689-2693, Jan. 2011.

[17] Edgar R. Weippl and Martin Ebner, "Security Privacy Challenges in E-Learning 2.0", Association for the Advancement of Computing in Education (AACE), Nevada, USA, pp. 4001-4007, Nov. 2008.

[18] Meghna Bhatia and J. K. Maitra, "E-learning Platforms Security Issues and Vulnerability Analysis", 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES), Lucknow, India, pp. 276-285, Sep. 2018.

[19] Chuyang Li, et al., "A Blockchain System for E-Learning Assessment and Certification", 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, pp. 212-219, Aug. 2019.

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

[21] Donghyeok Lee and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 6, pp. 1593-1603, Dec. 2016.

[22] Namje Park and Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[23] Li Kuang, Yin Wang, Xiaosen Zheng, Lan Huang, and Yu Sheng, "Using location semantics to realize personalized road network location privacy protection", EURASIP Journal on Wireless Communications and Networking, 1, Jan. 2020.

[24] Jinsu Kim, Jaeyoung Cho, and Namje Park, "Block Chain Based CCTV Image Forgery · Modulation Verification Mechanism", The Journal of Korean Institute of Information Technology, Vol. 17, No. 8, pp. 107-114. Aug. 2019.

[25] Jinsu Kim and Namje Park, "Role Based Access Control based File Access Control Mechanism with Smart Contract", The Journal of Korean Institute of Information Technology, Vol. 17, No. 9, pp. 113-121. Sep. 2019.

[26] Zongda Wu, Ruiqin Wang, Qi Li, Xinze Lian, Guandong Xu, Enhong Chen, and Xiyang Liu, "A Location Privacy-Preserving System Based on Query Range Cover-Up or Location-Based Services", IEEE Transactions on Vehicular Technology, Vol. 69, No. 5, pp. 5244-5254, May 2020.

[27] Jinsu Kim and Namje Park, "Development of a board game-based gamification learning model for training on the principles of artificial intelligence learning in elementary courses", Journal of The Korean Association of Information Education, Vol. 23, No. 3, pp. 229-235. Jun. 2019.

[28] Jinsu Kim and Namje Park, "Dynamic/Static Object Segmentation and Visual Encryption Mechanism for Storage Space Management of Image Information", Journal of Korea Multimedia Society, Vol. 22, No. 10, pp. 1199-1207. Oct. 2019.

[29] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", Journal of Distributed Sensor Networks, Vol. 12, No. 1, Jan. 2016. https://doi.org/10.1155/2016/2965438

저자소개

이 동 혁 (Donghyeok Lee)

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2018년 2월 : 제주대학교 컴퓨터교육학과 공학박사
2007년 6월 ~ 2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월 ~ 2015년 6월 : KT 플랫폼개발단 과장
2018년 3월 ~ 현재 : 제주대학교 과학기술사회연구센터 학술연구교수
관심분야 : 블록체인, 지능형 영상보안, 5G보안, 데이터 비식별화, 컴퓨터교육, 디지털 트랜스포메이션 등

김 상 춘 (Sangchoon Kim)

1999년 8월 : 충북대학교 전자계산학과 박사
1983년 4월 ~ 2001년 3월 : 한국전자통신연구원 선임기술원
2001년 4월 ~ 현재 : 강원대학교 전자정보통신공학부 교수,
관심분야 : IoT보안, 융합보안 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 일반대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 교육부 창의교육거점센터장, 과학기술사회(STS)연구센터 부센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등