JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 11, pp. 311-318, November 2026
https://doi.org/10.9708/jksci.2026.31.11.311

A Study on IoT User Authentication Using a Privacy-Preserving Blockchain-Based SSO Model

Eun-Gyeom Jang*

*Professor, Dept. of Computer Engineering, Jangan University, Hwaseong, Korea

[Abstract]

As IoT devices proliferate across smart homes, industry, healthcare and autonomous mobility, users face repeated authentication burdens and growing credential-management risks. Conventional Single Sign-On (SSO) improves usability but creates a single point of failure at the central Identity Provider (IdP), which can also observe every service a user accesses. This paper proposes PB-SSO (Privacy-preserving Blockchain-based Single Sign-On), which uses a permissioned blockchain as a trust layer. PB-SSO combines Decentralized Identifiers (DIDs) with BBS+-signed Verifiable Credentials (VCs); randomized presentation proofs and per-service domain pseudonyms provide cross-service unlinkability, and only hashes and revocation data are recorded on-chain. Simulated analysis based on measured cryptographic costs shows an authentication latency of about 53 ms in an edge environment, compared with about 120 ms for an OIDC flow with a cloud IdP, while authentication remains available during IdP outages.

▸ **Key words**: Blockchain, Single Sign-On, IoT Authentication, Privacy

[요 약]

IoT 기기가 스마트홈, 스마트팩토리, 헬스케어, 자율주행 모빌리티로 확산되면서 사용자가 여러 IoT 서비스에 반복해서 인증해야 하는 부담과 인증 정보 관리의 위험이 커지고 있다. 기존 SSO(Single Sign-On)는 편의성을 높이지만, 중앙 신원 제공자(IdP)가 단일 장애점이 되고 사용자의 모든 서비스 이용 이력을 관찰할 수 있다는 한계가 있다. 본 논문은 허가형 블록체인을 신뢰 계층으로 활용하는 PB-SSO(Privacy-preserving Blockchain-based Single Sign-On) 모델을 제안한다. 제안 모델은 분산 식별자(DID)와 BBS+ 서명 기반 검증 가능한 자격증명(VC)을 사용하며, 제시할 때마다 무작위화되는 증명과 서비스별 도메인 가명으로 서비스 간 연결 불가능성을 보장하고, 블록체인에는 해시와 폐기 정보만 기록한다. 암호 연산을 실측하고 이를 바탕으로 모의 분석한 결과, 제안 모델의 엣지 환경 인증 지연은 약 53ms로 클라우드 IdP 기반 OIDC 흐름(약 120ms)보다 낮았으며, 중앙 IdP 장애 시에도 인증이 유지되었다.

▸ **주제어**: 블록체인, SSO, IoT 인증, 프라이버시

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Computer Engineering, Jangan University
• Received: 2026. 10. 12, Revised: 2026. 10. 29, Accepted: 2026. 11. 03.

Copyright © 2026 The Korea Society of Computer and Information
http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945
www.kci.go.kr

I. Introduction

사물인터넷(IoT, Internet of Things)은 센서, 액추에이터, 통신 모듈을 갖춘 사물이 네트워크로 연결되어 데이터를 수집·교환하고 상호 동작하는 환경이다[1]. 전 세계 IoT 연결 기기 수는 2025년 약 211억 대로 추정되며[2], 스마트홈의 원격 제어, 스마트팩토리의 예지보전, 헬스케어의 원격 모니터링, 스마트시티의 인프라 운영 등 생활과 산업 전반에 활용되고 있다.

가장 빠르게 고도화되는 분야는 자율주행 모빌리티다. 자율주행 차량은 수많은 센서와 ECU를 탑재한 '움직이는 IoT 플랫폼'으로, V2X(Vehicle-to-Everything) 통신을 통해 차량, 인프라, 클라우드 서비스와 실시간으로 연결된다. 이에 따라 IEEE 1609.2 보안 표준[3]과 차량 사이버보안 관리체계를 의무화한 UN R155 규정[4]이 도입되었으며, 차량 원격 공격이 실제로 가능하다는 사실도 입증되었다.

모빌리티 환경에서 사용자는 로보택시 탑승, 공유 차량 대여, 충전소·주차장 이용처럼 여러 사업자의 서비스를 연속해서 이용한다. 사용자에게는 하나의 이동이지만, 시스템 관점에서는 서로 다른 사업자의 IoT 기기에 대한 개별 인증이다. 이러한 환경에서 사용자 인증은 세 가지 문제를 갖는다.

첫째, 인증 반복과 자격증명의 과잉이다. 서비스마다 계정을 따로 쓰면 비밀번호 재사용과 연쇄 유출 위험이 커지며, 입력 인터페이스와 자원이 제한된 IoT 기기에는 강한 인증을 적용하기 어렵다[5].

둘째, 중앙 집중형 SSO의 단일 장애점이다. SAML, OAuth 2.0, OpenID Connect(OIDC) 기반 SSO[6][7][8]는 반복 인증을 줄이지만 모든 신뢰가 중앙 IdP에 집중된다. 상용 SSO의 구현 취약점이 보고되었고[9], 2023년에는 IdP 사업자 Okta의 고객 지원 시스템이 침해되었다[10]. Mirai 봇넷처럼 IoT 기기가 대규모 DDoS 공격에 동원될 수도 있다[11]. IdP가 마비되면 차량 도어 개방이나 충전 개시 같은 물리적 서비스가 모두 중단된다.

셋째, 사용자 추적과 프라이버시 침해다. 중앙 IdP는 사용자의 모든 로그인을 관찰할 수 있고, 서비스 제공자(SP)들이 같은 식별자를 공유하면 로그 결합만으로 이동 경로를 재구성할 수 있다. NIST SP 800-63-3도 이 위험을 지적하며 SP별 가명 사용을 권고한다[12].

본 논문은 이를 해결하기 위해 허가형 블록체인을 신뢰 계층으로 활용하는 PB-SSO(Privacy-preserving Blockchain-based Single Sign-On) 모델을 제안한다. 주요 기여는 다음과 같다.

(1) DID/VC 기반 블록체인 SSO로 중앙 IdP의 단일 장애점을 제거한다.
(2) BBS+ 서명 기반 무작위화 제시 증명과 서비스별 도메인 가명으로 SP 간 사용자 연결을 차단한다.
(3) 원장에는 해시와 폐기 정보만 기록하고, epoch 기반 갱신으로 연결 단서 없이 폐기를 처리한다.
(4) 인증 시 원장 쓰기 없이 엣지에서 검증하여 저지연 인증을 달성한다.
(5) 자율주행 모빌리티 시나리오에 적용하고 실측한 연산 비용으로 성능을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 과련 기술을 분석하고 3장은 제안한 PB-SSO 시스템과 사용자 인증 방안을 기술하고 4장에서 실험 및 분석, 5장에서 결론을 제시한다.

II. Literature Review

2.1 Blockchain

블록체인은 트랜잭션을 블록으로 묶고 각 블록이 이전 블록의 해시를 포함하도록 연결한 분산 원장으로, 과거 기록의 위·변조가 사실상 불가능하다[15]. 퍼블릭 블록체인은 누구나 참여할 수 있으나 PoW·PoS 합의로 확정 지연이 길다. 반면 허가형 블록체인은 인증된 기관만 참여하므로 BFT 계열의 효율적 합의를 쓸 수 있다. Hyperledger Fabric은 실행-정렬-검증 구조로 1초 미만의 확정 지연을 보였으며[13], PBFT는 전체 n개 노드 중 f개($n \geq 3f+1$)의 비잔틴 노드를 허용한다[14]. Christidis와 Devetsikiotis는 스마트 컨트랙트가 IoT 기기 간 신뢰 형성의 기반이 될 수 있음을 제시했다[15]. 본 논문은 즉시 확정성과 저지연이 필요한 IoT 인증 환경에 맞게 허가형 블록체인을 채택한다.

2.2 SSO Technologies and Anonymous Credentials

SSO는 한 번의 인증으로 신뢰 관계에 있는 여러 서비스를 이용하게 하는 방식으로, 사용자, 신원 제공자(IdP), 서비스 제공자(SP)가 참여한다. SAML 2.0은 IdP가 서명한 XML 어서션으로 기업 웹 SSO에 쓰이고[6], OAuth 2.0은 자원 접근 권한을 위임하는 인가 프레임워크이며[7], OIDC는 OAuth 2.0 위에 JWT 형식의 ID 토큰을 더한 인증 계층이다[8]. 이들은 모두 중앙 IdP를 전적으로 신뢰한다는 전제를 가진다. Wang 등은 상용 SSO에서 타인 계정으로 로그인할 수 있는 논리 결함을 다수 발견했으며[9], IdP는 모든 로그인을 중계하므로 이용 이력이 한곳에 축적

www.kci.go.kr

된다[12].

이에 대한 대안으로 사용자가 신원 정보를 직접 소유·관리하는 자기주권 신원(SSI)이 제시되었다. W3C는 분산 식별자(DID)[16]와 검증 가능한 자격증명(VC)[17]을 표준화했다. 다만 일반 디지털 서명으로 발급한 VC는 제시할 때마다 같은 서명값이 노출되어 SP 간 연결 단서가 된다. 이를 막는 익명 자격증명은 CL 서명[18]에서 출발했으며, BBS+ 서명[19]은 서명된 속성 중 일부만 공개하면서 매번 무작위화된 영지식 증명을 만들 수 있어 최근 분산 발급 연구로도 확장되고 있다[20]. 익명 자격증명을 SSO에 적용한 연구로 EL PASSO[21]와 Mir 등의 분산형 프라이버시 보호 SSO[22]가 있으나, 이들은 웹 서비스를 대상으로 하며 IoT 기기 제어나 모빌리티 환경의 엣지 검증은 다루지 않는다.

2.3 IoT Technologies and Security

IoT는 인지 계층(센서·기기), 네트워크 계층(Wi-Fi, BLE, LTE/5G, V2X 등), 응용 계층(서비스 플랫폼)으로 구성된다[1]. 위협은 계층별로 기기 탈취와 펌웨어 변조, 도청·재전송·중간자 공격, 인증 우회와 개인정보 유출로 나타난다[5]. 2016년 Mirai 봇넷은 기본 비밀번호를 쓰는 수십만 대의 기기를 감염시켜 대규모 DDoS를 일으켰다[11]. 차량 분야의 IEEE 1609.2[3]와 UN R155[4]는 주로 차량과 메시지의 인증을 다루므로, 여러 모빌리티 사업자를 이용하는 사용자의 인증과 프라이버시는 별도의 해결이 필요하다.

2.4 Blockchain-based IoT Authentication Research

Dorri 등은 스마트홈에 경량 블록체인을 적용해 기기 간 트랜잭션과 접근 정책을 관리했다[23]. Hammi 등은 이더리움 스마트 컨트랙트로 기기 그룹 단위의 신뢰 영역을 만드는 Bubbles of Trust를 제안했고[24], Ferrag 등은 확장성, 지연, 프라이버시를 블록체인-IoT의 미해결 과제로 꼽았다[25]. Hosseini 등은 블록체인 기반 IoT 분산 식별 프레임워크를 비교하고 자원 제약 기기 지원과 오프라인 동작을 한계로 지적했다[26]. Zhao 등은 zk-SNARK와 머클 트리로 도메인 간 익명 인증과 폐기를 지원하는 기법을 제안했다[27]. 차량 분야에서는 Dorri 등이 오버레이 블록체인 기반 차량 보안 구조를[28], Lu 등이 VANET용 프라이버시 보호형 익명 인증 기법을 제안했다[29]. 국내에서는 김성환과 김영곤이 프라이빗 블록체인을 활용한 분산 클러스터 기반 IoT 경량 인증을[30], 이광형과 정용훈이 분산 ID 기반 출입통제 시스템[31]과 블록체인 전자 ID를 이용한 개인형 이동장치 추적 방안[32]을 제시했다.

2.5 Necessity of the Proposed System

기존 연구는 다음과 같은 한계를 가진다. 첫째, 다수가 기기 간 인증에 초점을 두어 여러 사업자의 서비스를 넘나드는 사용자 SSO 관점이 부족하다[23][24][30]. 둘째, 공개키나 식별자, 고정된 서명값을 그대로 노출하여 원장이나 SP 로그가 추적 수단이 될 수 있다. 셋째, 인증마다 원장 쓰기가 필요하거나 무거운 증명을 쓰는 구조는 지연이 크다. 넷째, 익명 자격증명 기반 SSO[21][22]는 웹 환경에 머물러 IoT 기기 제어와 엣지 검증을 고려하지 않았다. 따라서 분산성, 연결 불가능성, 저지연을 동시에 만족하는 IoT 사용자 SSO 모델이 필요하다. 기존 방식과의 비교는 표 1과 같다.

Table 1. Comparison of conventional and proposed schemes

Item	Centralized SSO (OIDC)	Blockchain IoT auth. [23][24]	Anonymous SSO [21][22]	Proposed PB-SSO
Single point of failure	Yes (IdP)	No	Partly mitigated	No
Target	Web services	IoT device-to-device	Web services	IoT users and devices
Cross-SP unlinkability	No	No	Yes	Yes
Personal data on ledger	N/A	Public keys, identifiers	N/A	Hashes and revocation data only
Edge verification / device control	No	Partial	No	Yes

III. The Proposed PB-SSO System

본 장에서는 위협 모델을 정의한 뒤, 제안하는 PB-SSO (Privacy-preserving Blockchain-based Single Sign-On) 시스템을 시스템 구성도(Fig. 1), 등록·발급·폐기 절차(Fig. 2), 사용자 인증 절차(Fig. 3), 자율주행 모빌리티 적용 시나리오(Fig. 4)를 중심으로 설명한다.

www.kci.go.kr

3.1 Threat Model and Security Requirements

발급자와 원장 컨소시엄은 정직하게 동작한다고 가정한다. SP는 프로토콜은 따르지만 사용자 정보를 수집하려는 정직하지만 호기심 있는(honest-but-curious) 주체이며, 여러 SP가 로그를 공모해 결합할 수 있다. 네트워크 공격자는 Dolev-Yao 모델[33]에 따라 메시지를 도청·변조·재전송할 수 있다. 이에 따라 보안 요구사항을 (R1) 상호 인증과 재전송 방지, (R2) 가장·중간자 공격 방지, (R3) SP 간 연결 불가능성, (R4) 최소 속성 공개, (R5) 단일 장애점 제거로 정의한다.

3.2 System Architecture

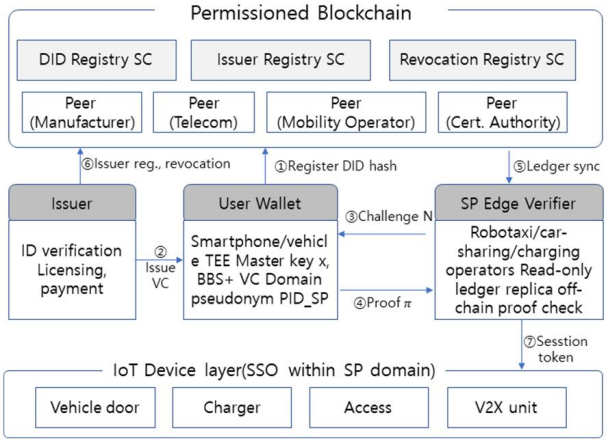


Fig. 1. Architecture of the PB-SSO system

Fig. 1은 제안 시스템의 전체 구성을 나타낸다. 상단의 허가형 블록체인은 제조사, 통신사, 모빌리티 사업자, 인증기관이 Peer로 참여하는 컨소시엄 원장으로, PBFT 계열 합의로 f개($n \geq 3f+1$) 노드 장애까지 견딘다[14]. 원장에는 DID 문서 해시를 기록하는 DID Registry, 발급자 공개키를 기록하는 Issuer Registry, 폐기된 DID 해시와 현재 epoch를 기록하는 Revocation Registry의 세 스마트 컨트랙트가 배치되며, 개인정보는 기록되지 않는다.

중앙의 발급자는 본인확인기관, 면허기관, 결제사처럼 사용자 속성을 보증하는 기관이다. 사용자 지갑은 스마트폰이나 차량의 보안 영역(TEE)에 마스터 비밀키 x와 BBS+ VC를 보관하고 서비스별 도메인 가명을 생성한다. SP 엣지 검증 노드는 로보택시, 카셰어링, 충전소 사업자가 운영하며, 원장의 읽기 전용 복제본을 이용해 제시 증명을 오프체인에서 검증한다.

Fig. 1의 흐름은 다음과 같다. ① 사용자 지갑이 DID 해시를 등록하고, ② 발급자가 VC를 발급한다. ③ SP가 일회성 챌린지 N을 보내면 ④ 지갑이 제시 증명으로 응답하고, SP는 ⑤ 동기화된 원장 복제본으로 이를 검증한다. ⑥ 발급자 등록과 폐기는 원장에 기록되며, ⑦ 검증에 성공하면 SP가 발급한 세션 토큰으로 하단의 차량 도어, 충전기, 출입 게이트 등 IoT 기기가 접근을 허가한다. 원장 쓰기는 ①과 ⑥의 등록·폐기 때만 발생하고 일상적인 로그인(③→④→⑦)은 엣지에서 끝나므로, 합의 지연이 인증에 포함되지 않고 중앙 IdP 없이도 인증이 유지된다.

3.3 Registration, Credential Issuance, and Revocation Procedures

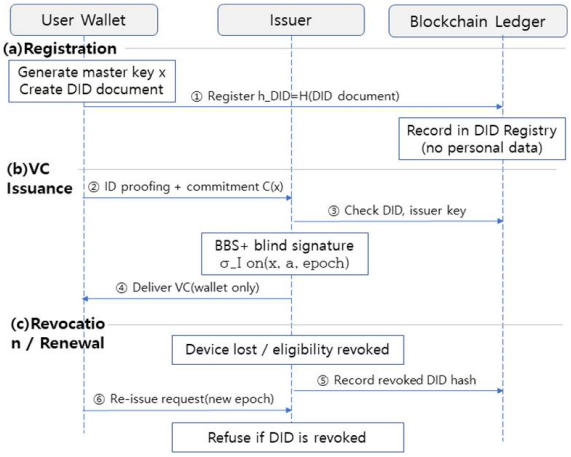


Fig. 2. Procedures for registration, VC issuance, and revocation

Fig. 2는 (a) 등록, (b) VC 발급, (c) 폐기·갱신 절차를 나타내며, 사용하는 표기는 표 2와 같다.

(a) 등록 단계에서 지갑은 x를 생성하고, ① DID 문서의 해시 h_DID만 원장에 등록한다. (b) 발급 단계에서는 ② 사용자가 본인확인과 함께 x에 대한 커밋먼트 C(x)와 그 소유 증명을 보내고, ③ 발급자가 원장에서 DID 해시와 자신의 공개키 등록을 확인한 뒤 x를 알지 못한 채 (x, a, epoch)에 대한 BBS+ 블라인드 서명 σ_I를 생성한다[19]. ④ VC는 원장을 거치지 않고 지갑에만 저장된다(Fig. 2의 점선). (c) 폐기는 VC의 유효 기간을 짧은 epoch(예: 1일)로 제한하는 방식으로 처리한다. 기기 분실이나 자격 상실 시 ⑤ 발급자가 폐기 DID 해시를 기록하면, ⑥ 다음 epoch의 재발급 요청이 거부된다. SP는 제시된 epoch가 현재 값인지만 확인하므로, 같은 epoch의 모든 사용자가 같은 값을 공개하여 폐기 확인이 연결 단서가 되지 않는다. 기기를 분실한 사용자는 사전에 등록한 복구 키로 DID 문서의 키를 교체하고 VC를 다시 발급받는다.

www.kci.go.kr

Table 2. Notations

Symbol	Description
x	User master secret key (never leaves the wallet)
a, epoch	Signed attributes, validity period
σ_I	Issuer BBS+ signature on (x, a, epoch)
B_SP = H_G(ID_SP)	Domain base: SP identifier hashed to a curve point
PID_SP = x·B_SP	Per-SP domain pseudonym
N, H(·)	One-time nonce, hash function

3.4 User Authentication Procedure

Fig. 3은 사용자 지갑, SP 엣지 검증 노드, 로컬 원장 복제본, IoT 기기 간의 인증 절차를 나타낸다.

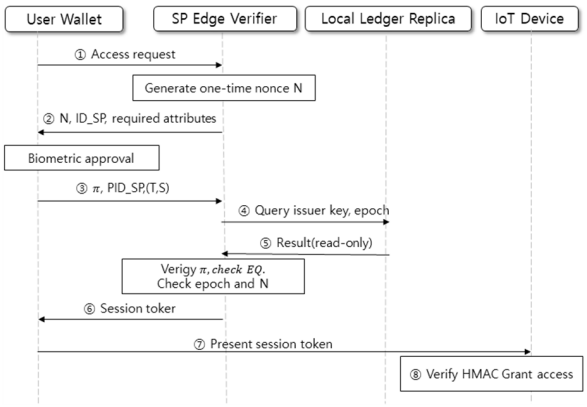


Fig. 3. User authentication procedure

①~② 챌린지: 사용자가 접속을 요청하면 SP는 일회성 챌린지 N, ID_SP, 요구 속성을 보낸다. 사용자가 생체인증으로 승인하면 지갑은 식 (1)로 도메인 가명을 계산하고, 식 (2)로 요구 속성과 epoch만 공개하는 BBS+ 제시 증명 π를 생성한다. 이어 식 (3)으로 가명에 대한 Schnorr 증명을 만든다. 이때 r은 π 안에서 x를 가리는 난수와 같은 값을 사용하여 두 증명이 같은 x에 대한 것임을 연결한다.

$$PID_SP = x \cdot B_SP, \quad B_SP = H_G(ID_SP) \tag{1}$$

$$\pi = BBS+.ProofGen(\sigma_I, \{a_req, epoch\}, N) \tag{2}$$

$$T = r \cdot B_SP,\ c = H(T \parallel PID_SP \parallel \pi \parallel N \parallel ID_SP),\ s = r + c \cdot x \tag{3}$$

③~⑤ 응답과 검증: 지갑은 (π, PID_SP, T, s)를 전송한다. SP는 로컬 원장 복제본에서 발급자 공개키와 현재 epoch를 조회한 뒤(쓰기 없음), (a) π를 BBS+ 검증하고, (b) 식 (4)를 확인하며, (c) epoch가 현재 값인지, (d) N이 재사용되지 않았는지 확인한다.

$$s \cdot B_SP = T + c \cdot PID_SP \tag{4}$$

⑥~⑧ 토큰과 기기 접근: 검증에 성공하면 SP는 단기 세션 토큰 tk = HMAC(K_dev, PID_SP ∥ 권한 ∥ 만료 시각)을 발급한다. K_dev는 기기 등록 시 SP와 IoT 기기가 공유한 키이며, 기기는 HMAC 확인만으로 접근을 허가하므로 자원이 제한된 기기에도 적용할 수 있다. 하나의 토큰으로 SP 영역의 여러 기기를 이용하므로 SP 내부 SSO가, 다른 SP에서도 지갑 승인 한 번으로 ①~⑥이 자동 수행되므로 사업자 간 SSO가 실현된다.

3.5 Application Scenario for Autonomous Mobility

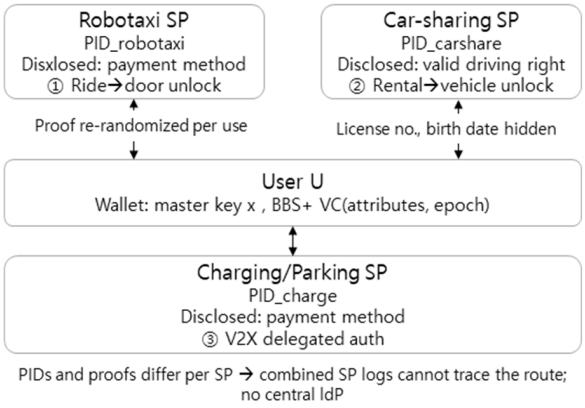


Fig. 4. Application scenario in autonomous mobility environments

Fig. 4는 사용자 U가 세 SP를 차례로 이용하는 시나리오다. ① 로보택시 SP는 '결제 수단 보유' 속성만 요구하며, U는 PID_robotaxi로 인증해 차량 도어를 연다. ② 카셰어링 SP는 '운전 자격 유효' 속성을 요구하며, 면허번호나 생년월일은 공개되지 않는다. ③ 충전소·주차장에서는 차량 내 지갑이 V2X로 대리 인증한다. 이를 위해 U는 자신의 지갑에서 차량 지갑에 범위(충전·주차)와 유효 시간이 제한된 위임 증명을 발급하며, 공유 차량에서는 대여가 끝나면 위임이 자동 만료된다. 세 SP는 서로 다른 PID와 매번 새로 무작위화된 증명만 받으므로 로그를 결합해도 U의 이동 경로를 재구성할 수 없고, 중앙 IdP가 없으므로 전체 이력을 수집하는 주체도 없다.

3.6 Security Analysis

3.1절의 요구사항에 대해 분석하면 다음과 같다. (R1) N이 식 (3)의 c에 포함되므로 이전 세션의 증명을 재사용할 수 없다. (R2) x 없이 식 (4)를 만족하는 (T, s)를 만드는 것은 이산로그 문제의 어려움에 의해 불가능하며, c에 ID_SP

www.kci.go.kr

와 π가 결합되어 있어 증명을 다른 SP로 중계하거나 다른 VC와 바꿔 끼우면 검증에 실패한다. (R3) BBS+ 제시 증명은 매번 무작위화되고, PID는 DDH 가정하에 SP 간 연결할 수 없으며, epoch는 모든 사용자가 공유하는 값이므로 공모한 SP들도 사용자를 연결할 수 없다. (R4) π는 요구 속성과 epoch 외의 정보를 공개하지 않는다. (R5) 검증이 각 SP 엣지에서 분산 수행되고 원장도 f개 노드 장애를 허용하며, 원장 조회가 SP 내부 복제본에서 이루어지므로 원장 운영 노드에도 로그인 기록이 남지 않는다.

IV. Experiment and Analysis

4.1 Experimental Environment and Cryptographic Operation Performance

Intel Xeon 2.80GHz(2 vCPU), Linux 환경에서 인증 과정의 암호 연산을 측정하였다. BBS+ 서명과 제시 증명은 공개 라이브러리 @mattrglobal/bbs-signatures (BLS12-381, Node.js 22)로, 도메인 가명과 Schnorr 증명은 Python 3의 ecdsa 라이브러리(secp256k1 가변 기저점 연산)로, HMAC은 cryptography 46.0.7로 구현하였다.

Table 3. Execution time per cryptographic operation (unit: ms)

Operation	Entity	Mean	Std.dev.
Domain pseudonym, Eq. (1)	User	1.683	0.353
BBS+ presentation proof generation, Eq. (2)	User	15.662	3.022
Pseudonym proof generation, Eq. (3)	User	2.024	0.553
BBS+ presentation proof verification	SP	8.095	1.593
Pseudonym proof verification, Eq. (4)	SP	3.969	0.905
HMAC-SHA256 session token	SP, device	0.003	0.002
(Ref.) BBS+ signature issuance	Issuer	5.732	0.708

속성 5개 중 2개를 공개하는 조건에서 연산별 100~5,000회 반복하여 측정한 결과는 표 3과 같다.

사용자 측 연산 합계는 약 19.37ms, SP 측은 약 12.07ms였으며, 제시 증명의 크기는 479바이트였다. 같은 VC로 생성한 두 증명이 서로 다른 값임을 확인하여 제시 증명의 무작위화도 검증하였다. 두 증명을 하나로 결합해 같은 곡선에서 구현하면 연산이 일부 줄어들 수 있으므로, 표 3의 합계는 보수적인 추정치이다.

4.2 Comparison of Authentication Latency (Simulation Analysis)

엣지 RTT 10ms, 클라우드 RTT 40ms, 로컬 원장 조회 2ms를 가정하였다. OIDC 인가 코드 흐름은 IdP와 약 3회, 제안 방식은 엣지 SP와 2회 왕복한다. 표 3의 측정값을 대입하고, 지갑 단말이 실험 환경보다 k배 느린 경우를 함께 계산한 결과는 표 4와 같다.

Table 4. Comparison of latency per authentication (unit: ms)

Scheme	Network	Computation	Ledger query	Total
OIDC (cloud IdP)	120	≈0.1	-	≈120.1
OIDC (edge IdP, ref.)	30	≈0.1	-	≈30.1
Proposed PB-SSO (k = 1)	20	≈31.4	2	≈53.4
Proposed PB-SSO (k = 4)	20	≈89.6	2	≈111.6

제안 방식은 클라우드 IdP 기반 OIDC보다 약 55% 낮은 지연을 보였고, 지갑 단말이 실험 환경보다 약 4.4배 느린 경우까지 OIDC보다 빠르다. 반면 IdP를 엣지에 배치한 OIDC는 약 30ms로 더 빠르다. 따라서 지연 차이의 근본 원인은 매 인증마다 IdP를 왕복해야 하는 구조에 있으며, 제안 방식의 주된 장점은 지연 자체보다 실시간 서비스에 충분한 지연을 유지하면서 가용성과 프라이버시를 확보한다는 데 있다. 원장 쓰기가 필요한 등록·폐기는 Fabric 수준의 1초 미만 확정 지연을 가정하면 드물게 발생하므로 영향이 제한적이다.

4.3 Availability and Privacy Analysis

표 5와 같이 제안 모델은 가용성과 프라이버시 모두에서 중앙형 SSO보다 우수하다. 다만 표 4는 네트워크 조건을 가정한 모의 분석이며, 블록체인 네트워크의 실제 조회·확정 지연과 동시 접속 처리량은 측정하지 않았다.

또한 epoch 기반 폐기는 폐기가 다음 epoch부터 반영되므로, 즉시 차단이 필요한 경우에는 epoch를 짧게 하거나 누산기 기반 비폐기 증명을 추가해야 한다. 보안성 분석도 서술적 분석에 머물러 있어 형식 검증 도구를 이용한 검증이 필요하다.

www.kci.go.kr

Table 5. Comparison of security and privacy characteristics

Item	Centralized SSO	Proposed PB-SSO
IdP failure	Authentication fails at all SPs	Authentication continues (edge verification)
Cross-SP user linking	Possible (shared identifier, signature)	Not possible (domain pseudonym, randomized proof)
History visible to a central party	Yes	No
Personal data on ledger	N/A	None (hashes and revocation data)

V. Conclusion

본 논문은 여러 사업자의 서비스를 연속해서 이용하는 자율주행 모빌리티 등 IoT 환경에서 중앙형 SSO의 단일 장애점과 사용자 추적 문제를 해결하는 PB-SSO 모델을 제안하였다. 제안 모델은 허가형 블록체인을 신뢰 계층으로 두고, DID와 BBS+ 기반 VC로 신원을 표현하며, 무작위화된 제시 증명과 서비스별 도메인 가명으로 SP 간 연결 불가능성을 확보한다. 원장에는 해시와 폐기 정보만 기록하고, 인증은 원장 쓰기 없이 엣지에서 검증한다.

실험 결과 암호 연산 비용은 사용자 측 약 19.37ms, SP 측 약 12.07ms였고, 엣지 환경의 인증 지연은 약 53ms로 클라우드 IdP 기반 OIDC(약 120ms)보다 낮게 분석되었다. 중앙 IdP 장애 시에도 인증이 유지된다는 점은 IoT 서비스 가용성 측면에서 큰 장점이다.

향후에는 Hyperledger Fabric 기반 프로토타입과 차량 단말을 포함한 테스트베드에서 원장 지연과 처리량을 실측하고, ProVerif 등 형식 검증 도구로 프로토콜의 안전성을 검증하며, 즉시 폐기를 위한 누산기 기법과 양자내성 서명 적용 가능성을 연구하고자 한다.

ACKNOWLEDGEMENT

The Work was supported by Jangan University Research Grant in 2026.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015. doi: 10.1109/COMST.2015.2444095.

[2] IoT Analytics, "State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally," IoT Analytics, 2025.

[3] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," IEEE Std 1609.2-2016, 2016. doi: 10.1109/IEEESTD.2016.7426684.

[4] UNECE, "UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," 2021.

[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015. doi: 10.1016/j.comnet.2014.11.008.

[6] OASIS, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS Standard, 2005.

[7] D. Hardt, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, 2012. doi: 10.17487/RFC6749.

[8] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, "OpenID Connect Core 1.0," OpenID Foundation, 2014.

[9] R. Wang, S. Chen, and X. Wang, "Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services," in Proc. IEEE Symposium on Security and Privacy, 2012, pp. 365–379. doi: 10.1109/SP.2012.30.

[10] The Record by Recorded Future News, "Okta: Hackers stole data on all customer support system users," Nov. 2023.

[11] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017. doi: 10.1109/MC.2017.201.

[12] P. A. Grassi et al., "Digital Identity Guidelines," NIST Special Publication 800-63-3, 2017. doi: 10.6028/NIST.SP.800-63-3.

[13] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. EuroSys, 2018, pp. 1–15. doi: 10.1145/3190508.3190538.

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. OSDI, 1999, pp. 173–186.

[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

www.kci.go.kr

[16] W3C, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022.

[17] W3C, "Verifiable Credentials Data Model v2.0," W3C Recommendation, 2025.

[18] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in Proc. EUROCRYPT 2001, LNCS 2045, pp. 93-118. doi: 10.1007/3-540-44987-6_7.

[19] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in Proc. Security and Cryptography for Networks (SCN 2006), LNCS 4116, 2006, pp. 111-125. doi: 10.1007/11832072_8.

[20] J. Doerner, Y. Kondi, E. Lee, A. Shelat, and L. Tyner, "Threshold BBS+ signatures for distributed anonymous credential issuance," in Proc. IEEE Symposium on Security and Privacy, 2023, pp. 2095-2111. doi: 10.1109/SP46215.2023.10179470.

[21] Z. Zhang, M. Król, A. Sonnino, L. Zhang, and E. Rivière, "EL PASSO: Efficient and lightweight privacy-preserving single sign on," Proceedings on Privacy Enhancing Technologies, vol. 2021, no. 2, pp. 70-87, 2021. doi: 10.2478/popets-2021-0018.

[22] O. Mir, M. Roland, and R. Mayrhofer, "Decentralized, privacy-preserving, single sign-on," Security and Communication Networks, vol. 2022, Article 9983995, pp. 1-18, 2022. doi: 10.1155/2022/9983995.

[23] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE PerCom Workshops, 2017, pp. 618-623. doi: 10.1109/PERCOMW.2017.7917634.

[24] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126-142, 2018. doi: 10.1016/j.cose.2018.06.004.

[25] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188-2204, 2019. doi: 10.1109/JIOT.2018.2882794.

[26] S. M. Hosseini, J. Ferreira, and P. C. Bartolomeu, "Blockchain-based decentralized identification in IoT: An overview of existing frameworks and their limitations," Electronics, vol. 12, no. 6, Article 1283, 2023. doi: 10.3390/electronics12061283.

[27] X. Zhao, F. Xia, H. Xia, Y. Mao, and S. Chen, "A zero-knowledge-proof-based anonymous and revocable scheme for cross-domain authentication," Electronics, vol. 13, no. 14, Article 2730, 2024. doi: 10.3390/electronics13142730.

[28] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, 2017. doi: 10.1109/MCOM.2017.1700879.

[29] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2792-2801, 2019. doi: 10.1109/TVLSI.2019.2929420.

[30] S.-H. Kim and Y.-G. Kim, "A study on light weight authentication method of distributed cluster-based IoT devices," The Journal of The Institute of Internet, Broadcasting and Communication, vol. 19, no. 2, pp. 103-109, 2019. DOI: 10.7236/JIIBC.2019.19.2.103.

[31] K. H. Lee and Y. H. Jung, "Blockchain-based access control and material management system," Journal of the Korea Academia-Industrial cooperation Society, vol. 22, no. 11, pp. 442-448, 2021. DOI: 10.5762/KAIS.2021.22.11.442.

[32] K. H. Lee and Y. H. Jung, "Object tracking using blockchain-based IoT sensor and RFID Active Tag," Journal of the Korea Academia-Industrial cooperation Society, vol. 23, no. 11, pp. 865-871, 2022.

[33] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198-208, 1983. doi: 10.1109/TIT.1983.1056650.

Authors



Eun-Gyeom Jang received the Ph.D. degree in Computer Information Security in 2007. He joined the faculty of the Department of Computer Engineering at Jangan University as a Professor in 2015. His research interests include mobile and system security, and computer forensics.

www.kci.go.kr