사물인터넷융복합논문지 Vol. 11, No. 6, pp. 137-145, 2025 https://doi.org/10.20465/KIOTS.2025.11.6.137

영지식 증명과 블록체인 기반 개인정보보호 시스템 설계 및 구현

이형우*
한신대학교 AISW대학 교수

Design and Implementation of a Privacy-Preserving System Based on Zero-Knowledge Proofs and Blockchain Mechanism

Hyung-Woo Lee*
Professor, School of Computing and Artificial Intelligence, Hanshin University

요 약 최근 디지털 전환과 함께 개인정보 활용 범위가 다양해지고 적용 분야가 지속적으로 증가하면서, 사용자 데이터의 안전한 저장, 관리 및 제공 과정이 필요하다. 기존 중앙화된 저장소 기반 개인정보 인증 모델은 데이터 유출 사고, 불법적인 추적, 서비스 제공자에 대한 과도한 신뢰 요구 등의 문제점을 내포하고 있다. 이를 해결하기 위해 본 연구는 영지식 증명(Zero-Knowledge Proof, ZKP)과 블록체인(Blockchain)을 결합한 개인정보보호 시스템을 설계하고 프로토타입을 구현하였다. 제안하는 시스템은 사용자의 민감한 개인정보를 공개하지 않으면서도 공개 검증이 가능하며, 블록체인 기반 무결성, 추적 방지 및 분산 신뢰 기능을 제공한다. 본 연구에서 구현한 결과물은 ZKP 기반 인증 프로토콜, 공개키 저장 블록체인 구조, 하이브리드 데이터 관리 및 사용자명 기반 공개키 검색 기능을 제공한다. 구현된 프로토타입을 통해 개인정보 최소 공개, 무결성 보장 및 익명성 강화 기능을 제공하여 향후 DID·공공 서비스 등 다양한 영역에서 확장 가능하다.

주제어 : 영지식 증명, 블록체인, 개인정보보호, 시스템 설계 및 구현, 정보보호

Abstract The rapid progress of digital transformation has expanded the scope and application of personal privacy data across diverse industry sectors, creating a growing demand for secure mechanisms for data storage, management, and verification. Traditional centralized personal privacy information authentication models remain vulnerable to data breaches, unauthorized tracking, and excessive reliance on service providers as trusted entities. To overcome these limitations, this study proposes a privacy-preserving personal data protection system that integrates Zero-Knowledge Proofs(ZKP) with blockchain technology. The proposed approach enables users to prove specific attributes without exposing sensitive personal information while ensuring integrity, trace resistance, and decentralized trust through blockchain. The system incorporates a ZKP-based authentication protocol, a blockchain structure for public-key storage, an on-chain/off-chain hybrid data management model, and a username-based public-key retrieval mechanism. A prototype implementation demonstrates effective data minimization, improved integrity assurance, and enhanced anonymity. The results indicate that the proposed framework can be extended to various domains, including decentralized identity (DID) systems and public-sector digital services.

Key Words : Zero Knowledge Proof, Blockchain, Personal Data Protection, System Design and Implementation, Information Security

이 논문은 한신대학교 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2025년 10월 21일 수정일 2025년 11월 12일 심사완료일 2025년 12월 16일

1. 서론

최근 디지털 전환이 가속화되면서 개인 정보가 활용되는 서비스의 종류와 규모가 급증하고 있다. 금융, 의료, 전자정부, 교육, 온라인 플랫폼 등 모든 분야에서 사용자의 신원 정보와 메시지 내 속성 정보는 서비스 이용의 기본 요소로 자리 잡았다. 그러나 이러한 환경 변화와는 대조적으로 개인정보의 안전한 저장 및 관리 방식은 여전히 중앙화된 구조에 의존하고 있으며, 이로 인해 대규모 정보 유출 사고가 지속적으로 발생하고 있다. 최근 국내에서도 발생하고 있는 개인정보가 유출되는 사례는 중앙화 데이터베이스 구조가 갖는 구조적 취약성을 보여준다. 이는 단순한 기술적 문제를 넘어 사회적·법적 문제로 확산될 가능성이 있기 때문에 개인정보에 대한 안전한 보호 체계가 더욱 필요한 시점이다.

기존의 인증 및 신원 관리 방식은 대부분 중앙화된 구조를 기반으로 서비스 제공자의 개인정보를 제공하고, 이를 기반으로 검증 절차를 통해 신원을 확인하는 방식이다. 그러나 이러한 구조는 불필요하게 많은 개인정보를 요구하며, 제출된 데이터는 검증 과정에서 제3자에게 노출되거나 재식별될 위험이 있다. 이러한 문제를 해결하기 위한 새로운 접근 방식으로 블록체인(Blockchain) 기술[1-3]과 영지식 증명(Zero-Knowledge Proof, ZKP) 기술[4-6]이 사용할 수 있다. 비트코인[7] 방식에 적용된 블록체인[8,9]은 분산 원장을 기반으로 데이터의 위변조를 방지하고 서비스 제공자에 대한 과도한 신뢰 요구를 줄여주는 기술로, 스마트계약(smart contract)과의 결합을 통해 안전한 신원 검증, 권한 관리, 데이터 무결성 보장 등 개인정보 기반 시스템의 핵심 기능을 제공할 수 있다.

그러나 블록체인 기술만으로는 개인정보 보호 문제를 완전히 해결하기에는 일정 부분 한계점이 존재한다. 예를들어 거래 기록이 공개적이고 투명한 특성 때문에 오히려 사용자의 개인정보가 외부로 노출되는 위험이 존재한다. 따라서, 만일 개인정보 데이터를 블록체인 내에 별다른 개인정보보호 조치 또는 암호화 과정 없이 저장하게 된다면 심각한 보안 문제가 발생할 수 있다.

따라서, 영지식 증명 기술은 이러한 문제점을 보완하기 위해 등장한 핵심 기술로, 사용자는 자신의 민감한 정보를 공개하지 않은 채 특정 조건을 만족한다는 사실을 수학적으로 증명할 수 있다. 예를 들어 사용자의 생년월일을 공개하지 않고도 “만 19세 이상임”을 증명할 수 있으며, 금융 정보 전체를 노출하지 않으면서도 “잔액이 일정 금액 이상임”을 증명할 수도 있다. 이러한 기능은 개인정보 노출을 최소화하면서도 신뢰 가능한 검증이 가능하다는 점에서 기존 인증 모델의 패러다임을 변화시키고 있으며, 글로벌 DID(Decentralized Identifier) 표준[10] 및 Verifiable Credential 프레임워크[11]에서도 적용 가능하므로, 이에 따라 ZKP 기반 개인정보보호 접근 방식이 빠르게 도입되는 추세다.

이에 본 연구에서는 영지식 증명과 블록체인을 결합한 개인정보보호 중심의 인증 및 데이터 검증 시스템을 설계하고 구현하였다. 제안하는 시스템은 사용자 개인정보를 블록체인에 직접 저장하지 않으면서도 블록체인의 위변조 방지 특성을 토대로 데이터 무결성을 확보한다. 또한 ZKP 기반 인증 프로토콜을 적용하여 서비스 이용 과정에서 개인정보를 노출하지 않고 요청한 속성 정보를 증명할 수 있도록 한다. 동시에 RSA 기반 공개키를 블록체인에 안전하게 저장하고, 사용자명 기반으로 해당 공개키를 검색할 수 있는 블록체인 모듈을 구현함으로써 실질적인 인증 절차에서 활용 가능한 구조를 제안한다.

본 연구에서 제시하는 구조를 적용할 경우 다음과 같은 장점을 제공한다. 첫째, 기존 중앙화 인증 구조가 가진 개인정보 과다 제공 문제를 해결하기 위해 영지식 증명 기반의 속성 인증 모델을 적용하였다. 둘째, 개인정보를 블록체인 내에 원본 그대로 노출시키지 않고도 데이터 무결성을 보장할 수 있는 블록체인 기반 아키텍처를 구현하였다. 셋째, 블록체인에서 RSA 공개키 및 ZKP 검증 관련 정보를 효율적으로 관리하기 위한 데이터 구조를 정의하며, 이를 통해 전체 시스템의 프로토타입을 구현하여 성능 평가 및 보안성 분석을 수행함으로써 제안한 시스템의 실용 가능성을 검증하였다.

본 논문의 구성은 다음과 같다. 제2장에서는 블록체인 기반 개인정보 보호 기술, 영지식 증명 기법, DID[10] 및 VC 표준[11] 등 관련 기술의 현황을 분석하였다. 제3장에서는 개인정보 보호 시스템 설계를 위한 요구사항을 정의하고 영지식 증명 기반 인증 프로토콜과 ZKP 연계 모듈 설계 구조를 제시하였다. 제4장에서는 블록체인 기반 개인정보보호 시스템 관련 프로토타입 구현 과정과 기술적 세부사항을 제시하며, 성능 평가 및 보안 분석 결과를 제시하였다. 마지막으로 제5장에서는 연구 결과를 요약하고 향후 연구 방향을 제시하였다.

2. 관련연구

2.1 개인정보보호 기술

개인정보보호 기술은 정보 주체의 프라이버시를 보호하고, 데이터 처리 과정에서 불필요한 노출을 최소화하는 것을 목표로 한다. 전통적으로는 접근 제어(access control), 암호화(encryption), 익명화(anonymization), 가명화(pseudonymization) 등의 기술이 활용되어 왔다. 그러나 이러한 기술은 정보 제공 이후에는 사용자가 통제력을 상실하는 문제가 존재하며, 정보 자체를 완전히 신뢰할 수 없는 제3자에게 제공해야 한다는 구조적 문제점을 내포하고 있다. 이에 따라 최근에는 사용자가 스스로 자신의 개인정보에 대한 제어권을 갖고, 필요한 경우에만 제한된 방식으로 정보를 증명하거나 제3자에게 공유할 수 있도록 하기 위해 영지식 증명 및 블록체인 기술을 접목할 수 있다.

2.2 영지식 증명(Zero-Knowledge Proof)

영지식 증명(ZKP)은 Goldwasser, Micali, Rackoff에 의해 처음 제안된 개념[1]으로, 어떤 주장이 참이라는 사실은 증명하되, 그 주장의 내용이나 근거에 대한 어떠한 정보도 제공하지 않는 암호학적 기법이다. 영지식 증명은 다음과 같은 세 가지 조건을 만족해야 한다.

- 완전성(Completeness): 참인 명제를 제시하면 검증자는 이를 항상 수용한다.
- 정당성(Soundness): 거짓 명제를 제시하면 검증자는 이를 거의 항상 거부한다.
- 영지식성(Zero-Knowledge): 검증자는 주장이 참임은 알 수 있으나, 그 외의 어떤 정보도 얻을 수 없다.

초기에는 대화형(Interactive)방식으로 설계되었으나, 실용적 응용을 위해 비대화형(Non-Interactive) ZKP로 발전[12]되었으며, 이밖에도 현재는 zk-SNARK[13], zk-STARK[14] 등 다양한 구현 방식이 존재한다.

2.3 zk-SNARKs의 원리와 응용

우선 zk-SNARK(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) 기법[13]의 원리와 응용 분야에 대해 살펴보고자 한다. zk-SNARK 기법은 비대화형 영지식 증명의 대표적인 구현 방식 중 하나로, 특히 간단하고 안전한 증명(Succinctness) 기능과 빠른 검증 속도를 제공하는 점에서 블록체인 환경에 매우 적합하다. zk-SNARK는 다음과 같은 구조를 갖는다.

- 초기 설정(Trusted Setup): 증명 생성 전 공통 참조 문자열(CRS)을 생성하는 초기 설정 과정
- 증명자(Prover): 개인 정보와 계산 과정을 바탕으로 짧은 증명(π)을 생성
- 검증자(Verifier): 증명과 공개 입력만으로 조건의 만족 여부를 신속하게 검증 과정 진행

zk-SNARK 방식은 Zcash[15,16] 등에서 실제로 활용되고 있으며, 사용자 자격 검증과 익명 송금 및 프라이버시 보존 스마트 컨트랙트 등의 분야에 응용되고 있다. 다만 초기 설정(Trusted Setup)이 필요하다는 점은 보안 측면에서 기존 방식과 차별점이 있는 부분이다.

2.4 블록체인 기반 개인정보보호 시스템

블록체인은 데이터의 위·변조 방지, 탈중앙화, 투명성 보장이라는 특성을 바탕으로, 개인정보 인증 시스템에도 다양하게 응용되고 있다. 대표적인 사례로는 다음과 같은 기술들이 있다.

- Self-Sovereign Identity(SSI): 사용자가 자신의 신원 정보를 직접 통제하는 디지털 신원 프레임워크
- Decentralized Identifiers(DID): 중앙기관 없이도 생성 및 검증 가능한 분산형 식별자
- Verifiable Credentials(VC): 발급자가 서명한 인증서를 사용자와 검증자가 검증하는 방식

이러한 구조는 신뢰할 수 있는 제3자 없이도 인증이 가능하며, 블록체인의 불변성과 투명성 덕분에 신뢰 기반을 제공할 수 있다. 그러나 기존 시스템들은 대개 자격 증명 자체를 암호화하거나 숨기는 수준에 머물며, 영지식 증명을 통합하여 정보 노출 자체를 제거하는 방식은 제한적으로만 시도되고 있다.

2.5 기존 연구의 한계 및 본 연구의 차별성

기존 연구들은 다양한 암호화 및 인증 기술을 통해 개인정보보호를 강화하고자 하였으나 다음과 같은 한계가 존재한다. 기존의 영지식 증명의 방식[18-22]은 실제 적용 사례가 부족하다. 또한, 기존 영지식 증명 기법을 블록체인 등의 실세 서비스 기술과 통합 가능성이 미비하며, 블록체인은 데이터 저장소로만 사용하는 수준이므로 증명 생성 및 검증 연계 구조 적용이 미흡한 실정이다.

이러한 문제점을 개선하기 위해 블록체인과 영지식 증명 기술을 적절히 조합할 경우 개인정보보호와 디지털

신원 분야에 적용하여 핵심적인 역할을 수행할 수 있도록 다양한 연구[22-25]가 활발히 진행되고 있다. 먼저 개인정보 보호 기술의 전체 흐름을 살펴보면, 기존 암호 기술[26]은 데이터의 기밀성·무결성·인증을 제공하는 데 효과적이지만, 데이터 자체의 비공개 상태에서 특정 조건을 증명하는 기능은 제공하지 못한다.

블록체인 기술은 분산된 형태로 데이터를 저장하여 중앙화된 신뢰기관 없이도 데이터의 무결성과 기록의 변경 불가능성을 보장할 수 있다는 장점이 있다. 이 때문에 의료 기록 관리, 전자 투표 시스템, 디지털 자산 관리 등 다양한 분야에서 블록체인이 개인정보 검증 및 기록 관리 기술로 활용되고 있으나, 블록체인에는 모든 거래 기록이 참여자에게 공개된다는 특성 때문에, 잘못된 방식으로 설계될 경우 오히려 개인정보가 노출될 가능성이 존재한다. 또한 블록체인의 저장 비용이 크고 확장성이 낮다는 점은 개인정보관리 서비스에 적용하는 데 실질적인 제약 요소로 작용한다.

따라서 블록체인 기술에 영지식 증명(ZKP)을 접목할 경우 이러한 문제점을 해결할 수 있다[9,10]. ZKP는 민감한 실제 데이터나 속성을 제3자에게 공개하지 않고도 “해당 데이터가 특정 조건을 만족함”을 증명하는 기능을 제공한다. 예를 들어 사용자의 생년월일을 공개하지 않고도 성인 여부를 증명할 수 있고, 잔고 정보를 밝히지 않고도 일정 금액 이상의 자산을 보유하고 있음을 증명할 수 있다. 이에 따라, 블록체인의 무결성·분산 신뢰 기반과 영지식 증명의 개인정보 비공개 인증 능력을 결합하는 것은 매우 높은 시너지를 제공할 수 있다. 그러나 이러한 결합 모델은 아직 연구 초기 단계에 있으며, 실제 구현 과정에서 데이터 구조 설계, 성능 문제, 보안 모델 취약점 등의 해결해야 할 과제가 다수 존재한다. 따라서, 본 연구는 이러한 한계를 보완하고 보다 실질적인 개인정보 보호 중심 시스템을 구축하기 위한 설계와 구현 방향을 제시한다는 점에서 기존 연구와 차별성을 가진다.

3. 제안하는 영지식 증명과 블록체인 기반 개인정보보호 시스템 모델 설계

3.1 시스템 요구사항 분석

본 연구에서 제안하는 시스템의 핵심 요구사항 중 첫 번째는 데이터 최소 공개(Data Minimization) 원칙이다. 서비스 이용 과정에서 필요한 정보만을 검증할 수 있어야 하며, 그 외 상세한 개인정보는 노출되어서는 안 된다. 예를 들어 사용자가 성인 인증을 위해 생년월일 전체를 공개해야 하는 기존 방식은 불필요한 정보 공개로 인해 재식별 공격이나 데이터 유출 시 개인에게 큰 피해를 입힐 수 있다. 두 번째 요구사항은 데이터 무결성(Data Integrity) 보장이다. 개인정보 자체는 오프체인에 저장하더라도, 그 정보가 변조되지 않았음을 누구나 검증할 수 있어야 한다. 따라서 블록체인을 활용한 무결성 증명 구조가 필요하다.

세 번째 요구사항은 익명성 및 비추적성이다. 시스템 사용자가 여러 서비스에서 동일한 식별자로 인증을 반복할 경우, 서비스 제공자들은 해당 사용자를 상호 연관해 추적할 수 있는 위험이 존재한다. 이를 방지하기 위해 ZKP 기반 일회성 인증 구조 또는 Nonce 기반 증명 구조가 요구된다. 네 번째 요구사항은 분산된 신뢰 모델 지원이다. 특정 기관이나 서버에 대한 과도한 신뢰가 필요 없는 구조여야 하며, 블록체인의 합의 메커니즘을 활용하여 전체 시스템의 신뢰성을 확보해야 한다.

이러한 요구사항을 바탕으로 본 연구에서는 다음과 같은 설계 목표를 설정하였다. 첫째, 사용자가 민감한 개인정보를 직접 공개하지 않고도 검증 가능한 영지식 기반 속성 인증 모델을 구축하며, 둘째, 블록체인에 저장된 데이터를 통해 모든 트랜잭션과 Credential[12]의 무결성을 검증할 수 있는 구조를 설계한다. 셋째, 개인정보는 오프체인에 저장하면서도 그 무결성을 온체인에서 확인할 수 있는 하이브리드 구조를 구현하며 블록체인에 저장된 사용자 공개키를 통해 인증 가능성을 확보하고, UserName 기반 탐색 기능을 제공하여 실제 서비스 활용성을 높이는 것을 목표로 한다.

3.2 영지식 증명 기반 인증 모델 설계

영지식 증명을 활용하여 개인정보를 노출하지 않고도 검증이 가능한 인증 프로토콜을 설계하는 인증 모델의 동작 과정을 아래와 같이 제시하고자 한다.

ZKP 기반 인증 모델의 기본 구조는 Prover(증명자:사용자), Verifier(검증자:서비스 제공자), Issuer(자격증명 발급기관) 그리고 Blockchain Layer로 구성된다. 사용자는 Issuer로부터 본인의 실제 개인정보를 기반으로 Credential을 발급받되, 이 Credential의 해시만 블록체인에 기록하여 무결성을 보장한다. 실제 개인정보 및 Credential 원본은 사용자 단말이나 Off-chain 저장소에 보관되며, 로컬 저장소를 활용할 수 있다.

Credential 발급 과정은 다음과 같다. 사용자는 자신을 증명하는데 필요한 개인정보를 Issuer에게 제출하고, Issuer는 이를 검증한 후 ZKP 생성에 적합한 속성 형태로 정규화된 Credential을 생성한다. 해당 Credential은 JSON 기반 구조로 설계될 수 있으며, Credential 전체 또는 핵심 속성의 해시가 블록체인에 기록된다. 이 과정에서 사용자는 자신의 공개키를 함께 등록하여 이후 Verifier가 검증을 수행할 수 있도록 한다.

ZKP 모델 핵심 구조 설계는 사용자가 증명해야 할 조건을 수학적 제약식(Constraint System)으로 표현하여 생성된다. 예를 들어 “사용자가 만 19세 이상임"을 증명하는 방식은 ”현재년도 – 생년월일“이 19보다 크거나 같은지를 판단하는 조건식으로 구성된다. 제안 모듈은 Python 언어를 사용하여 구현할 수 있으며, 증명 생성 및 검증 작업을 수행할 수 있다.

위 사항을 토대로 제시한 인증 프로토콜은 다음과 같은 흐름으로 진행된다. 첫째, Prover는 자신이 보유한 Credential을 이용해 ZKP를 생성한다. 둘째, Verifier는 Prover로부터 전달받은 증명과 공개 입력값을 기반으로 검증을 수행한다. 이때 블록체인에 저장된 Credential의 해시값을 조회하여 Credential이 변조되지 않았음을 확인한다. 셋째, Verifier는 증명이 유효하면 필요한 서비스 접근을 허용한다. 이 과정에서 어떤 개인정보도 공개되지 않으며, Prover는 동일한 Credential을 기반으로 여러 개의 ZKP를 생성하여 재사용 위험을 줄일 수 있다.

4. 영지식증명과 블록체인 기반 개인정보보호 시스템 설계 및 구현

4.1 시스템 설계

본 장에서는 제안 시스템의 전체 아키텍처와 블록체인 데이터 구조, 온체인·오프체인 데이터 관리 방식, 그리고 인증 흐름 과정에 대해 설명한다. 제안하는 시스템은 개인정보를 블록체인에 직접 저장하지 않으면서도 무결성을 확보할 수 있도록 설계되었으며, 영지식 증명을 활용해 서비스 제공자에게 개인정보를 공개하지 않고 검증할 수 있도록 한다.

시스템 아키텍처는 크게 네 가지 구성요소로 이루어진다. 첫째, 사용자 클라이언트는 Credential 저장, ZKP 생성, 인증 요청 등의 작업을 수행한다. 둘째, Issuer는 사용자에게 Credential을 발급하고, Credential 해시와 공개키를 블록체인에 기록한다. 셋째, Verifier는 사용자가 제시한 증명과 블록체인에 기록된 데이터를 통해 검증을 수행한다. 넷째, Blockchain Layer는 공개키, Credential 해시, ZKP 검증 기록 등 최소한의 정보만을 저장하는 용도로 사용된다.

블록 구조는 블록 인덱스, 이전 블록 해시, 타임스탬프, 사용자명(UserName), RSA 공개키, Nonce, 그리고 블록 해시 정보 등과 같은 필드 정보를 포함한다. 이러한 구조는 블록체인의 무결성을 유지하면서 사용자 인증에 필요한 최소한의 정보를 저장할 수 있도록 해준다. RSA 공개키는 사용자가 생성한 키이며, Verifier는 이를 통해 ZKP 검증 과정에서 필요한 서명 확인 절차를 수행할 수 있다.

UserName 기반 공개키 검색 기능은 블록체인의 탐색 기능을 통해 구현된다. Verifier는 사용자명이 주어진 경우 해당 사용자의 공개키를 블록체인에서 조회하여 검증에 활용할 수 있다. 이 기능은 실제 서비스 구현 시 인증 절차를 간소화하고 효율성을 크게 향상시킨다.

데이터 저장 방식은 온체인·오프체인 분리 구조를 따른다. 온체인에는 공개키, Credential 해시, ZKP 검증 정보 등 공개가 가능한 최소 정보만 저장되며, 개인정보 자체는 오프체인에 저장된다. 이는 개인정보 유출 위험을 줄이고, 블록체인의 저장 비용과 확장성 문제를 동시에 해결할 수 있는 방식이다.

이를 토대로 전체 처리 흐름은 다음과 같다. 사용자는 서비스 이용을 위해 ZKP를 생성하여 Verifier에게 전송한다. Verifier는 블록체인에서 해당 사용자 공개키와 Credential 해시를 조회하여 무결성을 확인하고 ZKP를 검증한다. 검증 결과가 유효하면 서비스 접근을 허용한다. 이 과정에서 사용자의 실제 개인정보는 어느 단계에서도 노출되지 않아 높은 수준의 프라이버시를 제공한다.

4.2 시스템 구현 과정

제안된 시스템을 구현한 프로토타입의 구성 요소와 개발 환경, 구현 방식, 그리고 동작 시나리오는 다음과 같다. 프로토타입 구현은 Python 언어를 사용하였으며, 블록체인 모듈과 영지식 증명 모듈로 구성되어 있다.

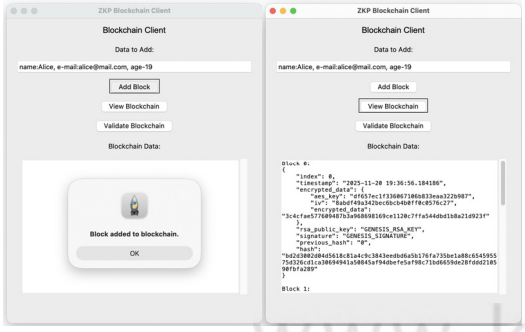
개발 환경은 Python 3.11과 PyCryptodome 라이브러리를 기반으로 하였으며, SHA-512 해시 함수, RSA 키 생성, AES 암호화 등 다양한 암호 기능을 제공한다. 개발된 시스템은 로컬 환경에서 실행되며, 사용자가 ZKP를 생성하고 Verifier가 이를 검증하는 과정을 수행한다. 블록체인 모듈은 Block 클래스와 Blockchain 클래스로 구성되며 각 블록은 인덱스, 타임스탬프, 이전 해

시, 사용자명, 공개키, Nonce 그리고 블록 해시를 포함한다. mine_block() 메서드는 PoW(Proof of Works) 기반 합의 과정을 수행하여 블록을 생성한다. 시스템은 UserName 기반으로 공개키를 탐색할 수 있으며, 이를 바탕으로 ZKP 검증 시 인증 기능을 수행한다.

프로토타입 동작 시나리오는 다음과 같다. 사용자는 자신의 실제 생년월일을 기반으로 ZKP를 생성한다. 이때 Verifiable Credential의 해시는 이미 블록체인에 기록되어 있다. Verifier는 사용자로부터 받은 ZKP를 검증하며, 블록체인에서 해당 사용자 공개키 및 Credential 해시를 조회하여 무결성을 확인한다. 검증이 유효할 경우, Verifier는 인증 결과를 반환하고 서비스 접근을 허용한다.

4.3 시스템 구현 결과

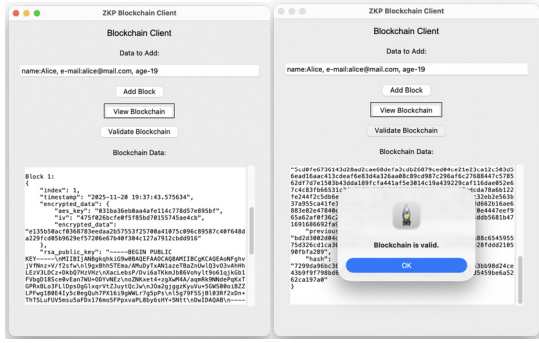
클라이언트/서버 기반 개인정보 데이터 블록체인 정보 시스템 구현 결과는 다음과 같다. 개인정보 데이터 정보를 저장한 블록체인에 대해 등록 과정을 수행하고 저장된 블록 정보를 검색하는 과정은 다음 그림 1과 같다. Python 3.11 인터프리터를 이용하여 아래 그림과 같이 개인정보 데이터 블록체인 서버와 클라이언트 모듈을 구현하였다. 블록체인 데이터에 대한 기밀성, 무결성 및 위변조 방지 기능을 제공하기 위해 PyCryptodome 모듈을 이용하여 AES 암복호화 과정 및 SHA-512 기반 해시 값 및 RSA 기반 전자서명을 생성하고 이를 개인정보 데이터 블록체인 내에 저장할 수 있는 시스템을 구현하였다. PyCharm IDE를 이용하였으며, TCP 소켓을 이용하여 Multi-Thread 방식으로 클라이언트/서버 모듈을 개발하였다. 아래 그림 1과 같이 개인정보 데이터 블록체인 클라이언트 모듈에 개인정보 데이터 정보를 입력하면 해당 내용은 암호화되어 서버로 전송되며, 서버 내 블록체인에 등록되는 구조이다.



[Fig. 1] ZKP Blockchain Client Module

서버에서는 클라이언트와의 연결 정보를 표시하며, 클라이언트로부터 개인정보 데이터 데이터 등록 요청을 받아 블록체인 내에 저장/등록하는 과정을 수행한다.

블록체인 시스템에 대해 아래 그림 2와 같이 블록체인에 저장/등록된 정보에 대한 검색 과정을 제공한다. 클라이언트에서 개인정보 데이터 정보에 대해 키워드 검색 과정을 수행하면 스마트 컨트랙트 정보를 토대로 서버 내 블록체인에 저장된 해당 블록 정보를 검색하고 이를 서버에 출력하는 기능을 설계 및 구현하였다.



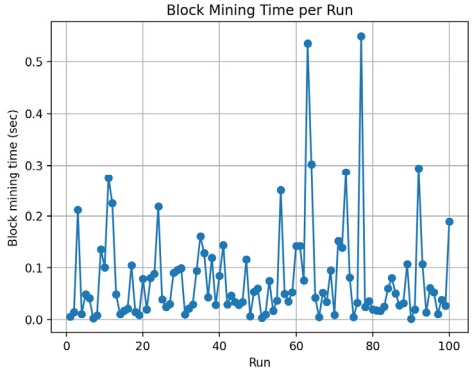
[Fig. 2] ZKP Blockchain 저장 및 확인

구현한 시스템에는 아래 그림 3과 같이 블록체인 내에 개인정보에 대한 영지식 증명 기반 검증 과정을 제공한다.

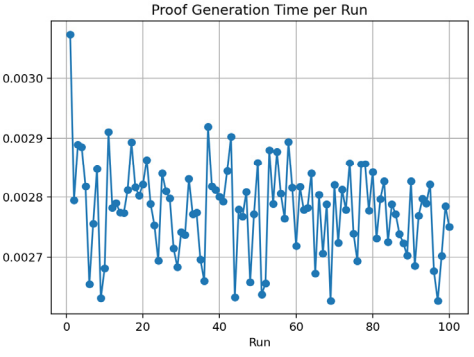
[Fig. 3] ZKP Blockchain 기반 개인정보 데이터 검증결과

4.4 성능 평가

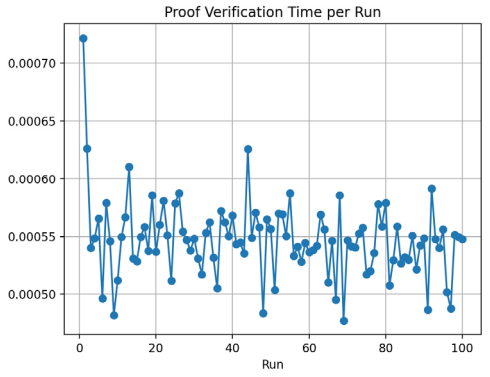
본 장에서는 제안된 시스템의 성능과 보안성을 평가하고, 기존 중앙화 인증 구조와 비교하여 본 연구의 효과를 검증하였다. 우선 제안 시스템의 성능을 평가하기 위해 아래 그림 3~5와 같이 블록 생성 속도, ZKP 생성 및 검증 속도, 온체인·오프체인 데이터 처리 시간 등을 측정(총 100회 수행)하였다. 블록 생성과 검증 작업은 비교적 빠르게 이루어졌으며, ZKP 생성 단계가 가장 큰 연산 부담을 차지했으나 최신 하드웨어 환경에서는 실용적인 수준으로 나타났다. ZKP 기반 구조로 인해 사용자의 실제 개인정보는 Verifier에게 전혀 공개되지 않으며, 블록체인에 저장된 Credential 해시를 통해 데이터 무결성이 보장된다. 또한 인증 과정에서 일회성 Nonce를 활용하여 동일한 증명이 반복 사용되는 것을 방지할 수 있다.



[Fig. 4] ZKP Blockchain 시스템 성능 평가 결과
(블록체인 생성 시간 : 100회 수행)



[Fig. 5] ZKP Blockchain 시스템 성능 평가 결과
(블록체인 영지식 증명 관련 내용 생성 시간 : 100회 수행)



[Fig. 5] ZKP Blockchain 시스템 성능 평가 결과
(영지식 증명 기반 블록체인 검증 수행 시간 : 100회 수행)

실험 결과 PoW 관련 블록 채굴 과정의 난이도에 따라 블록 생성 시간에 다소 차이가 발생하며 100회 수행 시 평균 0.15초가 소요되는 것으로 나타났다. 그리고 영지식 증명 과정 수행 및 검증 과정에 각각 소요되는 시간을 확인할 수 있었다. 또한 기존 중앙화 인증 모델과 비교했을 때 본 연구에서 설계 및 구현한 시스템은 다음과 같은 장점을 제공한다. 첫째, 개인정보 제공량이 크게 줄어 재식별 위험이 감소하였다. 둘째, 신뢰기관에 대한 의존성이 줄어들고, 서비스 제공자도 사용자 데이터에 접근할 필요가 없어 보안 위협이 감소하였다. 셋째, 모든 검증 기록은 블록체인에 의해 보호되므로 조작 및 위변조가 불가능하였다. 이러한 분석 결과는 제안된 시스템이 개인정보보호 중심의 차세대 인증 모델로서 충분한 가능성을 지니고 있음을 확인할 수 있었다.

구현한 시스템에서 제공하는 기능을 요약하면 다음과 같다. 첫째로 무결성 검증 측면에서는 블록체인의 해시 기반 검증 절차와 스마트 컨트랙트의 자동화된 검증 로직이 실효성 있게 작동되는 것을 확인할 수 있었다. 또한 기존 시스템은 공유된 개인정보 데이터의 변경 여부를 외부에서 실시간으로 확인하기 어렵지만, 제안 시스템에서는 모든 트랜잭션 기록이 블록에 포함되어 감사 추적이 가능하였다. 지연 시간 측면에서는 블록체인의 블록 생성 주기가 일부 성능 제한 요소로 작용하였으나, 실제 공유 지연 시간은 평균적으로 오히려 감소하였다. 이는 데이터 전송 및 검증 절차가 중앙 서버를 거치지 않고 클라이언트/서버 간에 직접 이루어졌기 때문이다. 결국 제안한 시스템은 정보 공유의 신뢰성과 실시간성, 무결성 보장 측면에서 기존 개인정보보호 모델보다 우수한 성능

을 보였으며, 특히 자동화 및 감사 기능 구현에 있어 실질적인 효과가 있음이 확인되었다.

5. 결론

본 연구에서는 영지식 증명과 블록체인을 결합한 개인정보 보호 시스템을 제안하고, 이를 기반으로 한 프로토타입을 설계 및 구현하였다. 제안된 시스템은 개인정보를 직접 공개하지 않고도 인증할 수 있도록 하여 데이터 최소 공개 원칙을 실현하며, 블록체인의 분산 신뢰 기반으로 데이터 무결성을 보장한다. 또한 사용자 공개키를 블록체인에서 검색할 수 있는 구조를 구현하여 실제 인증 절차에 적용 가능한 실용적 모델을 제시하였다. 실험 결과, 제안된 모델은 성능 측면에서도 실용적이며 다양한 서비스 환경에 적용 가능함을 확인하였다.

그러나 본 연구에서 제시한 내용은 일부 추가적인 개선사항을 포함하고 있다. 먼저 ZKP 적용 난이도 및 생성 비용이 아직 높아 모바일 환경에서의 성능 최적화가 필요하다. 또한 블록체인의 확장성 문제는 여전히 해결해야 할 과제로 남아 있다. 마지막으로 본 연구에서 구현한 모듈은 특정 속성 정보에 대한 영지식 증명 과정에 초점을 맞추었기 때문에, 금융·의료·공공 서비스 등에서 요구되는 복잡한 조건을 처리하기 위해서는 추가적인 모듈 수정 및 보완 과정이 필요하다.

향후 연구로는 블록체인 확장성 기술을 접목하여 ZKP 기반 인증의 성능을 개선하고, 스마트계약을 활용해 검증 과정을 자동화하는 방안을 연구할 계획이다. 또한 기존의 개선된 프라이버시 보호 기술과의 결합 가능성을 탐구하여 보다 강력한 개인정보 보호 기반을 구축할 수 있을 것으로 예상되며, 궁극적으로는 DID 및 Verifiable Credential 표준과 완전한 호환이 가능한 ZKP 기반 인증 프레임워크를 구축하여 실제 산업 환경에 적용할 필요가 있다.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Proc. IEEE BigData Congress, pp.557–564, 2017.

[2] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems,” SIAM Journal on Computing, Vol.18, No.1, pp.186–208, 1989.

[3] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A survey on privacy in blockchain systems using zero knowledge proofs,” IEEE Communications Surveys & Tutorials, 2023.

[4] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” Journal of Cryptology, Vol.1, No.2, pp.77–94, 1988.

[5] A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” in Proc. CRYPTO, pp.186–194, 1986.

[6] E. Ben-Sasson et al., “Zero-Knowledge Proofs: Survey and Applications,” Foundations and Trends in Privacy and Security, Vol.2, No.1, pp.1–98, 2017.

[7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[8] S. R. Shashidhara, R. Chirakarotu Nair & P. K. Panakalapati, “Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions,” Security & Privacy, Vol.8, No.1, 2024.

[9] S. Ruj, “Zero-Knowledge Proofs for Blockchains,” in Proc. DSN-S (Dependable Systems and Networks Symposium), IEEE Computer Society, 2024.

[10] W3C, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, 2022.

[11] W3C, “Verifiable Credentials Data Model v1.1,” W3C Recommendation, 2021.

[12] J. Groth, “Short pairing-based non-interactive zero-knowledge arguments,” ASIACRYPT, Vol.6477, pp.321–340. 2010.

[13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, “SNARKs for C: Verifying program executions succinctly and in zero knowledge,” CRYPTO, Vol.8042, pp.90–108, 2013.

[14] I. Bentov, A. Gabizon, and Z. Ji, “ZK-STARKs: Proofs with Polylogarithmic Verification,” IACR ePrint, Vol.46, 2018.

[15] I. Miers, C. Garman, M. Green and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” IEEE S&P, pp.397–411, 2013.

[16] D. Chaum, “Blind signatures for untraceable payments,” CRYPTO, 1982.

[17] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou,“Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” IEEE S&P, pp.839–858, 2016.

[18] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” CRYPTO, Vol.10401, pp.357–388, 2017.

[19] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," IEEE Communications Surveys & Tutorials, Vol.20, No.4, pp.3416-3452, 2018.

[20] S. Bowe, J. Grigg, and D. Hopwood, "Hash-based Accumulators and Applications in Zero-Knowledge Proofs," IACR ePrint, Vol.1188, 2018.

[21] K. Christidis and M. Devetsikiotis,"Blockchains and smart contracts for the Internet of Things," IEEE Access, Vol.4, pp.2292-2303, 2016.

[22] P. Dunphy and F. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," IEEE Security & Privacy, Vol.16, No.4, pp.20-29, 2018.

[23] H. Halpin and V. Bucena, "Zero-Knowledge Proofs for Verifiable Credential Issuance and Presentation," IEEE Security & Privacy, Vol.19, No.2, pp.14-25, 2021.

[24] L. S. Ferreira, J. F. Santos, and D. C. Muchaluat-Saade, "Blockchain and distributed ledger technologies for identity management: A survey," Computer Communications, Vol.181, pp.120-142, 2022.

[25] Z. Hou, Q. Zhang, X. Li and X. Xie, "Leveraging zero knowledge proofs for blockchain-based data-centric privacy and security," Electronics, Vol.13, No.21, Nov. 2024.

[26] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. CRC Press, 2020.

이 형 우(Hyung-Woo Lee) [종신회원]

■ 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
■ 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
■ 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
■ 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
■ 2003년 3월 ~ 현재 : 한신대학교 AISW대학 교수

〈관심분야〉
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식, 지능형 사이버공격 대응