논문 2025-3-1 http://dx.doi.org/10.29056/jsav.2025.09.01

개인 데이터 저장 기술의 보안 취약점 분석에 관한 연구

홍두표*, 장성일*, 조용준*, 신동명*†

A Security Vulnerability Assessment of Personal Data Storage Technologies

Du-Pyo Hong*, Sung-Il Jang*, Yong-Joon Joe*, Dong-Myung Shin*†

요 약

디지털 경제와 데이터 주권 규제 변화에서 PDS가 대안으로 부상했지만, 실제 운영 단계에서 보안 취약점과 실증적 검증이 부족하다는 한계가 지적된다. PDS 기술은 (1) 인증·접근제어, (2) 서드파티 앱, (3) 반복·조합 질의로 인한 유출·추론 취약점에 대한 체계적·정량적 검증과 시장·정책 동향의 정합적 반영이 필요하다. 이에 본 논문에서는 조합 증명 기반 접근제어, 정적 분석·권한 재확인, 맥락 기반 질의 모니터링 및 응답 정밀도 제어로 취약 유형별로 차단하는 보안 아키텍처를 제시한다. 제안 기법의 적용 가능성을 시나리오별로 분석하여 위·변조·권한 탈취 시도 차단, 악성 코드 유입 선제 차단, 반복 질의·추론형 공격 조기 탐지의 타당성을 확인했다. 이를 통해 데이터의 무결성, 프라이버시와 사용자 통제권이 강화되고, 전송요구권 등 국내 규제 요구와의 정합성을 충족시키고자 한다. 공공서비스, 보건·교육·미디어 등 다양한 도메인에 적용 가능하며, 표준 API·동의·인증 체계와 연계해 실무 도입의 현실성을 뒷받침한다.

Abstract

Against the backdrop of shifts in the digital economy and data-sovereignty regulation, Personal Data Stores (PDS) have emerged as a viable alternative; however, limitations persist—most notably security vulnerabilities and a lack of empirical validation in operational settings. This work identifies three principal attack surfaces—(1) authentication and access control, (2) third-party applications, and (3) leakage and inference via repetitive/compound queries—and argues for systematic, quantitative evaluation aligned with market and policy developments. We propose a security architecture that counters each vector through composite proof–based access control, static analysis with permission re-confirmation, and context-aware query monitoring with response-precision control. Scenario-based analyses indicate effectiveness in preventing impersonation and privilege-escalation attempts, preempting malicious code ingress, and detecting query-driven inference attacks at an early stage. The approach strengthens data integrity, privacy, and user agency while aligning with domestic regulatory requirements such as data portability and purpose/Scope specification. The architecture is applicable across healthcare, education, and media, and is deployable alongside standardized APIs, and authentication frameworks to support real-world adoption.

한글키워드 : 개인 데이터 저장소, 웹3.0, 솔리드 프로젝트, 보안 취약점, 데이터 주권

keywords : Personal Data Store, Web3.0, Solid project, Security Vulnerability, Data Sovereignty

* 엘에스웨어㈜
† 교신저자: 신동명(email: roland@lsware.co.kr)

접수일자: 2025.09.01. 심사완료: 2025.09.15.
게재확정: 2025.09.20.

1. 서 론

디지털 경제의 성장과 함께 개인 데이터의 수집과 활용이 폭발적으로 증가했다. 소셜 미디어와 사물인터넷(Internet of Things) 장치는 대량의 데이터를 생성하고 중앙 서버에 저장하며, 이러한 중앙집중형 아키텍처에서는 사용자가 자신의 데이터 처리에 대한 통제권을 갖기 어렵다[1,2]. 한편, 현재 서비스 구조는 개인정보 제공 후 사용자가 데이터 이용 목적을 변경하거나 삭제를 요청하기 어려우며, 이는 데이터 주권을 침해한다. 유럽 일반 개인정보보호법(EU General Data Protection Regulation, GDPR)과 같은 규제는 데이터 이동권, 삭제권을 명문화하고 개인의 데이터 주체 권리를 강화했다. 개인 데이터 저장소(Personal Data Store, PDS) 모델은 이러한 배경 속에서 등장한 사용자 중심 데이터 관리 모델로, PDS는 사용자가 데이터 공유 여부와 범위를 결정할 수 있도록 설계되어 중앙집중형 구조 대비 높은 프라이버시를 제공한다[3]. PDS 기술 배경은 소셜 미디어와 IoT의 확산으로 많은 데이터가 중앙 서버에 저장되며 사용자 통제권이 부족하다는 한계점에서 시작되었으며, 개인이 자신의 데이터를 직접 소유하고 관리하며 서비스에 접근 권한을 위임하는 데이터 주권(Data Sovereignty)에 관해 연구가 진행되고 있다. PDS는 데이터 주권과 상호운용성을 강화하지만, 실제 운영에서는 (1) 인증·접근제어, (2) 서드파티 앱, (3) 반복·조합 질의를 통한 유출·추론 등 보안 취약점이 존재한다. 기존 연구에서는 PDS의 개념·구조적 장점에 비해 위와 같은 취약점에 관한 실증적 보안 검증이 부족하다.

본 연구에서는 PDS 기술의 핵심 구성요소와 도메인 적용 사례를 중심으로 PDS 기술과 생태계 동향을 조사하였다. 또한 PDS 운영에 요구되는 이슈를 정리하고, 이를 충족하기 위한 기술의 적용 필요성을 검토하였으며, 규제 환경(e.g., GDPR)을 고려해 PDS의 보안 취약점에 따른 대응 방안을 제시한다. 이를 위해 본 논문의 2장에서는 PDS 기술의 검증하기 위한 기반을 마련하기 위해 PDS 기술 배경과 표준 및 아키텍처 등 배경 지식을 살펴본다. 3장에서는 PDS 기술의 연구 및 생태계 동향을 분석한다. 4장에서는 현재 PDS 기술의 보안 취약점을 분석하고 대응 방안을 제시한다. 5장에서는 본 논문에서 제안한 대응 방안을 평가하고, 6장에서는 결론으로 마무리한다.

2. 배경 지식

본 장은 개인 데이터 저장 기술의 보안 취약점 분석의 근거가 되는 배경 지식을 제공한다. 데이터 이동성을 포함하는 규제 동향을 요약하고, 이어 PDS 구조와 이를 구현하는 표준을 정리한다. 마지막으로 기존 관련 기술과의 차별성을 정리한다.

2.1 데이터 주권 및 규제 동향

현재 국내·외 데이터 주권 및 규제 동향에 관한 내용은 표 1과 같다. 표 1에서 볼 수 있듯이, 데이터 주권 및 규제 환경이 점차 변화하고 있다. 이러한 변화는 개인이 특정 플랫폼에 종속되지 않고 데이터 소유권을 행사하며, 자신의 정보에 관한 접근을 통제할 수 있는 인프라의 도입 및 연구의 배경이 되어가고 있다[4,5,6].

2.2 PDS 아키텍처

PDS 아키텍처는 논리적으로 구분되는 여러 구성요소로 구성되어 있다. 이러한 구성요소는 데이터 저장, 데이터 및 접근 제어 관리, 신원 관리, 프라이버시 선호 관리(인증, 인가), 그리고 개인이 동의 및 알림을 관리할 수 있도록 하는 웹 인터페이스 제공과 같은 핵심 기능을 담당한다. 이러

한 기본 아키텍처 구성요소는 그림 1과 같다. 각 PDS 플랫폼은 다양한 구성요소를 활용한다[1].

PDS의 대표적 구현 모델은 팀 버너스리의 Solid(Social Linked-data) 프로젝트다. Solid는 기존

표 1. 데이터 주권 및 규제 동향
Table 1. Data Sovereignty and Regulatory Trends

구 분	내 용
개인정보 전송요구권[4]	• 2023년 국내 개인정보보호법 전면 개정을 통해 전 산업 분야에 일반적 개인정보 전송요구권을 도입하였고, 2025년 기존 의료·통신 분야에 우선 시행되었던 정보주체 본인 대상 정보전송자(개인정보처리자)와 전송정보의 범위를 전 분야로 확대하는 것으로 개정함
GDPR 및 데이터 이동권[5]	• 데이터 주체의 권리를 명문화하며, 데이터 이동권을 통해 개인이 제공한 데이터를 구조화된 기계 판독 가능 형식으로 다른 서비스에 이전할 수 있도록 규정함. 이는 데이터의 호환성 및 재사용을 촉진하는 것으로, PDS 기술 도입의 기반이 됨
EU 데이터법(Data Act)	• IoT 기기·산업 데이터의 공유를 촉진하고 중소기업의 협상력을 강화하기 위해 사용자에게 데이터 접근 및 공유 권리를 부여하며, 클라우드 서비스 제공자 간 전환 비용을 줄이는 규정을 제안함. 이는 PDS 모델을 활용해 데이터 주체가 생성한 데이터를 다양한 서비스로 이전할 수 있게 함
영국 ICO(Information Commissioner's Office) 가이드	• 데이터 이동권이 개인이 데이터를 안전하게 다른 조직으로 이전하거나 재사용할 권리임을 강조하며, 이는 사용자가 제공한 데이터에 적용되고, 기계 판독 가능한 형식으로 안전하게 전달되어야 함을 명시함

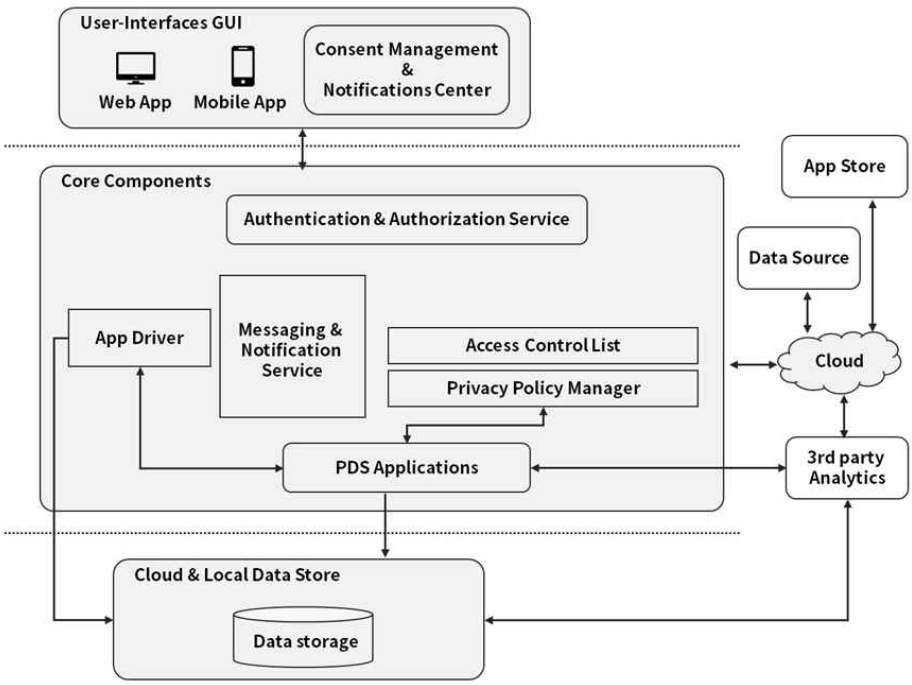


그림 1. PDS 플랫폼의 아키텍처 구성요소
Fig. 1. Architecture Components of PDS Platform

웹을 탈중앙화하여 사용자가 자신의 데이터에 대한 진정한 소유권을 가지도록 하는 것을 목표로 한다. Solid 기반 PDS의 핵심 요소는 Pod라 불리는 개인 데이터 저장 공간이다. Solid 프로젝트에서는 사용자가 다수의 Pod를 만들 수 있으며, 각 Pod는 사용자가 지정한 위치에 존재하고 데이터에 접근할 수 있는 애플리케이션을 사용자가 정의한다[7]. Pod에는 RDF(Resource Description Framework) 또는 JSON-LD(JSON-Linked Data) 포맷의 웹 리소스들이 저장되며, 링크드 데이터(Linked-data) 방식으로 의미를 명시한다. 이러한 구조는 데이터의 물리적 위치와 소유권을 사용자에게 귀속시키는 것을 목표로 한다. Pod는 WebID 및 OpenID Connect 같은 표준을 통해 사용자 인증을 수행하고, 애플리케이션은 필요한 데이터에 대한 권한 요청을 한다. 사용자는 접근 권한을 부여하거나 철회할 수 있으며, 애플리케이션은 승인된 범위 내에서만 데이터를 읽거나 쓸 수 있다. Pod 서버는 데이터에 대한 읽기(Read), 쓰기(Write), 추가(Append), 제어(Control) 권한을 구분하여 관리한다[8].

PDS 아키텍처는 구현 방식에 따라 중앙집중형, 탈중앙형, 혼합형으로 구분된다. 중앙집중형 모델은 신뢰할 수 있는 중앙 서버를 두어 관리 편의성이 높으나 단일 실패 지점에 취약하고, 탈중앙형 모델은 중앙 권한 없이 여러 노드에 분산되지만 데이터 검색과 상호운용성이 어려울 수 있으며, 혼합형 모델은 소수의 신뢰된 기관이 메타데이터를 관리해 두 방식의 장점을 결합한다[5]. 연구자는 사용 사례의 신뢰 모델과 성능 요구에 따라 적절한 아키텍처를 선택해야 한다.

2.3 표준 및 기술 스택

ODRL(Open Digital Rights Language)는 W3C에서 디지털 콘텐츠와 데이터의 사용권과 의무를 표현하는 표준 정책 언어로서, 상업적 거래나 오픈 액세스, 개인정보 규정 등 다양한 시나리오에서 활용될 수 있다. '데이터 주권' 프로파일은 기존 ODRL 모델에 사용 제한·의무를 위한 추가 용어를 정의하며, 이를 실제 시스템에서 적용하기 위해 기술 종속적 언어로 변환할 수 있다.

WAC(Web Access Control)는 분산형 웹 리소스에 대해 ACL(Access Control Policy) 기반으로 읽기, 쓰기, 추가, 제어 권한을 정의하는 메커니즘이며, Pod 서버는 WAC 문서를 통해 리소스의 접근 규칙을 관리한다. ACP는 WAC를 확장한 접근 제어 정책 언어로, 리소스에 대한 권한 부여를 세분화해 다양한 정책을 표현할 수 있다[6,7].

Pod와 애플리케이션 간 인증에는 OpenID Connect, WebID-TLS, GNAP(Grant Negotiation and Authorization Protocol) 등이 사용된다[9]. 또한 자기주권 신원(Self-Sovereign Identity, SSI) 체계를 적용하면 사용자가 중앙 ID 제공자 없이 스스로 신원을 관리할 수 있다. SSI는 W3C 분산식별자(Decentralized Identifier, DID)와 검증 가능한 자격증명(Verifiable Credential)을 기반으로 하며, PDS와 결합할 경우 개인은 데이터와 신원 속성을 모두 제어할 수 있다[10,11].

2.4 데이터 모델 및 메타데이터

PDS는 링크드 데이터(Linked Data) 원칙을 준수하여 RDF나 JSON-LD를 사용한다. 각각의 리소스에는 스키마와 온톨로지로 의미를 부여하고, 메타데이터에 권한 정책(ODRL/ACP 문서), 데이터 출처와 감사 로그를 저장한다. 이는 다양한 애플리케이션이 데이터를 상호운용하고 추적할 수 있도록 한다. 또한 변조 방지를 위해 해시나 블록체인 기반의 무결성 메커니즘을 도입할 수 있다.

2.5 관련 기술 비교

본 절에서는 기존 클라우드 스토리지와 PDS 간 데이터 주체의 권한과 데이터 통제 방식에서

의 차이를 비교한다.

클라우드 스토리지는 사용자가 데이터를 업로드하면 서비스가 저장·처리 권한을 대부분 가진다. 반면 PDS는 데이터 소유권이 개인에게 있으며, 서비스는 필요한 범위와 기간에 한해 접근 권한만 위임받는다. 데이터 클린룸이나 연합 학습 환경도 데이터 프라이버시를 강화하지만, 데이터가 중앙 호스팅 모델 또는 클라우드에 저장된다. PDS는 데이터를 사용자의 저장소에 두고 타 서비스와 표준 인터페이스로 연동하기 때문에 탈중앙화와 프라이버시가 강화된다.

3. 연구 및 생태계 동향

3.1 글로벌 정책 · 표준화 동향

유럽, 미국 등 주요 경제권은 데이터 주권과 상호운용성에 관한 정책을 추진하고 있다. 2023년 제정된 EU 데이터 법은 사용자와 기업 간 데이터 공유를 촉진하며, 기업 간 협력적 데이터 공간을 만들도록 요구한다[5]. 미국도 소비자 개인 정보 보호법(California Consumer Privacy Act, CCPA) 등을 통해 데이터 이동권과 삭제권을 강화하고 있다. 또한, Gaia-X, MyData Global과 같은 국제 컨소시엄이 데이터 공간(Interoperable Data Space)과 PDS 표준화를 주도하고 있다. 한국은 신용정보법(마이데이터)을 통해 분야별 전송요구권을 도입·시행하고, 개인정보보호법(PIPA) 개정을 통해 전 분야 전송요구권을 체계화·확장하고 있다. 이에 따라 표준 API·동의·인증 등 구현 기준이 정비되며, PDS 보안·컴플라이언스 요구와의 접점이 뚜렷해지고 있다.

3.2 오픈소스 및 상용 플랫폼 현황

PDS 기술을 구현한 오픈소스는 Community Solid Server(CSS)와 ESS(Enterprise Solid Server)가 있다. CSS 및 ESS는 Solid 스펙을 구현한 오픈소스 서버로, Pod 호스팅과 ACP/WAC 정책 해석 기능을 제공한다. Digi.me, Dataswift(데이터 박스) 등은 사용자에게 데이터 저장소와 API를 제공하는 상용 PDS 서비스를 운영하며, Inrupt는 기업용 ESS 솔루션과 SDK를 제공한다[12].

공공 도입 사례로는 벨기에 플랑드르 정부는 전 국민(약 650만 명)을 위한 Solid 기반 개인 데이터 금고(Personal Data Vaults)를 구축해 “athumi”라는 데이터 에코시스템을 조성하였다[13]. 시민들은 Pod를 통해 급여 명세, 교육 기록 등을 저장·공유하고, 기관들은 승인된 범위 내에서 해당 데이터를 조회한다. 이는 PDS가 정부 서비스에서 활용될 수 있음을 보여준다.

3.3 적용 분야 · 활용 사례

PDS는 건강 정보, 공공서비스, 교육, 미디어 등 다양한 분야에서 시범 적용되고 있다. 아래 표 2는 PDS 기술 적용 분야 및 활용 사례를 나타낸다[13,14].

3.4 비즈니스 모델

PDS 기술의 비즈니스 모델은 현재 탐색 단계다. 데이터 윤리 연구 단체인 Dataethics.eu의 조사에 따르면 PDS 시장은 초기 단계이며 솔루션들의 성숙도가 다양하다. 일부 기업은 사용자에게 서비스를 무료로 제공하는 대신 데이터 기반 부가가치를 창출하고, 다른 기업은 PDS 플랫폼 이용료를 받는다. Digi.me와 Dataswift와 같이 투자금을 확보한 업체가 상대적으로 성숙한 모델을 보이는 반면, 수익 모델을 데이터 상품 판매에 의존하는 서비스는 프라이버시 침해 우려를 초래할 수 있다. 또한, 유료 모델이 사용자에게 과도한 비용 부담을 줄 수 있다는 지적도 있다.

따라서 투명한 수익 구조와 데이터 사용에 대한 공정한 보상 체계 확립이 필요하다. 또한 공공

표 2. PDS 기술 적용 분야 및 활용 사례
Table 2. PDS Technology Application Areas and Use Cases

사 례	내 용
Flanders 정부	• Solid 기반 PDS를 650만 시민에게 제공해 소득 증명, 교육 기록 등 저장 • 공공서비스에 제출할 때 간편하게 활용할 수 있도록 함
영국 NHS	• 환자가 진료 기록을 관리하는 health PDS 연구 진행 • 건강 데이터 저장과 공유에 대한 신뢰와 프라이버시 제고
Personicle 프로젝트	• 웨어러블 센서와 스마트폰에서 수집한 건강 데이터를 개인 서버에 저장 • 건강 상태 변화를 추적해 개인 맞춤형 헬스케어 서비스 제공
IoT 분야	• 스마트홈 기기 데이터가 제조사 서버가 아닌 PDS 저장 • 사용자가 분석 알고리즘 접근만 허용하는 Compute To Data(C2D) 방식 검토 중
미디어·게임 방송 분야	• 시청 기록 및 구독 데이터 PDS 저장 • 개인화 추천과 저작권 관리에 활용될 수 있음
교육 분야	• 학생 학습 기록 및 성적 PDS 보관 • 취업 또는 학위 신청 시 필요한 정보만 선택적 제공

부문에서는 서비스 비용 절감이나 법적 준수 비용 감소가 동기 부여가 될 수 있다.

3.5 기술 성숙도

시장 분석 보고서는 프라이버시 강화 컴퓨팅 시장이 2025년 6.7억 달러 규모에서 2034년 26.9억 달러로 성장하며, PDS의 시장 규모는 연평균 32.9%의 높은 성장을 보일 것으로 전망한다[15]. 이는 프라이버시 규제 강화 및 사용자의 인식 제고가 PDS 기술 채택을 촉진할 수 있음을 나타낸다.

시장 성숙도 측면에서, 연구자들은 PDS 기술의 성숙도가 초기 단계이며 사회적·법적·기술적 과제가 존재한다고 지적한다. 또한 인증·접근제어, 서드파티 앱 실행, 질의 응답 데이터 노출로부터 위험이 존재한다. 본 논문에서는 이러한 취약점 발생 지점을 분석하고, 그에 따른 대응 방안을 제시한다.

4. 취약점 분석 및 대응 방안

PDS 아키텍처에서는 여러 보안 취약점이 존재하며, 이는 사용자 개인정보의 기밀성과 무결성, 프라이버시를 위협한다. 아래에서는 PDS 아키텍처에서 나타날 수 있는 대표적인 보안 취약점을 세 가지로 정리하고, 각 취약점에 대해 1) 취약점 발생 지점, 2) 이론적 대응 방안을 제시한다.

4.1 인증 및 접근제어 취약점

1) 취약점 발생 지점 : PDS는 여러 애플리케이션과 사용자들이 접속하기 때문에 아래와 같은 단계에서 취약점이 발생할 수 있다.

- 인증 단계 : 공격자가 취약한 프로토콜 설정을 악용하여 세션 토큰이나 인증 코드를 탈취하여 사용자로 가장하여 PDS에 접근할 수 있음[16]
- 인가·접근제어 단계 : PDS 구조에서는 일반적으로 사용자 식별 후 ACL이나 정책에 따라 데이터 접근을 허용하는데, 사용자 신원만 확인, 애플리케이션 신뢰도를 검증하지 않았다면, 사용자 권한을 탈취할 수 있음

2) 대응 방안 : PDS 인증 및 접근제어를 위해 요청과 관련된 정보들을 조합하여 허가된 증

명만 접근하도록 한다.

- 조합 증명 : PDS 질의 요청을 위한 인증 시 로그인만 성공하는 것이 아니라 사용자, 질의 요청 애플리케이션, 질의 대상 리소스, 질의 목적을 조합하여 제출한 증명을 검증하여 허가된 증명만 접근하도록 함

4.2 신뢰할 수 없는 서드파티 애플리케이션에 따른 취약점

1) 취약점 발생 지점 : 사용자 PDS 내부에 서드파티 애플리케이션의 질의 모듈은 API 호출 또는 플러그인 형태로 PDS 데이터베이스에 질의하고 결과를 외부로 반환한다. 이때 PDS와 서드파티 애플리케이션이 상호작용하는 과정에서 악의적인 데이터 유출이 발생할 수 있다. 이러한 취약점은 다음과 같은 상황에서 발생할 수 있다.

- 애플리케이션 모듈 연동 단계 : PDS 내부에서 정상적으로 동작하던 모듈이 PDS와 연동 후 악성 업데이트를 통해 악의적인 코드를 실행하게 될 수 있음
- 애플리케이션 모듈 실행 단계 : PDS 내부에서 애플리케이션 모듈이 PDS 데이터베이스 질의 결과를 출력할 때, 결과를 암호화하여 외부 채널로 보내거나 로컬 기기에 복제하여 사용자 제어 범위를 벗어나면, 데이터가 유출될 위험이 있음

2) 대응 방안 : 다층적인 애플리케이션 격리 및 검증 체계를 구축하여 PDS 내부에 들어오는 외부 코드에 대한 신뢰성을 확보하고, 악성 애플리케이션에 따른 취약점을 선제적으로 대응한다.

- 정적 분석 및 서명 검증 : PDS 내부에 애플리케이션 모듈을 설치하기 전에 코드 서명을 요구하고, 모듈 코드에 대한 정적 분석을 수행하여 허용되지 않은 API 호출이나 정보 유출 의도를 탐지함
- 권한 감시 및 민감정보 재확인 : 사용자가 앱 설치 시 어떤 권한을 부여하는지 UI에 알림을 제공하고, 민감정보에는 태그 기반 추적 기법을 도입하여 민감정보에 접근하는 요청은 그때마다 재확인(Consent) 받도록 설계함

4.3 데이터 유출 및 추론 공격 취약점

1) 취약점 발생 지점 : 개인정보 보호를 위해 PDS가 가공된 질의 결과를 출력하더라도 반복 질의 또는 데이터 조합을 통해 민감정보가 추론되어 유출되는 추론 공격이나 재식별 공격의 위험이 발생할 수 있다.

- 공격적 질의 설계 단계 : 공격자는 PDS가 허용하는 쿼리 또는 함수 내에서 최대한 특정한 조건을 넣어 사용자의 민감 특성을 확인할 수 있음
- 다중 질의 수행 단계 : 한 번의 질의로는 확실하지 않던 정보를 수차례의 질의 결과를 교차 분석하여 좁혀나가는 binary search 방식임. 이때 PDS는 각 질문에 개별적으로 허용된다고 판단하여 결과를 반환하지만, 결과적으로 사용자의 상세한 행태가 드러날 수 있는 상황이 발생함
- 추론 결과 통합 단계 : 공격자가 모든 질의응답과 정보를 취합해 사용자의 숨겨진 속성(e.g., PDS 저장 데이터가 사용자의 온라인 결제 기록, 진료 결제 내역 등을 저장하는 경우 소비 패턴, 질병 여부와 같은 민감정보)을 추론하는 등 장기적인 면에서 정보가 누적 공개되어 민감 패턴이 드러날 위험이 있음

2) 대응 방안 : PDS가 요청받는 질의를 검사하는 모듈을 구축하여 일련의 질의를 분석 및 탐지하여 취약점에 대응한다.

- 질의 제어 및 모니터링 : PDS는 요청받는 질의들을 맥락 기반으로 모니터링하여 동일 사용자가 유사한 데이터를 반복적으로 조회

하면 경고 신호를 인식함. 일정 기간 내 연관된 속성에 대한 다수의 질의가 들어오면 이를 동일한 그룹의 질의 요청 시도로 판단하여 추가 인증을 요구할 수 있음

- 사용자 대시보드 제공 : 누가, 언제 어떤 데이터에 접근했는지와 같은 접근 기록을 사용자가 쉽게 볼 수 있도록 대시보드를 제공하면, 이상 패턴을 사용자가 직접 발견하고 해당 앱의 권한을 취소할 수 있음

5. 대응 방안 평가

5.1 인증 및 접근제어 평가

질의 요청과 관련된 정보들을 기반으로 증명 검증을 기반으로 접근을 제어함으로써, 사용자 신원 위·변조 및 권한 탈취 시도를 차단할 수 있는 대응 방안을 제시하였다. 이를 통해 단순 사용자 인증에서 벗어나 애플리케이션 신뢰도까지 검증하는 체계를 확립하여 사용자 및 서비스 제공자에게 데이터 무결성 보장을 달성한다. 또한 국내 전송요구권 절차에서 요구되는 주체, 목적, 범위 특정을 충족하며 표준 API, OAuth 범위 설계에 대응한다.

5.2 서드파티 애플리케이션 위협 대응 평가

정적 분석 및 코드 서명 검증 절차를 통해 악성 코드 삽입·업데이트 위협을 사전에 차단하는 대응 방안을 제시하였다. 애플리케이션 권한 요청을 사용자에게 투명하게 알리고, 민감정보 접근 시 재동의 요청을 보냄으로써 사용자 주도적 프라이버시 통제권을 강화한다.

5.3 데이터 유출 및 추론 공격 대응 평가

맥락 기반 질의 모니터링을 통해 반복 질의·추론형 공격을 조기 탐지 및 차단하는 대응 방안을 제시하였다. 사용자 대시보드를 통해 접근 내역을 제공하여 이상 징후를 사용자가 직접 확인 및 제어가 가능하다. 결과적으로 반복적이거나 의도적인 세밀한 질의를 조기에 탐지하고, 결과값의 정밀도를 제어하는 방식은 데이터를 목적 외로 활용하는 시도를 줄이고 재식별 위험을 예방하는 역할을 한다. 결과적으로 사용자가 의도하지 않은 방식으로 정보가 조합되어 드러나는 것을 차단하여, 국내 규제에서 강조하는 목적 외 이용 억제와 재식별 방지 요구에 대응한다.

6. 결 론

본 논문은 개인 데이터 저장소(PDS) 기술의 등장 배경과 아키텍처, 표준 및 생태계 동향을 분석하고, PDS 운영 과정에서 발생할 수 있는 보안 취약점을 식별하여 대응 방안을 제시하였다. 특히 인증 및 접근제어, 서드파티 애플리케이션, 데이터 유출 및 추론 공격이라는 세 가지 대표적 취약점에 대해 위협 발생 지점을 정리하고, 다차원 증명 검증, 코드 서명·정적 분석·격리 실행, 질의 모니터링과 사용자 대시보드 제공 등 구체적 대응 전략을 도출하였다. 향후 연구는 PDS의 보안 취약점에 대응 전략을 도입하여, 보다 높은 안정성·신뢰성을 갖춘 Web 3.0 환경 기반 온라인 거래 플랫폼, 전자계약 등 실제 서비스에 적용하는 방안에 관해 연구하고, 이에 따른 PDS 보안 모델의 확장성과 사용성 간 균형, 프라이버시 강화 기술 적용 및 검증 연구 등이 필요하다.

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2025년도 신기술 융합 저작권 기술개발 사업으로 수행되었음(과제명 : Web3.0 탈중앙화 환경에서 창작자간의 저작권 이용허락 거래 자동화 기술 개발, 과제번호 : RS-2024-00441360, 기여율 : 100%)

참 고 문 헌

[1] Khalid, A., Khan, F., Ahmad, H., Ahmad, S., Almogren, A. Personal Data Stores (PDS): A Review. Sensors, 23(3), 1477, 2023, https://doi.org/10.3390/s23031477

[2] Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., Boneh, D. A Critical Look at Decentralized Personal Data Architectures. arXiv preprint, 2012. https://arxiv.org/abs/1202.4503

[3] D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., Bourka, A. Privacy by Design in Big Data: An Overview of Privacy-Enhancing Technologies in the Era of Big Data Analytics. arXiv preprint. 2015. https://arxiv.org/abs/1512.06000

[4] Personal Information Protection Commission (PIPC), "Notification on the Designation of Personal Information Management Institutions and Procedures for Data Portability," 2025, National Law Information Center, https://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000255726

[5] European Commission. Decentralized Data Processing: Personal Data Stores and the GDPR. International Data Privacy Law, 10(4), 356 - 370. 2021. https://doi.org/10.1093/idpl/ipaa021

[6] Gurses, S., Del Alamo, J. M. Privacy Engineering: Shaping an Emerging Field of Research and Practice. IEEE Security & Privacy, 14(2), 40 - 46. 2016. https://doi.org/10.1109/MSP.2016.44

[7] Zichichi, M., Ferretti, S., D'Angelo, G. On the Efficiency of Decentralized File Storage for Personal Information Management Systems. arXiv preprint. 2020. https://arxiv.org/abs/2007.03505

[8] Marillonnet, P., Laurent, M., Ates, M. Personal Information Self-Management: A Survey of Technologies Supporting Administrative Services. arXiv preprint. 2021. https://arxiv.org/abs/2109.12968

[9] Khalid, A., Khan, F., Ahmad, H., Ahmad, S., Almogren, A. A Systematic Review on Privacy-Aware IoT Personal Data Stores. Sensors, 24(7), 2197. 2025. https://doi.org/10.3390/s24072197

[10] Perentis, C., Vescovi, M., Leonardi, C., Moiso, C., Musolesi, M., Pianesi, F., Lepri, B. Anonymous or Not? Understanding the Factors Affecting Personal Mobile Data Disclosure. arXiv preprint. 2017. https://arxiv.org/abs/1701.08308

[11] Cavoukian, A. Privacy by Design: The Definitive Workshop. Identity in the Information Society, 3(2), 247 - 251. 2010. https://doi.org/10.1007/s12394-010-0062-y

[12] De Montjoye, Y. A., Shmueli, E., Wang, S. S., Pentland, A. openPDS: Protecting the Privacy of Metadata Through SafeAnswers. PLoS ONE, 9(7), e98790. 2014. https://doi.org/10.1371/journal.pone.0098790

[13] Kim, H., Lee, D. Architecture and Security Features of Personal Data Stores for Privacy Protection. Journal of KIISE, 48(6), 563 - 575. 2021. https://doi.org/10.5626/JOK.2021.48.6.563

[14] Park, J., Kim, S. MyData Personal Data Store Model (PDS) to Enhance Information Security for Guarantee of Data Portability. Journal of Information Security and Applications, 63, 103040. 2022.https://doi.org/10.1016/j.jisa.2021.103040

[15] Shivani Zoting, "Privacy-enhancing Computation Market Driving the Future of Secure Data Innovation", 2025, Precedence RESEARCH, https://www.precedenceresearch.com/privacy-enhancing-computation-market

[16] Esposito, C., Horne, R., Robaldo, L., Buelens, B., Goesaert, E. Assessing the Solid Protocol in Relation to Security and Privacy Obligations. Information, 14(7), 411. 2023. https://doi.org/10.3390/info14070411

저 자 소 개

홍두표(Du-Pyo Hong)

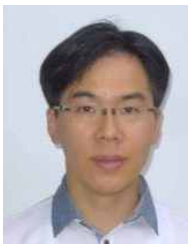
2024.2 숭실대학교 컴퓨터학과 석사
2024.1-현재 : 엘에스웨어㈜ 주임연구원
<주관심분야> 빅데이터, 분산 컴퓨팅, 블록체인

장성일(Sung-Il Jang)

2019.8 숭실대학교 컴퓨터학과 석사
2021.8 숭실대학교 소프트웨어학과 박사수료
2021.9-현재 : 엘에스웨어㈜ 수석연구원
<주관심분야> 시스템 프로그래밍, 분산 컴퓨팅, 블록체인

조용준(YongJoon Joe)

2011.03 큐슈대학교 전기정보공학과 학사
2013.03 큐슈대학교 정보학부 석사
2016.03 큐슈대학교 정보학부 박사 수료
2013.04-2016.03 일본 학술진흥원 특별연구원
2016.04-현재 : 엘에스웨어㈜ 소프트웨어연구소
연구개발본부 기술이사
<주관심분야> 오픈소스, 저작권, 병렬·분산 컴퓨팅, 게임이론, 분산 제약 최적화 문제



신동명(Dong-Myung Shin)

2003.08 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원(KISA)
응용기술팀 선임연구원
2006-2014 한국저작권위원회
저작권기술팀 팀장
2014-2016 한국스마트그리드사업단
보안인증팀 팀장
2016-현재 : 엘에스웨어㈜ 소프트웨어연구소
연구개발본부 연구소장/전무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크 보안, SW 취약점 분석·감정, 블록체인 기술