온라인 교육 서비스에서 부정 시청 방지를 위한 사용자 인증 시스템 제안

*김민지, *이세은, *이승신, *정명주, *백호기
*경북대학교 IT 대학 컴퓨터학부
kimminjy30@gmail.com, seorang0320@gmail.com, ggonggi0819@gmail.com,
cathy4025@gmail.com, neloyou@knu.ac.kr (Corresponding Author: 백호기)

A Proposal of User Authentication System to Prevent Fraudulent Viewing in Online Education Services

*Minji-Kim, *Seeun-Lee, *Seungsin-Yi, *Myeongju-Jung, *Hoki Baek
*School of Computer Science and Engineering, College of IT Engineering,
Kyungpook National University, Daegu, Korea

요 약

최근 온라인 교육 서비스 시장은 코로나 19 로 인해 수요가 급증하였다. 또한, 이동통신 기술의 발달로 그 규모가 확대되었고, 사용자는 시간과 장소에 구애 받지 않고 원하는 강의를 시청할 수 있게 되었다. 그러나 온라인 교육 환경에서는 아이디 공유를 통해 강의를 부정 시청하는 사례가 빈번하게 발생하고 있다. 특히나 하나의 계정을 다수의 사용자가 공유하거나 타인에게 양도함으로써 온라인 교육 서비스 업체가 손해를 입거나 사용자의 개인정보가 유출될 수 있다. 따라서 본 논문에서는 온라인 강의 플랫폼에서 본인 인증을 강화하고 강의 부정 시청을 방지할 수 있는 시스템을 제안한다.

1. 서론

2020 년 3 월에 세계보건기구(WHO)가 신종 코로나바이러스 감염증(이하 코로나 19)에 대해 세계적 대유행인 팬데믹을 선언한 후 우리는 강도 높은 사회적 거리두기를 실천하는 가운데 사회 전반에 걸쳐 비대면화를 경험하고 있다[1]. 특히, 교육 분야는 비대면 교육 프로그램을 제공하는 온라인 교육 시장의 급속한 성장세를 보이고 있다. 페이오니아(Payoneer)에 따르면 전문기술 분야 교육자 82%, 외국어 분야 교육자 55%가 '온라인 강의 수강생이 늘었다'고 답했다[2].

한편, 온라인 교육 시장의 급속한 성장세에 잇따라 다양한 문제점도 대두되고 있다. 가장 크게 부각되는 문제점은 수강생 간에 ID 를 공유하여 컨텐츠를 부정 시청하는 것이다. ID 공유를 통한 컨텐츠 부정 시청은 사용자의 개인정보 유출 및 해당 온라인 강의 제공 업체에 경제적 손실을 발생시킨다. 따라서 이와 같은 문제를 해결하기 위한 근본적인 대안이 필요하다.

본 논문에서는 이러한 문제를 해결하기 위해 UUID, 인증코드 등의 다중요소 인증 시스템을 제안한다. 제안 기법은 UUID 를 통하여 기기를 식별 및 등록하는 것이다. 기기 등록 시에는 인증 코드를 활용 및 최대 등록 기기 수에 제한을 둔다. 강의 시청 시에는 등록된 기기만 강의 수강이 가능하도록 함과 동시에 로그에 남은 UUID 정보를 통해 서로 다른 기기가 동시에 강의를 시청하는 것을 방지한다. 제안 기법을 통해 이용자의 무분별한 아이디 공유로 인한 개인 정보 유출 문제 및 강의 동시 수강을 방지할 수 있다.

2. 관련 연구

2.1. 인증기술

인증을 위해서는 판단의 근거가 되는 정보가 필요한데, 이를 인증요소라고 한다. 인증요소는 지식기반 인증요소(비밀번호, PIN), 소지기반 인증요소(OTP: One Time Password), 특성기반 인증요소(생체정보)로 분류될 수 있다. 기존에는 사용자 인증을 위해 비밀번호 기반 인증을 가장 많이 사용하였다. 이 방식은 구현하기 쉽고, 변경이 용이하여 널리 적용되고 있지만 공격자의 엿보기 공격, 추측 공격, 피싱 공격에 취약한 단점을 가지고 있다[3][4].

이를 보완하기 위해 다중요소 인증기술들이 연구되고 있다. 다중요소 인증기술은 각각의 단일요소 인증기술을 두 가지 이상의 인증요소를 결합하여 사용자를 인증하는 방법을 의미한다. 포털, 금융, 게임사이트 등의 국내 온라인 서비스에서 대표적으로 사용되는 다중요소 인증 기술로는 사용자의 지식기반 인증요소인 비밀번호와 소지기반 인증요소인 OTP 의 두 가지의 인증요소를 이용하는 것을 예로 들 수 있다. 다중요소 인증기술은 하나의 인증요소가 해킹에 의해 유출 또는 탈취되더라도 이와 독립적인 다른 인증요소에 의해 안전하게 사용자 인증을 제공할 수 있기 때문에 단일요소 인증에 비하여 보안성을 향상시킬 수 있다[5].

2.2. 범용고유식별자(UUID: Universal Unique Identifier)

네트워크상에서 서로 모르는 개체들을 식별하기 위해서는 각각 고유의 이름이 필요하다. 동시다발적이고 독립적으로 개발되고 있는 시스템들에게 고유성을 완벽하게 보장하기 위해서 탄생한 것이 범용고유식별자(UUID: Universal Unique Identifier)이며 국제기구에서 RFC4122 표준으로 정하고 있다. UUID 는 16 옥텟(octet)의 숫자이다. 표준형식에서 32 개의 십육진수로 표현되며 4 개의 하이픈을 포함하여 36 개 문자로 된 8-4-4-4-12 라는 5 개 그룹으로 구성되어 있다[6].

UUID 는 한번 할당하면 영구적으로 사용할 수 있는 식별자이다. 별도의 할당 및 관리 기관이 필요 없어서 등록 절차가 필요 없다. UUID 는 100 나노초 단위의 시간과 MAC 주소(Media Access Control Address)로 구성되기 때문에 UUID 를 생성과정에서 고유한 식별자 할당이 가능하다. UUID 표준에 따라 식별자를 할당하면 완벽하게 유일성을 보장할 수는 없지만 같은 MAC 주소를 사용하는 장비 2 개 이상이 같은 100 나노초에 UUID 를 할당할 가능성이 거의 없어서 사용상에서 중복될 가능성이 거의 없다고 인정되어 많이 사용되고 있다[7].

스마트폰 초기에는 제조사가 생산 과정에서 부여한 고유 식별 번호인 국제단말기식별번호(IMEI: International Mobile Equipment Identity)을 주로 사용하였으나, 이 고유번호는 휴대폰 사용자의 개인정보와 직결되기 때문에 개인정보보호 강화를 위해 해당 값의 이용을 강력히 제한하는 추세이다[8]. Google, Apple 등의 모바일 운영체제 사업자 또한 마케팅 영역(광고성과분석 포함)에서는 광고식별자를, 앱 서비스 및 사용자 분석에는 UUID 사용을 권고한다.

3. 제안 기법

3.1. 아이디 공유 방지

아이디 공유를 막기 위해서 UUID 를 통해 기기를 구별하여 등록한다. 한 아이디당 최대 2 대의 기기만 등록 가능하도록 기기 등록에 제한을 둔다. 이때 기기등록에서 비밀번호와 UUID 를 함께 사용한 다중인증 요소를 활용한다.

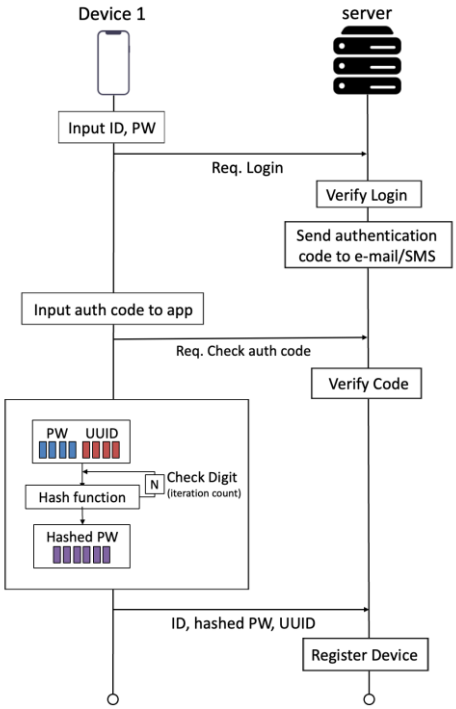

그림 1. 기기 등록 과정

세부 동작은 그림 1 과 같다.

① 사용자는 아이디와 비밀번호를 입력한다.

② 본인 인증을 위해 이메일 또는 SMS(Short Message Service) 인증을 수행한다.

③ 비밀번호는 UUID 를 SALT(데이터, 비밀번호, 통과암호를 해시 처리하는 단방향 함수의 추가 입력으로 사용되는 랜덤 데이터)로 이용하여 단방향 해시 처리한다. 이때 체크 디지트를 반복 횟수로 지정하며, 체크 디지트가 0 일 경우 10 으로 처리한다.

④ 아이디, 해시 처리된 비밀번호, UUID 를 인증 서버로 전송한다.

⑤ 인증서버에서 사용자 정보를 확인하여 기기가 등록되어 있지 않은 사용자이면, 데이터베이스 서버로 정보를 저장하여 등록을 마친다[9].

3.2. 동시 시청 방지

사용자가 기기에서 강의를 시청할 때마다 서버 상에 로그를 통해 시청 기록을 남긴다. 로그를 활용하여 동시 시청을 확인 할 수 있다. 만약 동시 시청을 시도할 경우, 시도한 기기에 동시 수강 경고 팝업을 띄운다. 이를 통해 한 기기에서만 강의를 시청할 수 있도록 한다.

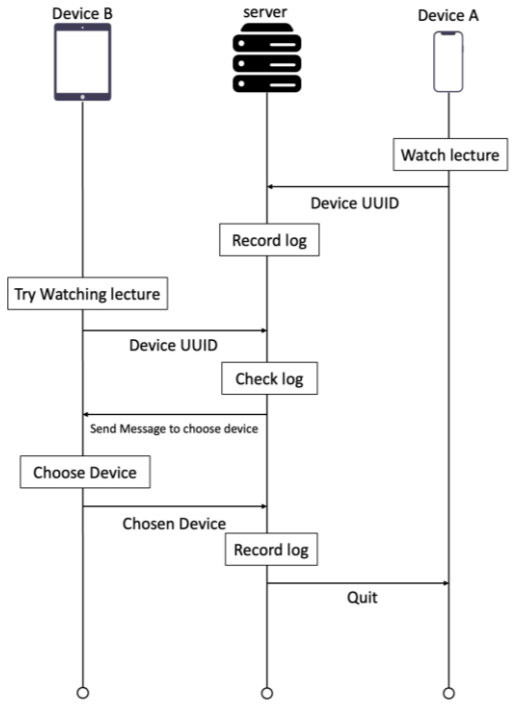

그림 2. 동시 시청 방지 과정

세부 동작은 그림 2 와 같다.

① 사용자가 기기 A 에서 강의를 시청한다.

② 서버로 기기 A 의 UUID 를 보내 기기 A 의 강의 시청 로그를 기록한다.

③ 사용자가 기기 B 에서 강의 시청을 시도한다.

④ 사용자의 강의 시청 로그를 통해 현재 강의 시청 여부를 확인한다.

⑤ 이미 기기 A 에서 강의 시청중이므로, 기기 B 에 강의를 시청할 기기의 변경 여부를 묻는 팝업을 띄운다.

4. 제안 기법의 효과성 및 결론

본 논문에서는 아이디 공유를 이용한 온라인 강의 부정 시청 방지를 위해 UUID 정보 활용과 기기 등록 시 다중 인증을 통한 온라인 강의 인증 시스템을 제안하였다. 기기 등록 시 인증 코드를 통한 다중 인증 방식을 적용하여 사용자가 무분별하게 기기를 등록하는 것을 방지하였고, 강의를 수강하고 있는 기기의 UUID 를 서버에 전송함으로서 여러 기기에서 동시에 강의를 수강하는 것을 방지할 수 있었다. 결과적으로 본 시스템을 통해 여러 사용자가 한 아이디를 통하여 동시에 강의를 수강하는 부정 시청 문제를 해결하고, 사용자 개인정보 유출 문제를 방지할 수 있을 것으로 기대된다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW 중심대학사업의 연구결과로 수행되었음(2021-0-01082)

참고문헌

[1] 송수연, 김한경 , “언택트 시대의 대학교육: 코로노 19 에 따른 비대면 강의 만족도와 수강지속의사에 영향을 미치는 요인에 관한 연구” , 아시아교육연구, 21(4), 1100

[2] 이효상, “코로나 19 이후, 전세계 온라인 교육 수요 큰 폭 증가”, 아웃소싱타임즈, 2020

[3] 이재흥, “모바일 기기 기반의 사용자 인증 기술 동향”. 정보과학회지, 35(2), 28-33, 2017

[4][5] 김근옥, 정영곤, 심희원, 강우진. “모바일 기기 기반의 다중요소 인증기술 국제 표준화 동향”. 정보보호학회지, 24(4), 26-32, 2014

[6] 강희복, 장행천, 장창수, “IUWT 기반 토큰 인증 기술. 한국정보기술학회논문지”, 17(2), 143-150, 2019

[7] 김성혜, 안윤영, “전기설비 안전관리를 위한 식별체계 표준기술 동향”. 전기의세계, 69(12), 29-35, 2020

[8] 김영식, “IMEI 와 일련번호란…개인정보와 연결되는 '고유번호'”, 아시아경제, 2013

[9] 정필성, 조양현, “모바일 환경에서 상호 협력 기반 스마트폰 사용자 인증 알고리즘”. 한국정보통신학회논문지, 21(7), 1393-1400, 2017