JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 4: 462~469, Apr. 2019

블록체인을 이용한 CCTV 협력 검증 모델

권용빈[1] · 안규황[1] · 권혁동[1] · 서화정[2*]

CCTV Cooperation Authentication Model Using Block Chain

Yong-Been Kwon[1] · Kyu-Hwang An[1] · Hyeok-Dong Kwon[1] · Hwa-Jeong Seo[2*]

[1]Graduate Student, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea
[2*]Assistant professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

요 약

2018년 행정안전부의 통계 조사에 따르면 대한민국의 공공, 민간 CCTV의 대수는 1000만대에 이르며 증가 추세 또한 줄지 않고 있다. 또한 영상판독기술의 발달로 지능형 CCTV를 이용하여 많은 정보를 얻을 수 있다. 최근 CCTV를 활용한 다양한 서비스들이 제공되고 있다. 그러므로 CCTV 영상 데이터의 무결성을 보장하는 것은 매우 중요하다. 하지만 영상에서 일어나는 일을 검증할 수 있는 시스템은 아직까지 존재하지 않는다. 본 논문에서는 수많은 CCTV를 관리하고 활용하며 검증할 수 있는 시스템 모델을 제안한다. 제안하는 모델은 CCTV의 영상을 주변의 CCTV 데이터로 인증한다. 이 모델은 블록체인을 이용하여 영상의 무결성을 보장한다. 또한 큰 영상 데이터가 아닌 훨씬 작은 분석된 데이터들을 사용함으로써 CCTV의 프라이버시 문제와 블록체인의 데이터 크기 문제를 해결한다.

ABSTRACT

According to the survey of Ministry of the Interior and Safety in Korea, The number of public and private CCTV reached over ten million and is still increasing. Also with improving Image Processing Technology, it is possible to obtain diverse information. Recently, various services using CCTV are being provided. Therefore it is necessary to ensure CCTV image integrity. However there is no system to prove events in film yet. In this paper, we suggest system model that can manage, use and authenticate CCTV. This model allows a CCTV film to be verified by other nearby CCTVs' data. This model ensures film's integrity by using blockchain. And also, It addresses privacy problem in CCTV and file size problem in blockchain by using not large film data but much smaller analyzed data.

키워드 : CCTV, 블록체인, 영상 검증, 영상 분석

Keywords : Blockchain, CCTV, Image analysis, Image authentication

Received 26 January 2019, **Revised** 6 February 2019, **Accepted** 10 February 2019

***Corresponding Author** Hwajeong Seo(E-mail:hwajeong84@gmail.com, Tel:+82-2-760-8033)
Assistant professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.4.462 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

CCTV의 수는 이미 공공부분 100만대, 민간부분 900만대 총 1000만대에 이르며 매년 10%의 증가율이 지속되고 있다[1]. 또한 영상분석 기술의 발달로 인공지능형 CCTV에 대한 연구도 활발히 진행 중이다. 하지만 현재 설치된 CCTV중 무시할 수 없는 숫자가 낮은 해상도를 가지고 있다. 또한, 영상분석 기술이 발달한다 하더라도 센서의 한계 등으로 인해 오작동하는 경우가 많이 존재한다. 악의적인 용도로 영상을 조작하는 경우 또한 발생할 수 있다. 이외에도 다양한 이유들이 CCTV에 찍힌 영상 데이터의 무결성을 위협하고 있다. 반면 CCTV를 이용한 서비스들은 강화되고 다양화되고 있다. 따라서 이러한 서비스들을 올바르게 제공하기 위해 영상의 무결성은 반드시 지켜져야 한다. 개인 정보 보호법에서는 공개된 장소의 공공의 목적을 위한 CCTV설치를 허용하는데 이를 위해서는 CCTV의 소유자와 연락하여 영상정보를 획득해야 한다. 하지만 이러한 과정에서 많은 시간이 소요되며 영상을 획득했다 하더라도 그 영상이 필요한 영상이라는 점과 조작되지 않았다는 점이 보장되지 않으므로 공공기관에서의 활용에도 어려움이 있다. 본 논문에서는 영상 데이터의 조작에 의한 무결성 침해뿐만 아니라 해상도나 알고리즘의 문제로 발생할 수 있는 영상 판독 데이터의 무결성 침해까지도 방지할 수 있는 검증 시스템을 최초로 제안한다. 영상 정보를 검증하는 방법으로서 분산원장 기술의 블록체인을 활용하며 개발을 위해 이더리움(Ethereum)의 솔리디티(Solidity) 언어를 이용한 스마트 컨트랙트(Smart Contract)기능을 활용하였다. 또한 제안하는 모델에서는 블록체인을 이용함으로써 발생하는 프라이버시 문제와 데이터의 크기 문제를 해결하기 위해 영상 분석 정보를 이용한다. 2장에서는 CCTV의 목적과 영상 검증의 필요성을 설명한다. 3장에서는 블록체인 기반의 이더리움을 설명하고 이를 활용하는 서비스를 소개한다. 4장에서는 제안하는 모델을 설명하고 5장에서 결론을 내린다.

Ⅱ. CCTV

본 장에서는 CCTV의 목적과 발전 추세를 기존의 연구를 바탕으로 살펴보고[2] CCTV 인증 시스템의 필요성에 대하여 설명한다.

2.1. CCTV의 목적

CCTV란 특정 수신자에게만 영상을 전달하는 목적으로 설계되었다. 최근에는 그 개념이 확장되어 자동차에 설치하는 블랙박스 등도 CCTV로 분류한다. CCTV의 기본적인 목적은 범죄예방이다. 이외에도 질서유지를 목적으로 공공 또는 민간에서 이용하기도 하고 증거물로서의 역할도 한다. 마지막으로 항상 감시되고 있다는 사실은 안전하다고 인식될 수 있다. CCTV의 목적은 표 1과 같이 정리할 수 있다.

Table. 1 Function of CCTV

Function
Crime Prevention
Preserve order
Evidence
Safety Awareness

실제로 CCTV의 범죄억제, 질서유지에 대한 효과는 많은 연구와 통계를 통해 입증되었으며, 현재 실제로 증거물로서도 이용되고 있다. 사람들의 CCTV에 대한 우호도 또한 사생활 침해에 대한 우려를 뛰어넘기 때문에 CCTV가 설치된 지역에서 불편함 보다는 안전감을 더 느낀다. 물론 프라이버시에 대한 인식 또한 변화하고 있지만 올바른 절차로 영상이 활용된다는 전제하에 앞으로도 CCTV는 활용될 것이다.

2.2. CCTV의 발전 추세

CCTV의 목적을 더욱 잘 달성하기 위해 필요한 것은 즉각적인 대응이다. 표1의 목적에 대하여 즉각적인 대응을 대입한다면 다음과 같은 효과를 기대할 수 있다. 먼저 즉각적인 대응이 일어난다면 범죄자는 범죄를 일으킬 때 더욱 큰 부담을 느끼게 된다. 이는 질서를 어지럽히는 행위를 하는 사람에게도 마찬가지로 적용된다. 또한, 범죄자를 현장에서 잡을 수 있게 되며 마지막으로 더욱 더 안전함을 느낄 수 있게 된다. 이러한 즉각적인 대응의 중요성은 CCTV 시스템의 시간에 따른 발전 단계를 보면 더욱 잘 드러난다.

2.2.1. 모니터 요원

기존의 CCTV는 영상을 저장한 뒤 사건이 발생했을 시 돌려보는 형식으로 이용되었다. 하지만, 즉각적인 대응을 위해 실시간으로 감시하는 모니터 요원을 사용하게 되었고 현재도 많이 사용하고 있다.

2.2.2. 통합 관제 시스템

통합 관제 시스템은 CCTV 간의 협력 시스템이다. 기존에 개별적으로 존재했던 영상 데이터를 실시간으로 동시에 다루게 되면서 더 효과적으로 CCTV의 목적을 달성할 수 있다.

2.2.3. 지능형 CCTV

지능형 CCTV란 이벤트를 스스로 감지하며 영상을 분석하여 판단을 내리는 차세대 CCTV를 의미한다. 이러한 차세대 CCTV는 현재 주거지 침입알림이나 차량에 충돌이 발생했을 시 즉각 알림 등 개인을 위한 서비스와 사건 발생을 판단하여 경찰을 출동시키는 등의 공공 서비스를 제공하는데 적극적으로 활용되고 있다.

2.3. CCTV 인증 시스템의 필요성

CCTV의 주요한 목적들을 효율적으로 달성하기 위해 즉각적인 반응이 중요하지만 이를 사람이 달성하는 것에는 한계가 있다. 따라서 앞으로 지능형 CCTV를 활용한 자동화 관제 시스템이 더욱 발전할 것으로 여겨진다. 하지만 이러한 시스템은 보안적인 관점에서 영상의 무결성에 대한 취약점이 존재한다. 자동화된 관제 시스템의 모든 판단은 영상 데이터에 의존하기 때문에 노후한 CCTV, 환경에 따른 오작동, 악의적인 사용자의 조작 등은 이러한 시스템의 효율을 망가뜨릴 수 있다. 따라서 영상 정보에 대한 검증을 통해 무결성을 확보하는 것이 필요하다.

Ⅲ. 블록체인

블록체인이란 한 곳에서 모든 데이터를 관리할 때 생기는 문제점들을 해결할 수 있는 분산 데이터베이스 시스템이다. 모든 데이터들은 블록화 되며 블록들은 서로를 체인 형태로 연결하게 된다. 블록들은 이전 블록의 모든 데이터를 입력으로 하는 해시 값을 갖는다. 따라서 조금이라도 데이터가 변경된다면 해시 함수의 특성에 의해 모든 블록이 타당하지 않게 된다. 블록의 구조는 그림 1과 같다.

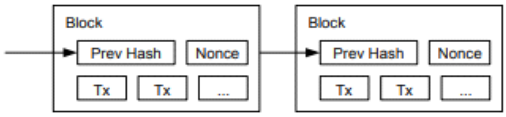


Fig. 1 Structure of Block

이러한 블록들로 구성된 체인은 모든 노드들에 동일하게 복사되며 조작될 수 없다. 이를 통해 블록체인은 데이터에 대한 무결성을 보장한다. 본 장에서는 블록체인기반 플랫폼 이더리움을 설명하고 이더리움을 이용한 서비스를 통해 이해를 돕는다. 마지막으로 다른 블록체인 네트워크에 대해 설명한다.

3.1. 이더리움(Ethereum)

이더리움은 금융과 관련된 트랜잭션을 처리하도록 만들어진 비트코인(Bitcoin)과 다르게, 일반적인 데이터 또한 용이하게 다를 수 있게 설계된 블록체인 시스템이다. 특정 조건에 도달했을 시 코드가 실행되도록 하는 스마트 컨트랙트의 개념을 포함하며, 이 개념을 이용하여 다양한 응용프로그램을 개발할 수 있다. 스마트 컨트랙트는 그림 2과 같은 형태로 동작한다.

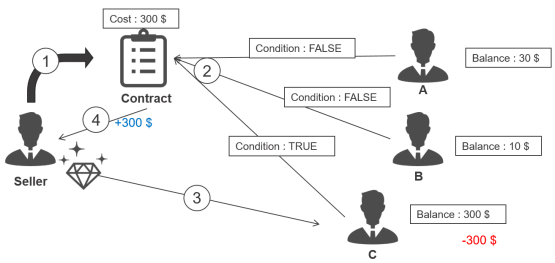


Fig. 2 Flow of Smart Contract

3.2. 이더리움 어플리케이션(투표 시스템)

기존의 온라인 투표 서비스는 중앙에 서버가 존재하고 참가자들이 투표를 한다. 이 경우 중앙의 서버만 해킹한다면 투표 결과를 조작하는 것이 가능하며 투표자는 올바른 투표가 일어났는지 알 수 없다. 따라서 이더리움을 활용한 투표 시스템이 제안되었다[3]. 제안된 투표 시스템은 컨트랙트를 통해 투표 자격을 부여받고 투

표 결과를 분산 저장함으로써 투표 결과에 대한 무결성을 보장한다. 또한, 모든 기록은 이더리움 네트워크에 저장되어있기 때문에 누구든 열람이 가능하다. 따라서 참여한 노드들은 투표 결과를 신뢰할 수 있게 된다.

Ⅳ. CCTV 협력 검증 모델

본 장에서는 블록체인을 이용한 CCTV 협력 검증 모델을 제안한다.

4.1. CCTV 협력 검증 모델

기존의 통합 관제 시스템에서 각 CCTV들이 공통으로 관측하는 범위가 존재한다. 이 범위를 활용하여 CCTV 간 인증에 사용하며 이를 도식화하면 그림 3과 같다.

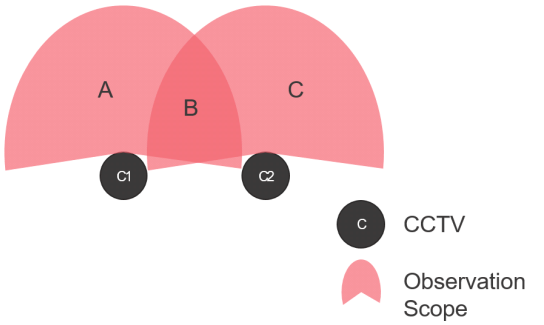


Fig. 3 CCTV observation scope

먼저 첫 번째 CCTV를 통해 B 지역에 대상이 있을 경우 두 번째 CCTV를 통해 B 지역의 대상을 확인할 경우 B에 대상이 존재한다는 사실이 두 CCTV에 의해 검증된다. 다음으로 첫 번째 CCTV에서 대상이 A에서 B를 거쳐 C로 이동했다면 두 번째 CCTV에서 협력하여 대상을 추적하는 것이 가능해진다. 이러한 시스템은 현재 모니터 요원에 의해 이용하고 있는 시스템이다. 이를 위해 충분한 수의 CCTV를 확보하고 통합 관제 시스템을 구축하는 것은 상당한 비용이 소요된다. 따라서 최대한 효율적으로 CCTV를 설치하게 되며 범위를 넘어가는 부분에 대해서는 증명할 수 없거나 다른 관제 시스템을 갖는 CCTV와의 협력이 필요하게 된다. 예를 들어 현재 공공 부분의 CCTV 통합 관제 시스템은 관측 범위를 넘어가는 부분에 대하여 다른 민간 CCTV의 도움을 요청한다. 이 과정에서 많은 시간이 소요되기 때문에 즉각적인 대응이 일어날 수 없으며 CCTV의 목적을 효율적으로 달성할 수 없다. 실제로 민간 CCTV까지 통합 관제 시스템에 포함된다면 공통으로 관측하는 범위가 늘어나기 때문에 상당 부분을 검증할 수 있게 된다. 그림 4은 민간 CCTV가 포함되었을 때의 관측 범위이다.

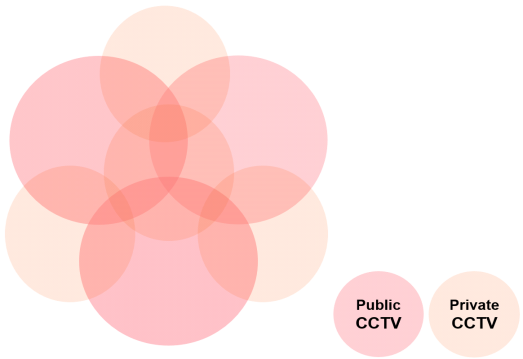


Fig. 4 CCTV observation scope with private CCTVs

이렇게 민간 CCTV와 공공 CCTV를 협력하여 이용할 수 있다면 대부분의 영역을 검증할 수 있게 되며, 이는 CCTV가 늘어날수록 검증 가능 영역은 더욱 늘어나게 된다. 이 협력을 위해 블록체인을 이용한다. CCTV의 소유자들은 노드로서 블록체인 네트워크에 참여하게 된다. 이를 도식화하면 그림 5와 같다.

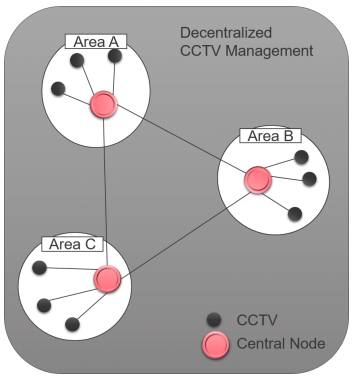


Fig. 5 Decentralized control system

CN(Central Node)은 CCTV의 소유자로 네트워크에 참여하는 노드이다. 자신의 CCTV를 네트워크에 등록하며 구체적으로 CCTV의 위치, 관측 범위 등을 등록할

수 있다. 이렇게 함으로써 서로 다른 시스템에 속한 CCTV들이 협력하여 서로의 영상을 검증할 수 있게 된다. 하지만, 블록체인의 특징 중 하나인 모든 데이터가 모든 노드에 복사되는 점 때문에 두 가지 문제점이 발생한다. 첫 번째 문제점은 용량이다. 영상 데이터는 저장과 보관에 상당한 비용을 요구하며 이는 블록체인 네트워크 환경에 적합하지 않다. 두 번째 문제점은 데이터가 영구적으로 저장된다는 점이다. 영상 데이터가 직접 저장된다면 영상에 찍힌 개개인의 프라이버시가 침해될 수 있으며, 삭제가 불가능한 블록체인의 특징은 개인 정보 보호법의 개인 정보 자기 결정권을 위배하게 된다. 이 두 가지 문제점을 해결하기 위해서 영상 데이터를 저장하는 것이 아닌 영상 분석 기술을 통해 분석된 영상 분석 정보를 저장하게 된다. 이를 통해 블록체인에 저장되는 데이터의 크기를 크게 줄임과 동시에 개인의 프라이버시 문제를 해결할 수 있다. 구체적으로, 영상 분석 정보는 영상을 분석한 텍스트 정보이기 때문에 영상 데이터와 비교하여 큰 용량 감소 효과를 지닌다. 또한 현재 개인 정보 보호법에서는 정보를 수집하는 기관이 개인의 명확한 동의를 얻도록 하고 있다. 하지만 CCTV분야에서는 개인의 명확한 동의를 촬영 시간, 활용 목적 등이 명시된 안내판으로 대체하고 있다. 이는 암묵적인 동의를 요구하는 것이며 이를 인지하지 못하는 아이들과 같은 경우 얼굴이 그대로 저장되게 된다. 뿐만 아니라 촬영을 인지한다 하더라도 이를 피해 다니는 것은 전국의 CCTV의 수와 그 촬영범위를 고려했을 때 불가능하며 가능하더라도 개인이 이동할 수 있는 곳을 매우 제한할 것이다. 이에 개인식별정보에 해당하는 얼굴대신 영상분석정보를 저장하는 방법은 프라이버시를 최대한 보장하면서도 서비스를 제공하는 데에 큰 도움이 될 것이다. 저장되는 정보의 형태는 그림 6과 같다.

Core Information

	Car A	Person A	Fight	Dumping	Crash
CCTV A	Y	N	N	N	Y

Fig. 6 Sample Form of Analyzed Data

CCTV A는 영상 분석을 통해 이벤트를 감지하고 결과를 반환한다. 분석 알고리즘이 탑재된 지능형 CCTV의 경우 자동으로 특정 시점 특정 지점의 영상을 분석하고 자동차 A 존재, 사람 A가 존재하지 않음, 싸움 일어나지 않음, 쓰레기 투기 일어나지 않음, 충돌 사고 일어남이라는 정보를 컨트랙트를 통해 네트워크에 업로드한다. 이 때, 이더리움 컨트랙트는 수집하는 정보 형태를 명시하고 있으며 이에 맞추어 정보를 갱신하게 되고 틀린 정보의 갱신이 일어날 경우 다수의 CCTV가 판단한 정보를 따르게 된다. 영상분석알고리즘이 탑재되지 않은 경우라도 스마트컨트랙트의 수집 정보 형태에 맞는 입력을 한다면 본 모델을 적용 가능하다. 모델의 신뢰성은 비신뢰관계에 있는 다수 노드에 의해 결정이 되므로 정보 입력의 주체가 사람이거나 도구여도 적용은 가능하다. 다만 이에 대한 부가적인 취약점이 발생할 수 있어 보완할 수 있는 장치가 필요할 것이다. 이와 같이 기밀 데이터의 누수를 구조적으로 방지하기 위한 연구가 존재한다[4]. 본 논문에서는 저용량의 분석 결과만을 저장함으로써 용량 문제가 해결되고 이렇게 분석된 핵심 정보만을 이용하여 서로를 검증하게 되어 영상에 찍힌 개개인의 프라이버시 문제를 보장할 수 있게 되며 개개인을 직접 식별하는 것이 어려움으로 개인 정보 자기 결정권을 위배하지 않는다. 그림 7은 한 지역 B를 관측하는 세 CCTV가 영상 분석 결과로 생성한 핵심 정보이다.

Area B

	Car B	Person B	Fight	Dumping	Crash
CCTV E	N	Y	N	Y	N
CCTV F	N	Y	N	Y	N
CCTV G	N	Y	N	N	N

Fig. 7 Authentication Example

CCTV E, F는 완전하게 같은 영상 분석 정보를 결과로서 제출하였다. 반면 G에서는 어떠한 이유에서 다르게 분석 정보를 결과로 제출하였다. 이 결과로 사용자는 G가 오작동을 일으킨 것을 바로 판단할 수 있다. 이러한 판단은 CCTV의 개수가 늘어날수록 더 정확할 것이다. 만약 쓰레기 투기에 관한 실제 영상 데이터가 필요하다면 G가 아닌 E, F에게 영상 협조를 구함으로써 시간을 절약할 수 있을 것이다.

4.2. CCTV 협력 검증 모델 구현

본 모델의 샘플 구현을 이더리움 네트워크에 구현하였다. 개인의 프라이버시를 지켜주는 등의 부가적인 기능을 원한다면 다른 블록체인 플랫폼에 구현하는 것도 가능하다. 또한 컨트랙트를 사용하는 환경이 전문적일

수 있으므로 이를 웹에서 구현하여 연동하였다. CCTV 소유자에 대한 설계는 그림8과 같다.

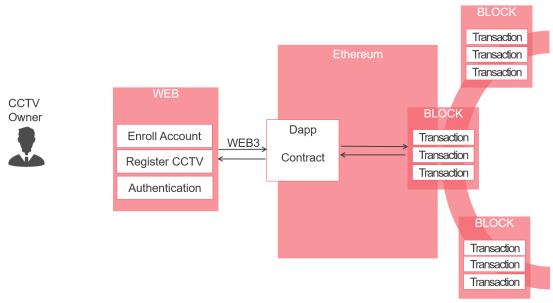


Fig. 8 Design Part for CCTV Owner

CCTV를 소유한 노드는 자신의 계정을 통해 CCTV를 등록할 수 있고 자신의 CCTV에서 나온 데이터의 인증을 요청할 수 있다. 이 과정은 웹에서 진행되며 WEB3를 통해 컨트랙트를 실행시키고 이더리움 네트워크에 영구히 저장되게 된다. 영상 데이터 사용자에 대한 설계는 그림9와 같다.

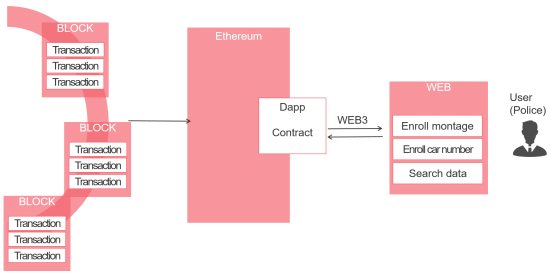


Fig. 9 Design Part for CCTV user

사용자의 경우 트랜잭션을 검색하여 자신이 필요로 하는 정보가 검증된 정보인지 알 수 있다. 또한 몽타주나 차량정보를 넣어서 해당 정보가 포함된 영상 데이터를 찾는 것도 가능할 것이다. 실제 샘플 구현은 그림8까지만 진행하였다. 그림 10은 구현된 요소들이다.

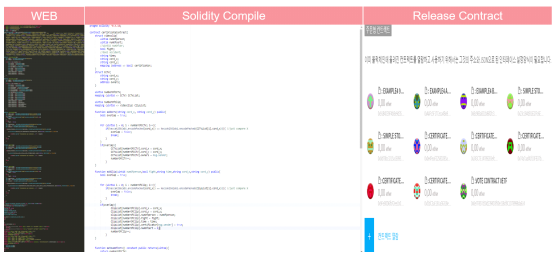


Fig. 10 Components of Implementation

먼저 솔리디티 언어를 이용하여 스마트 컨트랙트를 작성한다. 다음으로 작성한 컨트랙트를 이더리움 네트워크에 배포한다. 이 단계에서도 배포한 컨트랙트를 이용하여 데이터를 읽고 쓰는 것이 가능하지만 사용자의 편의를 위해 웹으로 구현한 뒤 web3 API를 통해 이더리움 네트워크와 연동하였다. [5,6]그림 11은 결과 화면이다.

Fig. 11 Result of Implementation

최초 등록된 노드와 다른 이더리움 계정으로 똑같은 영상 분석 정보를 입력한다면 이더리움 네트워크의 인증 노드 수에 해당하는 값이 증가하는 것을 볼 수 있다. 코드는[7], 시연 동영상은 [8]에서 확인할 수 있다.

4.3. 기타 블록체인 네트워크

본 모델의 구현은 이더리움 네트워크를 사용하였다. 이는 현재 많은 참여자들이 존재하기 때문에 네트워크가 안정화 되어있다는 점과 스마트 컨트랙트 등 구현관점에서의 용이함 때문이다. 하지만 이외에도 서로 다른 기술을 토대로 한 블록체인 네트워크들이 존재하며 연구되고 있다[9]. 이들은 크게 퍼블릭 블록체인과 프라이빗 블록체인 그리고 이를 섞은 하이브리드 블록체인으로 분류할 수 있다. 퍼블릭 블록체인은 이더리움과 같이 모든 참가자들이 참여할 수 있는 네트워크를 말한다. 이 경우 네트워크가 이미 활성화되어 안정적이라는 장점을 갖지만 모든 정보들이 모든 노드에 복사 저장된다는 특징 때문에 본 모델에 적용 시 특정 지역에 대한 장기적인 정보를 누구나 취득할 수 있다는 단점이 존재한다. 프라이빗 블록체인의 경우 특정 노드들을 중심으로 데이터를 취합 저장하여 공공기관만이 이용할 수 있게 하는 등 퍼블릭 블록체인에서 발생하는 문제를 일부 해결할 수 있으나 탈중앙화라는 성질을 잃기 때문에 참여 기관의 안전성에 대한 담보와 해킹에 대한 보안이 중요해진다. 하이브리드 블록체인의 경우 공개되는 데이터와 아닌 데이터를 분리해서 공개하는데 이러한 블록체인 형태를 이용할 경우 사용자의 개인 정보를 보호하면서도 공공기관에서는 데이터를 이용할 수 있는 본 모델에

적합한 블록체인 서비스를 개발하고 활용할 수 있을 것으로 기대된다.

Ⅴ. 결론과 연구 방향

제안된 모델은 다른 시스템에 속해 있는, 서로 신뢰할 수 없는 노드 간의 신뢰를 만드는 구조이다. 한 노드는 한 번의 인증이 가능하며 영상을 분석한 결과가 동일해야만 입증이 가능하므로 해당 정보가 정확한지 아닌지 구별 가능하다. 또한 정확한 정보만을 검색하여 협조를 요청함으로써 비용을 절약할 수 있으며 인증된 데이터를 공공기관 또는 수사기관이 활용할 경우 보상을 제공하는 등의 방면으로 사용될 수 있다. 용량이 큰 영상 데이터를 사용하지 않으므로 블록체인 네트워크에 적합하다. 이더리움 네트워크의 경우 이미 배포한 컨트랙트에 대하여 수정이 불가능하다. 따라서 보완사항이 발생했을 시 모든 노드들이 다시 참여해야한다는 단점이 존재한다. 또한, 그 지역에 해당하는 정보들은 모든 사람에 의해서 열람 가능하며 이는 모든 노드에 데이터베이스가 복사되어있음을 의미하며 따라서 최소정보수집의 원칙을 벗어나기에 프라이버시 침해의 우려가 있다. 그러므로 이러한 이더리움의 단점을 보완하는 블록체인 플랫폼을 활용한다면 더 완성도 높은 인증 시스템의 구현이 가능할 것이다. 또한 CCTV 협력 검증 모델의 경우 분석 결과를 이용하기 때문에 특징을 추출하여 영상을 분석하는 지능형 CCTV에 적합한데 기존의 CCTV가 찍은 영상의 경우에도 이를 대신 분석해주는 영상 분석 서비스를 이용하거나 사람이 직접 분석하는 방법을 적용할 수 있다. 하지만 이를 적용할 시 분석 서비스를 해킹하거나 한 사람이 다수의 CCTV를 등록하는 방식으로 다수를 선점하여 무결성을 해칠 수 있다. 따라서 이러한 취약점과 그 해결책에 대한 연구가 필요할 것이다.

ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017 R1C1B5075742) and was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). This research of Hwajeong Seo was financially supported by Hansung University.

REFERENCES

[1] Ministry of the Interior and Safety. Research on the personal information protection total support system[internet]. Available: http://www.index.go.kr/potal/main/EachDtlPage Detail.do?idx_cd=2855.

[2] S. K. Jung, “Legal Limit and Improvement Plan of CCTV Installation and Operation,” *Inha Law Research Institute*, vol. 21, no. 2, pp. 35-63, Jun. 2018.

[3] C. J. Kim, “An Online Voting System based on Ethereum Block-Chain for Enhancing Reliability,” *Journal of the Korea Academia-Industrial*, vol. 19, no. 4, pp. 563-570, Apr. 2018.

[4] V. Bhavana, “Data Security in Cloud environments,” *Asia-pacific Journal of Convergent Research Interchange*, vol. 1, no. 4, pp. 25-31, Dec. 2015.

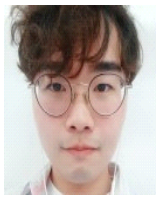
[5] web3 API, web3 Document[Internet]. Available: https://web3js.readthedocs.io/en/1.0/.

[6] Go-Ethereum. Ethereum Installation[Internet]. Available: https://ethereum.github.io/go-ethereum/downloads/.

[7] Github. CCTV implementation code[Internet]. Available: https://github.com/DragonBeen/CCTV.

[8] Youtube. Demonstration CCTV cooperation authentication model using Ethereum platform[Internet]. Available: https://youtube/2r-NmbG-p6U.

[9] J. S. Kim, “A Survey of Cryptocurrencies based on Blockchain,” *Journal of The Korea Society of Computer and Information,* vol. 24, no. 2, pp. 64-74, Feb. 2019.



권용빈(Yong-Been Kwon)

2018년 8월: 한성대학교 IT응용시스템공학과 공학학사
2018년 9월~현재: 한성대학교 IT응용시스템공학과 석사과정
※관심분야 : TEE, 부채널분석, 사이버 보안

안규황(Kyu-Hwang An)

2018년 2월: 한성대학교 IT응용시스템공학과 공학학사
2018년 3월~현재: 한성대학교 IT응용시스템공학과 석사과정
※관심분야 : 블록체인, 블록암호, IoT 보안

권혁동(Hyeok-Dong Kwon)

2018년 2월: 한성대학교 IT응용시스템공학과 공학학사
2018년 3월~현재: 한성대학교 IT응용시스템공학과 석사과정
※관심분야 : 암호구현, 블록체인

서화정(Hwa-Jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT