블록체인 기술을 이용한 스마트시티 데이터 보안 모델 연구

[1*]조도은

A Study on Smart City Data Security Model Using Blockchain Technology

[1*] Do-Eun Cho

요 약

스마트 시티는 정보통신기술의 혁신과 도시 생활의 질 향상을 추구하는 현대 도시 계획의 산물이다. 스마트 시티의 효율적인 운영을 위해서는 실시간 수집되고 저장 및 처리되는 데이터가 핵심자원이다. 따라서 다양한 분야에서 수집되는 스마트 시티의 데이터는 안전하게 관리되어야 하며, 개인정보보호가 무엇보다 중요하다. 본 연구에서는 스마트 시티의 데이터를 안전하게 관리하기 위하여 블록체인 기술을 이용한 스마트 시티 데이터 보안 모델을 제안하였다. 제안 모델은 블록체인 네트워크에 IPFS를 통합하여 데이터를 분산 저장함으로써 데이터의 기밀성과 무결성을 확보하고, CP-ABE를 이용하여 데이터를 암호화하여 사용자로부터 데이터의 접근제어가 효율적으로 수행되도록 하였다. 또한 데이터 접근 제어 정책과 동형 암호를 사용함으로써 데이터의 활용성을 강화하면서 프라이버시를 보장하도록 하였다.

Abstract

Smart cities are the product of modern urban planning that seeks to innovate information and communication technology and improve the quality of urban life. For the efficient operation of smart cities, data collected, stored, and processed in real time is a key resource. Therefore, data from smart cities collected in various fields must be managed safely, and personal information protection is paramount. In this study, a smart city data security model using blockchain technology was proposed to safely manage smart city data. The proposed model integrates IPFS into the blockchain network to distribute and store data to ensure data confidentiality and integrity, and encrypts data using CP-ABE to efficiently control access to data from users. In addition, privacy was guaranteed while enhancing the usability of data by using Homomorphic Encryption with data access control policies.

Keywords: *Blockchain, CP-ABE, Inter-Planetary File System (IPFS), Access Control, Smart City*

[1*] 교신저자 *목원대학교 SW 교양학부(decho@mokwon.ac.kr)*

Received: Mar. 30, 2024, Revised: Apr. 18, 2024, Accepted: Apr. 19, 2024

I. 서론

스마트 시티는 정보통신기술의 혁신과 도시 생활의 질 향상을 추구하는 현대 도시계획의 산물이다. 이 개념은 도시 인프라와 서비스의 효율성을 증대하고 에너지 소비를 줄이며, 시민들의 삶의 질을 높이는 데 중점을 두고 있다. 21 세기 초반부터 시작된 스마트 시티의 발전은 기술의 진보와 함께 더욱 가속화되고 있다. 스마트 교통 시스템, 지능형 에너지 관리, 고도화된 공공 서비스는 스마트 시티가 지향하는 핵심 목표들이다. 현대 도시는 스마트 시티로의 전환을 통해 다양한 정보통신기술(ICT)과 데이터 관리 전략을 채택하고 있다. 스마트 시티의 핵심은 정보통신기술을 활용하여 도시 운영의 효율성을 증대시키고, 시민의 삶의 질을 향상시키며, 자원 사용의 효율성을 극대화하는 데 있다. 데이터는 이러한 스마트 시티의 핵심 자원이며, 스마트 시티의 효율적인 관리와 운영에 필수적이다. 이에 따라 스마트 시티에서는 실시간으로 생성되는 방대한 양의 데이터가 안전하게 관리되어야 하며, 이러한 데이터의 보안과 개인정보보호는 중대한 연구 과제로 부상하고 있다. 스마트 시티에서 생성되는 데이터는 도시의 교통 시스템, 에너지 관리, 공공 안전 및 보건 서비스와 같은 다양한 분야에 걸쳐 있다. 이때 개인정보의 무단 유출이나 오용은 프라이버시 침해뿐만 아니라 법적 문제를 야기할 수 있다. 따라서 개인정보 보호는 시민들의 신뢰를 유지하고, 스마트 시티 서비스의 질을 보장하는 데 필수적이다[1][2].

현재 스마트 시티의 데이터 보안을 위해 다양한 연구가 진행중이다. 그 중에서도 스마트 시티의 도시 인프라, IoT 장비, 빅데이터 시스템 등의 보안 기술과 개인정보 보호를 위한 암호 기술 및 인증 기술은 중요한 연구 과제이다. 최근 경량 및 양자내성 암호 등 환경 적합형 다기종 · 고신뢰 암호 기술 개발이 활발히 추진 중이며, 생체인식기반 인증 서비스가 온라인(On-line)을 넘어 IoT 기기로 확대되어 관련 인증 기술에 대한 요구가 확대되고 있다[3]. 특히 GDPR 등 기업이 수집 및 활용하는 개인 데이터에 대한 프라이버시 강화 추세에 따라 데이터의 활용성을 강화하면서 사용자의 프라이버시를 보장할 수 있는 보안 기술과 보안 컴퓨팅 등 개인정보보호를 위한 암호 및 시스템 보안 연구도 활발히 진행 중이다[4].

시스템 및 데이터에 대한 접근 제어는 정보 보안의 핵심 요소이며, 무단 접근으로부터 자원을 보호한다. 스마트 시티 환경에서 데이터 접근 제어를 위한 기술에는 역할기반접근제어(RBAC), 속성기반접근제어(ABAC), 컨텍스트기반 접근제어(CBAC)기술이 있으며, 암호화된 데이터에 대한 접근 제어 기술로 속성기반 암호화(CP-ABE)기술은 클라우드 스토리지, IoT 등의 다양한 분야에 적용 방안이 연구되고 있다.

최근 들어 블록체인 기술은 차세대 보안 기술로 데이터 보안 문제에 대한 해결책으로 주목받고 있다. 블록체인은 분산 원장 기술로, 데이터의 불변성과 투명성을 보장한다. 이 기술은 원래 암호화폐와 금융 거래에 사용되었지만, 그 잠재력은 훨씬 더 넓은 범위에 걸쳐 있다. 블록체인의 불변성과 분산된 기록 보관 방식은 스마트 시티의 데이터 보안과 개인정보보호에 강력한 해결책을 제시할 수 있다. 블록체인을 활용한 데이터 보호 및 개인정보 보호기술로는 사용자 익명성 유지, 스마트 컨트랙트에서의 데이터 보호, 트랜잭션의 세부정보 은닉, 온체인 데이터 암호화 등의 기술이 다양하게 연구되고 있다[5]. 또한 사용자 주권을 강화하는 기술로 신원 확인 및 인증을 위한 다양한 프로젝트가 진행 중에 있다[6]. 그 외에도 분산원장 데이터 처리기술로 인메모리 DB, 분산 DB 등 기존 DB 와 결합을 통한 대용량 블록체인 데이터 처리를 위한 다양한 연구가 진행되고 있다. 이처럼 스마트 시티의 중앙 집중식 제어 기능을 가지는 시스템에서 수집하고 처리하는 데이터에 대한 위협을 보호하기 위해 블록체인 기술을 이용한 연구들이 활발히 시도되고 있다.

스마트시티에서 데이터의 효과적인 관리와 보호를 위해서는 신뢰할 수 있는 보안 모델의 개발이 필수적이다. 이에 스마트시티의 안전한 서비스를 위해서는 블록체인, 데이터 분배 서비스(DDS), 그리고 CP-ABE 와 같은 첨단 기술을 통합한 보안 모델은 안전한 데이터 저장과 데이터 활용 및 프라이버시 요구를 충족시킬 수 있는 가능성을 제시한다.

본 논문의 목적은 스마트 시티의 데이터 보안을 강화하기 위해 블록체인 기술을 이용한 데이터 보안 모델을 제안하는 것이다. 이를 위해 스마트 시티의 데이터 위협 요소와 분산 저장 방식, 그리고 접근제어 방법을 살펴보고, 적용 가능성을 분석하여 스마트 시티 미래 발전을 위한

실질적인 기술의 대안을 마련하고자 한다.

본 논문은 다음과 같이 구성되어 있다. 2 장에서는 스마트 시티와 블록체인 기술의 주요 특성과 관련 기술을 분석한다. 3 장에서는 블록체인 기술을 이용한 스마트 시티 데이터 보안을 강화하기 위한 보안 모델을 제안하고, 보안성을 분석한다. 4 장에서는 결론 및 향후 연구과제를 제시한다.

II. 관련 연구

2.1 스마트 시티(Smart City)

스마트 시티(Smart City)는 다양한 정보통신기술(ICT)을 활용하여 도시 운영의 효율성을 극대화하고, 시민의 삶의 질을 향상시키기 위한 목적으로 개발되고 있다. 이를 위해 도시 내에서 발생하는 데이터를 수집하고 분석함으로써 교통, 환경, 주거 등 다양한 도시 문제를 효과적으로 관리할 수 있다. 그러나 스마트 시티는 사이버 공격, 데이터 유출, 시스템 장애와 같은 보안 위협에 취약할 수 있다. 이러한 보안 위협은 도시의 기반 시설, 통신 네트워크, 데이터 관리 시스템 등에 영향을 줄 수 있으며, 결과적으로 시민의 안전과 개인정보보호에 큰 문제를 일으킬 수 있다. 따라서 스마트 시티를 설계하고 운영할 때는 이러한 보안 위협에 대응할 수 있는 철저한 보안 체계를 구축하는 것이 중요하다.

스마트 시티는 구현과정에서 여러 보안 문제가 발생할 수 있다. 스마트 시티의 구성요소는 디바이스와 인프라 그리고 플랫폼을 연계하는 서비스로 나눌 수 있다. 그림 1 은 스마트 시티의 프레임 워크를 나타낸 것으로, 각 구성 요소별로 보안 위협이 발생한다.

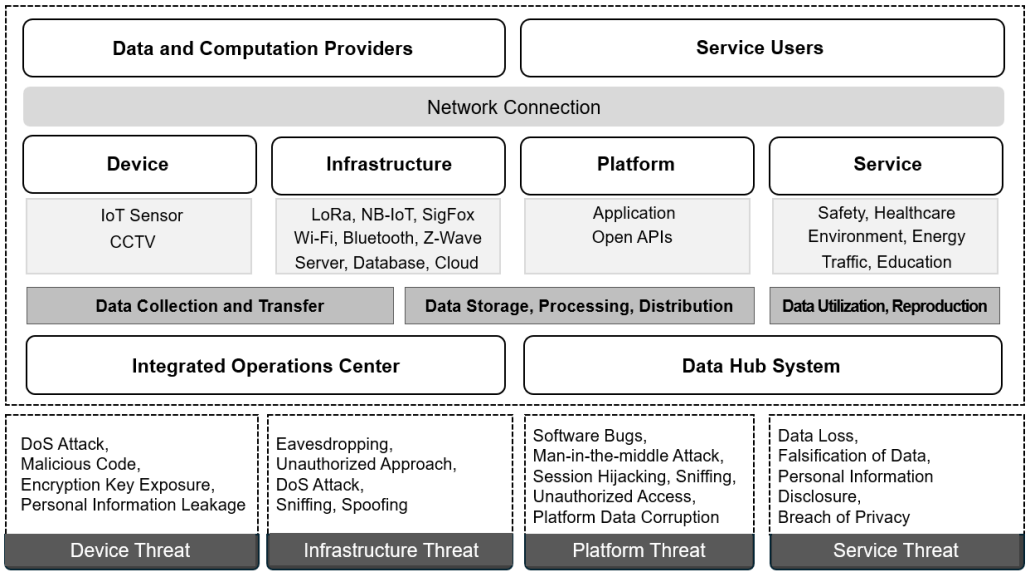

Figure 1. Smart City Framework
그림 1. 스마트 시티 프레임워크

디바이스 단계의 보안 위협으로는 디바이스 및 데이터 탈취, 데이터 위 · 변조, 비인가 디바이스 접근 등이 있으며, 이를 위해 인증 및 데이터 접근 통제, 암호화, 데이터 무결성 검증 기법 등이 필요하다. 인프라 단계의 보안 위협으로는 데이터 도청 및 감청, 정보 유출, 비인가 네트워크 접근, 서비스 거부 공격 등이 있으며 이를 위해 종단간 암호화, 비인가 접근 방지, 네트워크 침입 차단, DDoS 공격 차단 등이 필요하다. 플랫폼 단계의 보안 위협으로는 소스 코드 보안 취약점, 운영 플랫폼 물리적 보안 취약점, 다양한 인프라와 플랫폼에서 행해지는 사이버 보안 위협이 있으며, 이를 위해 Secure Coding, 사용자의 이력 통제 및 기록을 위한 로그 데이터

관리, 이상행위 탐지를 위한 보안 모니터링 및 통합 관제가 필요하다. 서비스 단계의 보안 위협으로는 신원 도용, 인증 우회, 비인가 데이터 접근, 데이터 위 · 변조 및 개인정보 유출, 프라이버시 침해 등이 있으며, 이를 위해 사용자 및 서비스 인증, 네트워크 망분리 혹은 망연계, 데이터 암호화, 개인정보 비식별화 기법 등이 필요하다. 이처럼 스마트 시티의 보안 위협은 스마트 시티 구성요소 별 전 구간에 걸쳐 발생하고 있다. 또한 전 구간에 걸친 데이터의 수집 및 활용 과정에서의 데이터 보안과 개인정보 보호는 매우 중요하다.

표 1 은 스마트 시티 구성요소별 발생 가능한 공격 및 보안 요소를 나타낸 것이다.

Table 1. Security Factors by Smart City Component
표 1. 스마트 시티 구성요소별 보안 요소

Component	Security Threat	Security Element
Device	•DoS Attack •Malicious Code •Encryption Key Exposure •Personal Information Leakage	•Physical Security(Tamper-Proofing) •Authentication / Access Control(OTP, HSM, Certificate-based Mutual Authentication) •Encryption •Data Integrity(MAC Authentication)
Infrastructure	•Eavesdropping •Unauthorized Approach •DoS Attack •Sniffing, Spoofing	•End-to-End Encryption(DTLS/TLS) •Prevent Unauthorized Access(NAC) •Detect and Block Network Intrusion(IDS/IPS) •DDoS Attack Blocking
Platform	•Software Bugs •Man-in-the-Middle Attack •Session Hijacking/Sniffing •Unauthorized Access •Platform Data Corruption	•Secure Coding •HTTP Packet Filtering •Operations Center Physical Security(PSIM) •Collecting and Archiving Logs •Security Monitoring and Integrated Control(SIEM/SOAR)
Service	•Data Loss, •Falsification of Data, •Personal Information Disclosure, •Breach of Privacy	•User/Service Authentication(FIDO, DID) •Network Separation/Network Connection •Encryption •De-identification of Personal Information

2.2 블록체인과 스마트 컨트랙트

블록체인은 분산된 데이터베이스의 형태로 데이터를 네트워크 상의 여러 노드에 분산하여 저장한다. 원장(Ledger), 해시 암호화 방식, 공개키 기반의 디지털 서명, 분산 합의 메커니즘 등의 핵심 기술이 결합되어 탈 중앙환경에서 동작하는 데이터베이스 시스템이다. 각 데이터 블록이 이전 블록에 대한 암호화된 참조를 포함하여 '체인'을 형성한다. 이 구조는 데이터의 무결성과 투명성을 보장하며, 중앙집중식 서버 없이도 정보의 안전성을 유지한다[7]. 이더리움 블록체인은 블록체인 기술을 기반으로 하는 공개 분산 컴퓨팅 플랫폼으로, 스마트 컨트랙트와 분산 어플리케이션(DApps, Decentralized Applications)을 개발하고 실행할 수 있는 환경을 제공한다. 스마트 컨트랙트는 블록체인 기술을 기반으로 한 자동 실행 계약으로, 이는 계약 조건이 충족될 때 자동으로 실행되는 프로그램 또는 프로토콜이다. 스마트 컨트랙트는 계약 조건을 코드로 작성하며, 이 코드는 블록체인 상에 저장되며 계약 조건이 충족되면 자동으로 거래를 실행한다. 이 과정은 변경 불가능하고 검증이 가능하다[8][9].

이더리움 블록체인은 표 2 와 같이 여러 계층으로 구성되어 있다. 사용자가 직접 상호작용하는 응용 계층(Application Layer), 네트워크의 모든 참가자의 합의 메커니즘이 구현된 합의 계층(Consensus Layer), 블록 체인의 데이터 구조를 관리하는 데이터 계층(Data Layer), P2P(Peer-to-Peer) 네트워크 연결을 통해 데이터를 전파하는 네트워크 계층(Network Layer)이다. 이더리움 블록체인의 각 블록은 이전 블록의 해시, 타임스탬프, 머클 루트(Merkle Root), 논스(Nonce)로 구성된다. 각 블록은 이전 블록의 해시를 사용하여 다른 블록과 연결된다. 타임스탬프는 각 블록이 생성되는 시간으로 트랜잭션의 순서를 추적하고 검증하는데 사용된다. 머클 트리는 모든 트랜잭션의 해시를 요약하여 하나의 해시값으로 집약하며, 논스는 작업 증명(Proof of

Work)과 합의 알고리즘에서 사용하는 값이다[10].

Table 2. Layered Structure of Ethereum Blockchain
표 2. 이더리움 블록체인의 계층 구조

Layer	Description	Components
Application Layer	Where users interact with smart contracts and DApps.	Smart Contracts, DApps, Business Logic, Chain Code
Consensus Layer	Ensures all nodes agree on the state of the blockchain.	Proof of Work, Proof of Stake, Consensus Algorithms
Data Layer	Manages the blockchain's data and ensures its integrity and security.	Digital Signatures, Hash, Merkle Trees, Transactions
Network Layer	Facilitates data propagation and communication across the blockchain network.	P2P Connections, Network Protocols

블록체인 기술을 스마트시티에 적용할 때, 블록체인의 불변성과 분산된 데이터 저장 방식은 스마트시티의 데이터 관리에서 높은 수준의 데이터 무결성과 보안성을 제공한다. 이는 공공 서비스의 신뢰성을 높이고, 시민들에게 안전하고 신뢰할 수 있는 디지털 환경을 제공하는 데 중요하다. 블록체인의 스마트 컨트랙트 기능은 다양한 서비스 제공에 있어서 데이터의 액세스와 관리에 필요한 복잡한 프로세스를 간소화하고 자동화와 효율성을 제공한다. 더불어 블록체인의 분산형 특징은 사이버 보안 위협에 취약한 기존 중앙 집중식 시스템의 한계를 극복하며, 데이터 보안성과 시스템의 효율성을 높일 수 있다. 이러한 강점들은 블록체인 기술이 스마트시티의 다양한 영역에서 투명성, 보안성, 자원 관리, 시민 참여, 자동화 및 데이터 통합 분야에서의 잠재력을 보여준다. 블록체인은 데이터 기록 상태를 저장하는 원장으로 내용 변경이 불가능하다. 데이터를 저장하기 위해서는 모든 네트워크 노드 간의 분산된 합의가 필요하며, 이에 대용량의 데이터를 저장하기에는 비용적으로 효율적이지 못하다. 따라서 스마트 시티의 데이터 공유 환경에 적용하기에 블록체인 기술은 P2P 네트워크가 원장을 동일하게 유지해야 하는 특성으로 많은 양의 데이터를 저장할 만큼 충분한 확장성을 지니지 못하며, 블록 생성 수행시간의 지나친 소요와 데이터의 투명성으로 발생하는 프라이버시 문제 등 기능적 한계를 가지고 있다.

2.3 IPFS(Interplanetary File System)

IPFS 는 P2P(Peer to Peer) 방식의 대용량 파일이나 데이터를 공유하기 위한 분산 파일 시스템으로, 특정 데이터가 가지고 있는 내용(Contents)으로 데이터에 접근 가능하게 한다.

클라우드와 같은 중앙 집중식 서버는 단일 클라우드 모델에 장애가 발생하면 전체 클라우드 서버가 마비되어 모든 데이터에 접근할 수 없게 된다. IPFS 는 과도한 파일 중복 문제를 해결하기 위해 설계된 분산 저장 프로토콜이다. IPFS 는 파일의 저장 위치가 아닌 파일 내용에 따라 고유한 해시 값을 할당하여, 동일한 파일을 반복적으로 저장하는 것을 방지하고 저장 공간을 절약한다.

그림 2 는 IPFS 를 이용한 데이터 분산 저장과정을 나타낸 것이다. Owner 가 IPFS 에 파일을 업로드하면 해시(Hash)를 생성한 후, 암호화된 파일의 저장 위치를 나타내는 해시 값을 반환받게 된다. 이후 업로드한 데이터는 여러 개의 암호화된 조각으로 나누어지며, 이 조각들은 블록체인에 저장되어 데이터의 안전성과 접근성을 보장하게 된다[11]. IPFS 는 웹의 분산화를 위해 만들어진 프로토콜이지만, 최근 블록체인에서 노드 수 증가에 따른 데이터 저장 문제를 해결하기 위해 IPFS 를 적용하는 사례가 증가하고 있다[12][13][14].

스마트 시티 환경에서 IPFS 의 사용은 데이터 저장과 관리의 효율성을 높이며, 블록체인과 결합하여 데이터의 분산 저장과 불변성 기록을 통한 보안성을 강화할 수 있다. 이로 인해 중앙 집중식 시스템의 단점을 극복하고 데이터 손실이나 변조의 위험 없이 안전한 데이터 공유 환경을 구축할 수 있다. 또한 대용량의 데이터 저장 및 관리의 실질적 대안으로 기능할 수 있다. 따라서 스마트 시티의 데이터 탈중앙화에 블록체인의 기능적 한계를 보완해 줄 효과적인 데이터 저장 메커니즘으로 활용할 수 있다.

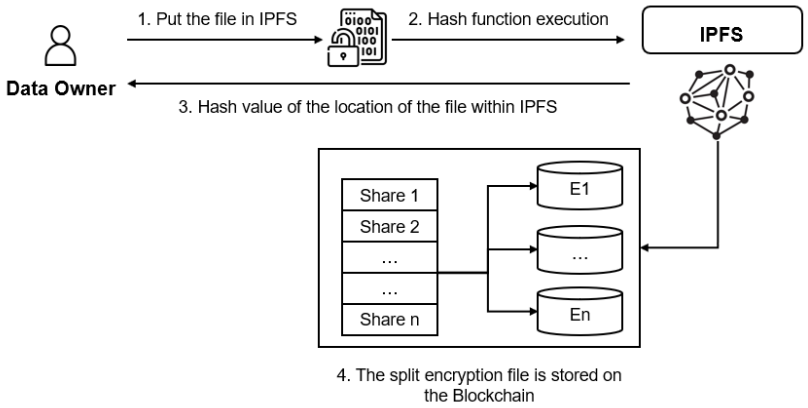

Figure 2. Data Distributed Storage Process with IPFS
그림 2. IPFS 를 이용한 데이터 분산 저장 과정

2.4 CP-ABE(Ciphertext-Policy Attribute-Based Encryption)

스마트시티에서의 데이터 접근 제어 기술은 데이터의 보안과 프라이버시를 보장하는 데 핵심적인 역할을 한다. 이러한 기술은 스마트시티의 다양한 구성 요소와 서비스가 생성, 수집, 저장, 처리하는 대량의 데이터를 안전하게 관리하는 데 필요하다. 데이터 접근 제어 기술은 무단 접근으로부터 데이터를 보호하고, 허가된 사용자만이 데이터에 접근할 수 있도록 보장한다.

속성기반암호화(ABE)는 키 정책 속성기반암호화(KP-ABE)와 암호문 정책 속성기반암호화(CP-ABE)로 구분된다. KP-ABE 는 주로 생체 인식 식별 시스템에서 사용되며, CP-ABE 는 암호화된 저장 시스템에 사용된다. CP-ABE 는 속성 기반 접근 제어(ABAC)의 암호화 버전으로, 데이터 자체에 접근 정책을 직접 통합하는 방식이다. 이는 데이터를 암호화할 때 특정 "정책(Policy)"을 적용하여, 사용자의 속성이 이 정책을 만족할 경우에만 데이터를 복호화하고 접근할 수 있게 한다. 이는 데이터가 저장되거나 전송되는 위치에 관계없이, 데이터 자체의 보안을 유지할 수 있게 하므로 클라우드 컴퓨팅과 같은 분산 환경에서 특히 유용한 방법이다. 또한 데이터 소유자는 필요에 따라 접근 정책을 변경하여 데이터에 대한 접근 권한을 동적으로 관리할 수 있다. 예를 들어 조직 내 역할 변동이 있을 때, 관련 데이터에 대한 접근 권한을 즉각적으로 조정할 수 있다.

CP-ABE 에서 접근 제어를 위한 정책 설정 시에는 임계 값 구조, 트리 기반 접근 구조, AND 게이트 및 선형 비밀 공유 구조 등이 사용된다.

다중 값 속성을 가진 일련의 AND 게이트 접근 구조는 다음과 같다[15][16].

예를 들어, 속성의 집합 $U = \{attr_1, attr_2, ..., attr_m\}$이 있을 경우, 각 $attr_i \in U$에 대해, $L_i = \{v_{i,1}, v_{i,2}, ..., v_{i,mi}\}$는 가능한 값의 집합이며, mi는 $attr_i$에 대한 가능한 값의 총합이다.

사용자의 속성 집합을 $S = \{S_1, S_2, ..., S_m\}$이라 하고, $S_i \in L_i$이고, $W = (W_1, W_2, ..., W_m)$를 접근 구조라고 하며, $W_i \in L_i$이다. 속성 집합 S 가 접근 구조 W 를 충족시킨다는 것은 즉, $S_i = W_i, i = (1, 2, ..., m)$을 의미한다.

CP-ABE 는 데이터의 암호화와 접근 제어를 데이터 소유자가 정의한 정책에 의해 직접적으로 제어할 수 있게 함으로써, 데이터 보안과 프라이버시 보호를 강화한다. 이 기법은 특히 다양한 사용자와 역할이 있는 환경에서 데이터 공유와 접근 제어를 관리하는 데 유용하다.

CP-ABE 의 구현은 복잡한 접근 제어 요구사항을 충족시키며, 효율적인 데이터 공유와 프라이버시 보호를 가능하게 한다.

2.5 동형 암호(Homomorphic Encryption)

스마트 시티 환경에서는 다양한 서비스와 시스템에 의해 많은 데이터가 실시간으로 수집되고 활용된다. 따라서 효율적인 도시 관리와 서비스 제공을 위해 개인의 위치 데이터, 건강 정보, 에너지 사용 패턴 등이 활용되지만, 이러한 정보의 무단 사용이나 유출은 개인 프라이버시를

침해할 수 있다.

동형 암호는 암호화된 데이터 상에서 직접 연산을 수행할 수 있게 하는 기술이다. 이 기술을 이용하면 데이터를 복호화 하지 않고도 필요한 계산을 실행할 수 있어, 데이터의 보안성을 유지하면서 처리 속도를 개선할 수 있다. 블록체인 내에서 이를 적용하여 차등적 데이터 활용 서비스에 사용할 수 있으며, 개인정보의 유출을 방지할 수 있다.

스마트 시티에서 동형암호를 적용하였을 때 개인의 데이터를 보호하면서도 데이터 분석 및 처리가 가능하게 한다.

예를 들어, 건강정보나 교통 패턴 데이터를 암호화된 상태에서 분석하여 서비스를 최적화할 수 있으며, 이 과정에서 사용자의 개인 정보는 외부에 노출되지 않는다. 또한 교통 시스템에서는 개인의 위치 데이터를 암호화하여 교통 흐름 분석의 통계자료로 사용할 수 있으며, 이를 통해 교통 관리의 효율성을 높이고, 개인의 이동 패턴에 대한 정보는 보호할 수 있다. 따라서 동형 암호는 개인정보를 철저히 보호하면서 기업 간, 혹은 정부조직 간 데이터를 공유하고 활용할 수 있게 한다.

III. 블록체인을 이용한 스마트 시티 데이터 보안 모델

3.1 스마트시티 데이터 보안 모델

본 장에서는 스마트시티의 데이터 보안을 위해 블록체인환경에서 IPFS 와 CP-ABE, 동형 암호 방식을 이용한 데이터 보안 모델을 제안한다.

블록체인은 분산된 방식으로 거래 내역을 기록하는 분산 원장으로, 블록체인 네트워크의 노드는 메모리 제한이 있으며, 완전한 파일이 아닌 거래 기록만 블록체인에 저장될 수 있다. 따라서 상대적으로 큰 데이터를 저장하기 위해 IPFS 를 적용하였으며, 데이터의 암호화와 접근 제어를 위해 CP-ABE 기법을 사용하였다. 또한 프라이버시 보호를 위해 데이터의 활용 목적에 따라 차등 데이터 공유 방안으로 동형 암호 방식을 적용하였다.

CP-ABE 를 이용한 데이터 암호화 과정에는 사용자의 속성 기반의 정책이 함께 포함되어 암호화 된다. 예를 들어, 시스템 속성 집합 U = {$attr_1, attr_2, attr_3, attr_4$}일 때 접근 정책 $P = ((attr_1 \ OR \ attr_2) \ AND \ attr_3 \ AND \ attr_4)$로 설정될 수 있다. 이때 데이터 사용자의 속성 집합이 접근 정책을 만족하는 경우, 해당 속성의 개인키를 사용하여 암호화된 데이터를 복호화 할 수 있다. 이러한 CP-ABE 는 사용자의 속성을 기반으로 한 데이터 접근 정책에 따라 접근 권한을 결정한다. 이를 통해 데이터 소유자는 데이터에 대한 세밀한 접근 제어를 설정할 수 있으며, 사용자는 자신의 속성에 따라 데이터에 접근할 수 있다.

제안 모델은 그림 3 과 같이 데이터 소유자(DO), 권한 에이전트(AA), 암호화 서버(ES), IPFS, 데이터 사용자(DU), 이더리움 블록체인(BC), 복호화 서버(DS)로 구성된다.

- **데이터 소유자(Data Owner, DO):** 데이터를 저장하는 주체로, 시스템 사용자에게 접근 권한을 설정하고, 속성을 기반으로 한 데이터에 대한 접근 정책을 정의한다. DO 는 암호화 서버(ES)를 통하여 CP-ABE 를 이용한 데이터를 암호화하고, 암호화된 데이터를 IPFS 에 업로드한다.
- **권한 에이전트(Authority Agent, AA):** 시스템 사용자 인증, 접근 제어 정책관리 등 IPFS 네트워크를 사용하여 안전한 데이터 공유를 위한 작업 수행을 중개하는 전달자이다. DO 가 업로드한 데이터가 IPFS 에 저장된 후, 저장된 해시 값과 데이터의 메타데이터를 블록체인에 저장한다. 이때 메타데이터에는 데이터의 생성 날짜, 키워드 인덱스 등 데이터를 사용하거나 관리하는 데 필요한 중요 식별 정보가 포함된다.

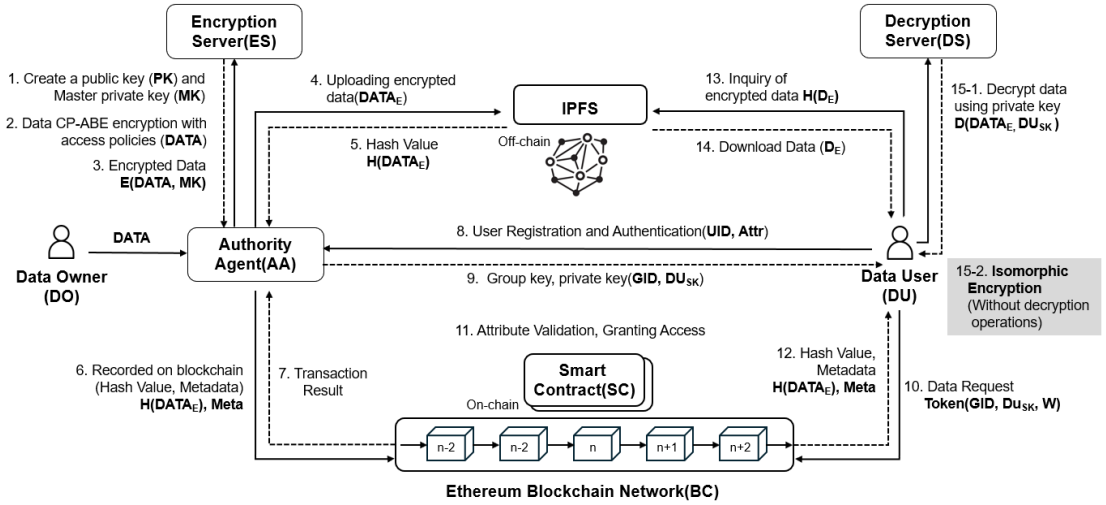

Figure 3. Proposed Smart City Data Security Model
그림 3. 제안한 스마트시티 데이터 보안 모델

• **암호화 서버(Encryption Server, ES):** 시스템 사용자에게 그룹 식별자(GID)와 속성 개인키(SK)를 발급하고, 관리한다. 또한 시스템 사용자의 인증을 수행한다. 그리고 IPFS 에 저장할 데이터를 CP-ABE 기법으로 암호화한다. CP-ABE 는 사용자의 속성(예:직책, 부서, 권한 등)을 기반으로 데이터 접근을 제어하므로, 사용자의 속성이 변경되는 경우 변경 사항을 업데이트하고, 개인키를 재발급한다.

• **IPFS(Inter Planetary File System):** 분산 파일 저장 시스템으로, DO 가 업로드한 암호화된 데이터를 분산 저장하고, 데이터에 대한 고유한 해시 값을 반환한다. 또한 DU 가 제공한 해시 값에 따라 암호화된 데이터를 반환한다. 이를 통해 데이터는 안전하게 분산되어 저장되며, DU 는 해시 주소를 통해 언제든지 해당 데이터에 접근할 수 있다.

• **데이터 사용자(Data User, DU):** 암호화된 데이터에 접근하고자 하는 사용자로, 스마트 컨트랙트에 암호화된 데이터의 해시 값을 요청한다. 해시 값을 통해 IPFS 에서 데이터를 얻을 수 있다. 이때 복호화 서버(ES)를 이용하여 사용자의 속성 집합이 접근 정책을 만족할 경우, 속성 개인키(SK)를 통해 해당 데이터를 복호화 한다. 데이터 접근 권한과 사용 목적에 따라 동형 암호를 이용하여 암호화된 상태에서 데이터를 통계 및 분석할 수도 있다.

• **블록체인(BC):** 암호화된 데이터가 업로드 된 해시 값과 데이터에 대한 메타데이터를 저장한다. 스마트 컨트랙트는 데이터에 접근을 위한 사용자와 데이터 접근 권한을 식별한다. 그리고 요청한 데이터를 찾기 위해 키워드 검색을 수행한다. 블록체인에는 데이터의 해시 값과 메타데이터만을 저장하여 블록체인의 데이터 양을 줄일 수 있다. 블록체인을 사용함으로써 시스템 내에 데이터가 업로드 되거나 공유될 때 그 정보가 블록체인에 기록되며, 블록체인 특성상 변경 불가능하며 시스템내의 모든 사용자에 의해 검증될 수 있다.

• **복호화 서버(Decryption Server, DS):** IPFS 에 저장한 암호화된 데이터를 복호화 하는 기능을 수행한다. 암호화 기능과 복호화 기능을 별도로 분리함으로써 ES 에 계산이 집중되는 것을 방지하고, DU 의 복호화 계산 비용을 줄일 수 있다.

(1) 초기 설정 및 키 생성

시스템 초기화 알고리즘이 암호화 서버(ES)에 의해 수행된다. 이 알고리즘은 DO 의 파라미터를 입력으로 받고, 공개 키(PK)와 마스터 개인 키(MK)를 생성한다. PK 는 시스템 전체에서 사용되는 반면, MK 는 중요한 정보의 암호화 및 복호화, 그리고 속성 개인키(SK)를 생성하는 데 사용된다. SK 는 DU 가 시스템에 등록하고, 자신을 식별할 수 있는 User_ID(UID)와 속성 집합(Attr)을 제시하면, ES 는 DU 가 제출한 속성을 검증하여 그룹키(GID)와 DU 의 속성 집합에 맞는 SK 를 생성한다. 생성된 SK 는 안전하게 DU 에게 전달되며, DU 는 자신의 SK 를

사용하여 데이터에 접근하고, 암호화된 데이터를 복호화 할 수 있다.

(2) 데이터 저장

DO 가 데이터를 업로드하면 AA 가 해당 데이터의 메타데이터를 생성하고, ES 에 데이터를 전달한다. ES 는 데이터를 CP-ABE 를 이용하여 암호화한다. 암호화된 데이터는 IPFS 로 업로드되며, 암호화된 데이터의 저장된 주소(해시 값)을 반환한다. 이때 IPFS 는 암호화 해싱을 사용하며, 저장된 데이터가 변경되면 해시 값도 변경되므로, 저장된 데이터의 무결성을 보장한다. AA 는 반환된 해시 값과 메타데이터를 블록체인으로 전송하고, 스마트 컨트랙트는 이를 블록체인에 기록한다. 그림 4 는 제안 모델의 암호화된 데이터를 IPFS 에 저장하는 과정을 나타낸 것이다.

(3) 토큰(Token) 생성과 데이터 검색

DU 는 토큰 생성 알고리즘을 실행한다. 이 알고리즘은 GID, SK, 쿼리 키(W)를 이용하여 토큰을 생성한다. 이때 W 는 스마트 컨트랙트에 의해 데이터 검색 프로세스에 사용되며, 검색 시 요청한 쿼리 와 일치하는 키워드를 가진 데이터의 메타데이터 암호문과 해시 값을 찾아 DU 에게 반환한다. DU 는 해시 값을 IPFS 로 전달하여 해당하는 암호화된 데이터를 다운로드 한다. 이때 복호화가 필요 없는 데이터 사용인 경우에는 동형 암호를 이용하여 암호화된 데이터 연산을 수행할 수 있다. 단, 암호화된 데이터의 복호화 가능여부는 DU 의 GID 또는 속성에 따라 달라 질 수 있다. 데이터 접근은 가능하나 복호화 가능 여부는 데이터의 접근 정책에 따라 결정된다. DO 의 데이터 등록 시 데이터의 중요도 또는 민감도에 따라 데이터 접근 정책을 설정할 수 있고, 이에 따라 암호화 기능이 수행된다. 따라서 타 그룹 또는 타 기관과의 데이터 공유 시 제한된 공유가 가능하며, 별도의 연산 없이 프라이버시를 보호할 수 있다.

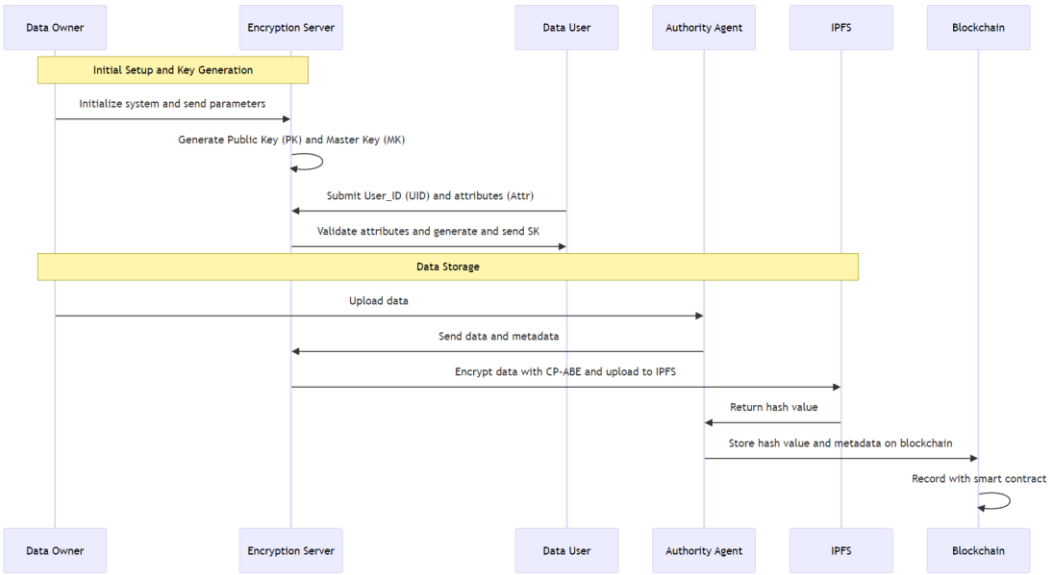

Figure 4. Data storage process for the proposed model
그림 4. 제안 모델의 데이터 저장 과정

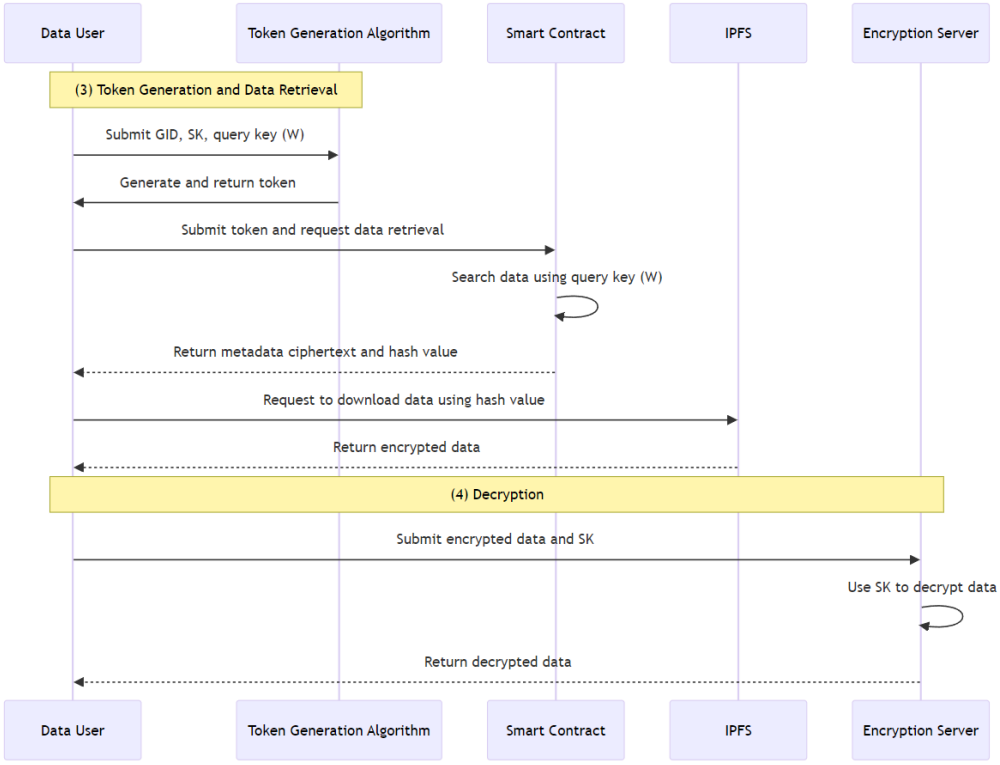

Figure 5. Data retrieval and decryption process of the proposed model
그림 5. 제안 모델의 데이터 검색과 복호화 과정

(4) 복호화

DU 는 스마트 컨트랙트로부터 검색 결과로 전달받은 해시 값을 사용하여 IPFS 에서 해당 암호화된 데이터를 검색하여 DU 장치로 다운로드 한다. DU 는 ES 를 통해 자신의 SK 를 이용하여 암호화된 데이터를 복호화한다. 이 과정은 DU 가 접근 권한을 가진 데이터에만 복호화가 가능하다.

그림 5 는 제안 모델의 데이터 검색과 암호화된 데이터의 복호화 과정을 나타낸 것이다.

3.2 스마트시티 데이터 보안 모델 보안성 분석

본 논문에서 제안한 보안 모델의 보안성을 분석하기 위하여 기밀성, 무결성, 프라이버시 보호 측면에서 분석하였다. 제안된 모델은 데이터의 안전한 저장과 데이터 활용에 있어서 CP-ABE 기법을 이용하여 데이터의 접근제어를 구현하고, 암호화된 데이터의 분산 저장을 위하여 IPFS 를 적용하였다. 또한 블록체인의 특성을 고려하여 IPFS 에 업로드 한 데이터의 고유한 해시 주소와 메타데이터를 블록체인에 저장함으로써 기밀성과 무결성을 확보하였다.

• **기밀성** : CP-ABE 는 사용자의 속성이 미리 정의된 정책에 부합하는 경우에만 복호화할 수 있도록 하므로, 이는 데이터의 기밀성을 강화하며, 오직 특정 속성을 가진 사용자만이 데이터에 접근 할 수 있도록 제한한다. 또한 동형 암호화를 사용하면 데이터를 암호화된 상태로 처리할 수 있으며, 이는 데이터의 기밀성을 유지하면서도, 필요한 연산이나 분석을 수행할 수 있다. 더불어 스마트 시티내의 타 기관 혹은 그룹간의 기밀성을 유지하면서 데이터 공유가 가능하다. 스마트 컨트랙트를 통한 접근 제어 정책의 실행은 데이터의 기밀성을 유지하지만 블록체인의 특성상 데이터의 투명성으로 인하여 블록체인을 사용하는 측면에서는 기밀성이 부분적으로 만족한다고 볼 수 있다.

• **무결성** : IPFS 는 데이터의 해시 값을 이용하여 데이터를 저장하고 접근한다. 데이터가 변경되면 해시 값도 변경되므로, 데이터의 무결성을 보장한다. 또한 IPFS 의 분산된 저장방식은

데이터의 손실 또는 변조로부터 보호된다. 블록체인의 불변성은 데이터 무결성의 중요한 특징이다. 모든 거래는 변경 불가능한 레코드로 저장되며, 모든 네트워크 참여자에 의해 검증된다. 이는 데이터의 변경 사항이 정확하게 기록되고 검증될 수 있음을 의미한다. 또한 스마트 컨트랙트는 데이터의 생성, 수정 또는 접근을 포함하여 블록체인의 모든 트랜잭션은 미리 설정된 규칙에 따라 작업이 수행되도록 관리할 수 있다. 이때 트랜잭션의 조건을 준수하지 않는 모든 트랜잭션은 자동 거부되므로 데이터의 무결성을 보장한다.

Table 3. Security Analysis of Proposed Model
표 3. 제안 모델의 보안성 분석

Security Element	Application Techniques	Security Satisfaction	Security Analysis
Confidentiality	CP-ABE	High	- Attribute-based access control enhances data confidentiality - Only users with specific attributes can access the data
	Homomorphic Encryption	High	- Allows data to be processed in its encrypted state, maintaining the confidentiality of the data.
	Blockchain	Partially Satisfied	- Access control via smart contracts supports data confidentiality, but the public nature of blockchain can limit it
Integrity	IPFS	High	- Using hash values to store and access data ensures data integrity. Changes in data alter hash values, protecting against tampering
	Blockchain	High	- All transactions are stored as immutable records and verified by network participants, effectively ensuring data integrity
Privacy	CP-ABE	High	- Strict access restrictions provided by attribute-based control effectively protect user data privacy from unnecessary access
	User Attributes & Access Policies	Medium	- User attributes could be associated with Personally Identifiable Information(PII), necessitating additional protection measures for direct privacy
	Smart Contracts & Blockchain	High	- Automatic execution of data usage policies through smart contracts, recorded immutably on the blockchain, enhances privacy protection in data usage

• **프라이버시** : CP-ABE 는 데이터 접근을 사용자의 속성에 기반하여 제한함으로써 데이터 접근 제어에서 프라이버시를 보장한다. 사용자는 자신의 속성이 정책에 부합할 때만 데이터에 접근할 수 있으므로, 불법 접근을 제한할 수 있다. 또한 사용자 등록 시 사용자를 식별하는 UID 를 사용하고, 이를 이용하여 그룹키(GID)와 사용자 속성 키(SK)를 발급함으로 데이터 접근에 더욱 세밀한 제어가 가능하다. 따라서 데이터 접근 제어를 위한 속성 기반 암호화 기법은 데이터 사용과 정책을 사용함으로써 데이터 사용에 대한 프라이버시 보호를 강화한다. 또한 데이터 사용에 따른 정책에 따라 접근 가능한 데이터일지라도 복호화 기능 유무를 결정할 수 있으며, 복호화 기능 없이도 암호화된 상태에서 연산이 가능한 동형 암호 연산을 수행함으로써 프라이버시 보호를 강화하였다.

표 3 은 제안한 스마트시티 환경에서 데이터 보안 모델의 기밀성, 무결성, 그리고 프라이버시 보호에 대한 분석을 종합적으로 나타낸 것이다. 제안 모델은 블록체인 환경에서 IPFS 추가하고, CP-ABE 와 동형암호 기법을 적용하여 데이터 보안과 프라이버시를 강화하였다.

IV. 결론

스마트시티는 다양한 정보통신기술을 활용하여 도시 운영의 효율성을 극대화하고, 시민의 삶의 질을 향상시키는 데 목적을 두고 있다. 이를 위해 많은 데이터가 수집되고, 저장 및 활용, 분석되는 과정에서 데이터 보안과 개인정보 보호에 각별한 주의가 필요하다.

본 연구에서는 스마트 시티에서 실시간으로 생성되는 대량의 데이터 관리에 있어서 향상된 데이터 보안과 개인정보보호를 위한 데이터 보안 모델을 제안하였다. 스마트시티 환경에서 데이터의 무단 액세스 및 변조로부터 데이터를 보호하기 위하여 스마트 컨트랙트를 활용하는 블록체인 네트워크에 IPFS 시스템을 적용하였다. 이는 대량의 데이터를 효율적이고 안전한 관리가 가능하게 하며, 데이터의 무단 접근 및 변조로부터 보호한다. 또한 제안된 모델은 사용자 속성을 기반으로 한 CP-ABE 암호화 기법을 활용하여 사용자의 특정 속성에 기반한 접근 제어

메커니즘을 강화함으로써 사용자 데이터의 기밀성을 높였다. 또한 데이터 접근 정책을 통해 동형암호를 활용하여 타 기관과 데이터 공유 시 암호화된 데이터를 복호화 하지 않고도 데이터 분석이 가능하게 함으로써 스마트 시티에서 처리되는 민감한 데이터에 대한 프라이버시 보호가 가능하게 하였다. 이는 스마트 시티에서 필수적인 데이터 분석과 서비스 제공을 이어갈 수 있으면서도 사용자 프라이버시를 보장할 수 있다. 블록체인과 IPFS 의 결합은 데이터 저장 및 관리의 분산화를 통해 시스템의 안정성을 강화하고, 스마트 컨트랙트를 통한 자동화된 정책 집행은 시스템의 투명성과 신뢰성을 높인다.

제안 모델의 보안성을 분석한 결과 CP-ABE 와 동형 암호화를 병행하여 사용하는 방법은 데이터의 저장과 활용성 측면에서 데이터의 기밀성과 프라이버시를 강화한다. 또한 IPFS 와 블록체인을 통합한 시스템의 구조는 데이터의 변경이 발생할 경우 해시 값의 변화를 통해 탐지할 수 있으며, 모든 거래는 변경 불가능한 레코드로 저장되어 검증되므로 데이터의 무결성을 높은 수준으로 보장한다.

본 연구에서 제안한 데이터 보안 모델은 스마트 시티의 복잡한 데이터 환경을 관리하는 데 있어서 효과적으로 사용될 수 있다. 데이터의 보안과 프라이버시 보호를 위한 다층적 접근 방식은 스마트시티가 직면한 주요 도전 과제를 해결하고, 시민의 삶의 질을 향상시키는 스마트시티 서비스의 제공을 가능하게 한다. 향후 연구에서는 제안 모델의 개념을 확장하고, 스마트시티의 안전한 보안 아키텍처를 확립하여 스마트시티 플랫폼에 도입할 수 있도록 추후 연구를 진행할 예정이다.

V. 참고문헌

[1] S. Chatterjee, A. K. Kar, Y. K. Dwivedi, and H. Kizgin, H, “Prevention of cybercrimes in smart cities of India: from a citizen’s perspective,” Information Technology & People, Vol. 32, No. 5, pp. 1153-1183, 2019.

[2] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy,” Journal of Advanced Research, Vol. 5, No. 4, pp. 491-497, 2014. https://doi.org/10.1016/j. jare.2014.02.006.

[3] A. Angelogianni, I. Politis, and C. Xenakis, “How many FIDO protocols are needed? Surveying the design, security and market perspectives,” arXiv preprint, 2021. Available: https://arxiv.org/abs/2107.00577

[4] NIST Big Data Public Working Group, “NIST Big Data Interoperability Framework: Volume 4, Security and Privacy Version 3,” National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.SP.1500-4r2

[5] Z. Xihua and S. Goyal, “Security and privacy challenges using IoT-blockchain technology in a smart city: critical analysis,” Int. J. Electr. Electron. Res, Vol. 10, No. 2, pp. 190-195, 2022.

[6] M. A. López, "Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain," IDB, 2021. http://dx.doi.org/10.18235/0002635

[7] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc, 2015.

[8] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, Vol. 151, No. 2014, pp. 1-32, 2014.

[9] D. H. Sin & J. H. Lee, “Smart contract security for Pin Tech,” *KIPS Review*, Vol. 22, No. 5, pp.54-62, 2015.

[10] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. N. Lee, “Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract,” *IEEE Access*, 2021. doi: 10.1109/ACCESS.2021.3140091.

[11] https://www.mdpi.com/2071-1050/11/24/7054

[12] A. Rajalakshmi, K. V. Lakshmy, M. Sindu, and P. P. Amritha, “A Blockchain and IPFS based framework for secure research record keeping,” International Journal of Pure and Applied Mathematics, Vol. 119, No. 15, pp. 1437-1442, 2018.

[13] I. Permatasari, M. Essaid, H. Kim, and H. Ju, “Blockchain implementation to verify archives integrity on cilegon E-archive,” Applied Sciences, Vol. 10, No. 7, 2621, 2020. http://doi.org/10.3390.app1007261

[14] J. Sun, X. Yao, S. Wang, and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS,” IEEE access, Vol. 8, pp. 59389-59401, 2020.
[15] T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based encryption with partially hidden encryptor-specified access structures,” in Applied Crypytography and Network Security, Springer, pp. 111–129, 2008.
[16] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, “A. Trustworthy users: Using IOTA and IPFS for attribute validation in CP-ABE and dCP-ABE schemes,” Smart Cities, Vol.6, No.2, pp. 913-928, 2023.

저자소개

조도은(*Do-Eun Cho*)

2007 년 2 월 충북대학교 대학원 컴퓨터공학과 박사
2008 년 3 월~현재 목원대학교 SW 교양학부 조교수

관심분야 : 정보보안, 센서네트워크, 공학교육