

2020

한국정보보호학회 하계학술대회

CISC- S'20

Conference on Information Security
and Cryptography - Summer 2020

07.15^{WED}

온라인 컨퍼런스

<http://www.cisc.or.kr/>

주최
주관



후원



Blockchain-empowered for Secure Data Storage and Sharing in Vehicular Edge Computing Networks	Muhammad Firdaus · Kyung-HyuneRhee / 197
허가형 블록체인을 활용한 자기 주권형 신원의 디지털 공공·민간서비스 플랫폼 융합 방안	조강우 · 정병규 · 신상욱 201

블록체인 2

무결성을 보장하며 보상체계를 갖는 블록체인 기반 커뮤니티 정보교류 Web 환경	윤혜원 · 김원희 · 김다영 · 노혜윤 · 김형종 / 207
블록체인 네트워크 한계 보완을 위한 사이드체인 동향	심민주 · 최승주 · 서화정 / 211
Secure Localized Training in Collaborative Learning Schemes	Sandi Rahmadika · Kyung-Hyune Rhee / 214
블록체인에서 랜덤 비콘 프로토콜을 이용한 PRNG 비교 분석	정병규 · 조강우 · 신상욱 / 218
사물 인터넷 환경에서 수정 가능한 블록체인 기반 접근제어 시스템 설계	임준호 · 천지영 · 노건태 · 정익래 / 222
IoT 환경에서의 블록체인 활용에 대한 연구	김대영 · 이덕규 / 226

어플리케이션보안

암표방지를 위한 모바일 티켓팅 시스템에 관한 연구	송윤민 · 황용운 · 이임영 / 233
하이퍼레저 패브릭 기반 장학금 통합 관리 시스템 개발	김은별 · 송경린 · 최찬미 · 최윤영 · 채기준 / 237
회전에 강한 특징을 이용한 돌로네 기반 대체 가능 지문 템플릿 연구	이민섭 · 이상훈 · 정익래 / 241
암호화 API 오용 탐지에 관한 연구 동향 조사	이민욱 · 조금환 · 김형식 / 245
Zero-Knowledge Proof 기반의 마이데이터 서비스 제공 방안	이민경 · 최슬기 · 곽진 / 249

산업보안

IEC 62443-4-2 기반 HVDC 및 ESS 보안 적용 방안	박원경 / 255
안전한 원격 근무를 위한 그룹키 기반 프로토콜 제안	김의진 · 김득훈 · 곽진 / 259
몬테카를로 시뮬레이션을 통한 기업의 위험표현 및 사이버보험 효과도 분석 연구	김민수 · 김예주 · 왕성진 · 김형종 / 263

해킹 및 방어기술

안드로이드 UI 은닉을 통한 소프트웨어 기반 카메라 프레임 탈취 기법	한수민 · 심현석 · 박정수 · 정수환 / 269
키보드 입력 감지 트리거 구현 및 분석	박연균 · 윤종희 / 273
Python Pickle 모듈을 통한 셸코드 Exploitation과 Mitigation 연구	윤창조 · 김경곤 / 275
N-gram 알고리즘을 이용한 Spectre 공격 바이너리 정적 식별 방법	김문선 · 양희동 · 김광준 · 이만희 / 279
Federated Learning에서 개선된 백도어 공격 방법	임규민 · 김창진 · 서재홍 / 283
안티바이러스의 자가 보호 기법 분석	이성원 · 윤종희 / 287

Zero-Knowledge Proof 기반의 마이데이터 서비스 제공 방안

이민경¹, 최슬기², 곽진³

^{1,3}아주대학교 사이버보안학과

²아주대학교 정보통신연구소

Zero-Knowledge Proof-based My Data Service Providing Method

Minkyung Lee¹, Seul-Ki Choi², Jin Kwak³

^{1,3}Department of Cyber Security, Ajou University

²Institute for Information and Communication, Ajou University

요 약

최근 빅데이터 시대에 들어서면서, 정보 주체가 자신의 정보에 대한 결정권을 갖고 정보를 스스로 활용할 수 있는 마이데이터가 등장하였다. 이에 따라, 개인이 데이터 활용을 개방에 대한 요청에 따라 금융정보나 의료 정보 등을 수집하여 통합조회, 비교, 추천 서비스 등 다양한 서비스에 활용할 수 있는 마이데이터 서비스가 등장하고 있다. 하지만, 최근 마이데이터 서비스가 다양해짐에 따라, 데이터 제공자의 수가 지속해서 증가하고 있다. 따라서, 데이터 제공자마다 인증관리가 필요로 하다. 또한, 다양한 마이데이터 서비스가 등장하면서, 마이데이터 서비스 제공자의 신뢰 문제가 발생하고 있다. 따라서, 본 논문에서는 마이데이터 서비스 제공자에게 인증정보와 같은 비밀정보를 누출하지 않으면서 서비스를 제공할 수 있는 영지식 증명을 활용한 마이데이터 서비스를 제공하는 방안을 제안한다.

I. 서론

4차 산업혁명에서 데이터의 중요성이 부각됨에 따라 정보 주체인 개인이 소외되는 정보보호 문제가 대두되고 있다. 따라서 개인이 자신의 정보를 관리 및 통제하기가 어려워지면서, 개인이 자신의 정보에 대한 결정권을 갖고 정보를 활용할 수 있는 마이데이터의 개념이 등장하였다. 마이데이터를 활용하여 정보 주체의 데이터 관리 및 활용을 지원할 수 있으며 동시에 소비패턴의 분석 등에 활용할 수 있다. 따라서, 분산되어있는 개인의 정보를 통합하고 분석함으로써, 사용자는 통합된 하나의 서비스만을 이용하여 다양한 정보를 활용할 수 있다[1,2,3]. 이에 따라, 마이데이터를 활용하고 제공하는

서비스가 증가할 것으로 예상된다. 하지만, 사용자는 데이터를 제공하는 기관마다 개별적인 인증이 필요로 하며, 이는 다양한 기관의 데이터 활용 시 인증 횟수가 증가할 것으로 예상된다. 또한, 마이데이터 서비스를 제공하는 다양한 업체가 생겨남에 따라, 마이데이터 서비스 제공 업체에 대한 신뢰성 문제가 생겨나고 있다[2].

따라서, 본 논문에서는 사용자가 데이터를 제공하는 각 데이터 제공자마다 개별 인증을 수행하지 않도록 마이데이터 서비스 등록단계와 마이데이터 서비스 제공자에게 비밀정보를 누출하지 않도록 Zero-Knowledge Proof를 활용하여 마이데이터 서비스를 제공할 수 있는 마이데이터 서비스 인증단계를 제안한다.

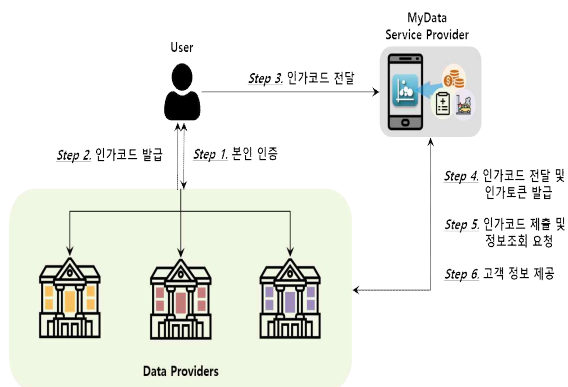
이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

II. 관련 연구

2.1 마이데이터

마이데이터는 정보 주체인 개인이 ‘정보 이동권(Right to Data Portability)’에 근거하여 본인 데이터에 대한 개방을 요청하면, 기업이 보유한 데이터를 개인 또는 개인이 지정한 제3자에게 개방하도록 하는 것이다. 마이데이터 서비스는 개방된 개인의 정보를 활용할 수 있도록 제공하는 서비스로, 본인 신용정보의 체계적 관리를 지원함과 동시에 소비패턴 등의 분석을 통해 개인의 신용관리 및 자산관리 서비스 등을 제공할 수 있다. 주요 서비스로 신용정보 통합조회, 재무 및 신용관리 지원, 금융상품 비교 및 추천 서비스 등이 있으며 최근에는 금융과 관련된 정보 이외에 직장정보나 건강정보 등 개인과 관련된 다양한 정보를 활용한 서비스를 제공하고 있다[1,2,3].

기존 마이데이터 서비스의 제공 방식은 다음 (Fig. 1)과 같다[2]. 사용자(User)는 정보 주체로 능동적으로 자기 결정권을 행사하는 주체이며, 데이터 제공자(Data Providers)는 사용자의 정보를 보유하고 있는 업체로, 은행 등의 금융기관이 될 수 있다. 마이데이터 서비스 제공자(MyData Service Provider)는 여러 금융정보의 데이터를 활용하여 서비스를 제공할 수 있도록 하는 서비스 제공자이다.



(Fig. 1) MyData Service

Step 1. 본인인증

사용자는 정보 제공을 원하는 각 데이터 제공자마다 인증을 수행한다.

Step 2. 인가코드 발급

본인인증 결과에 따라 각 데이터 제공자는

인증코드를 발급하여 사용자에게 전달한다.

Step 3. 인가코드 전달

사용자는 기관으로부터 전달받은 인가코드를 마이데이터 서비스 제공자에게 전달한다.

Step 4. 인가코드 전달 및 인가토큰 발급

마이데이터 서비스 제공자는 사용자로부터 전달받은 인가코드를 데이터 제공자에게 전달한다. 이후, 데이터 제공자는 기존에 발급한 인가코드와 비교하여 해당 인가코드가 유효한지 검증한 후, 인가토큰을 전달한다.

Step 5. 인가토큰 제출 및 정보조회 요청

마이데이터 서비스 제공자는 정보조회 요청을 바탕으로 데이터 제공자로부터 전달받은 인가토큰을 제출한다.

Step 6. 고객 정보 제공

데이터 제공자는 마이데이터 서비스 제공자에게 전달받은 인가토큰의 유효성을 검증한 후, 사용자에 대한 정보를 마이데이터 서비스에게 제공한다.

2.2. Zero-Knowledge Proof

Zero-Knowledge Proof는 증명자가 검증자에게 어떤 문장(Statement)이 참이라는 것을 증명할 때, 그 문장의 참/거짓 여부를 제외한 다른 어떠한 정보도 노출되지 않는 상호 절차를 의미한다[4]. Zero-Knowledge Proof에 참여하는 당사자들이 상대방을 속이려는 목적으로 프로토콜을 임의로 변경하는 경우, 당사자들이 부정직하다 또는 정직하지 않다고 한다. 그 외의 경우에는, 정직하다고 한다.

III. 제안 사항

3.1 고려 사항

본 제안 사항에서는 아래와 같이 TTP와 Zero-Knowledge Proof를 활용하여 개별 인증과 마이데이터 서비스 제공자의 신뢰 문제를 고려하였다.

□ TTP(Trusted Third Party)

마이데이터 서비스 등록단계에서 사용자와 데이터 제공자들 사이의 인가코드를 통합하여 배분해주는 TTP를 이용함으로써, 사용자는 각

데이터 제공자마다 개별 인증을 수행하지 않아도 된다.

□ Zero-Knowledge Proof

마이데이터 서비스 인증단계에서 TTP로부터 전달받은 인가코드를 증명하는 과정에서 Zero-Knowledge Proof를 이용하여 인가코드의 노출 없이 증명할 수 있다. 이에 따라, 마이데이터 서비스 제공자가 인가코드를 악의적으로 유출하거나 변조하였음을 검증하지 않아도 된다.

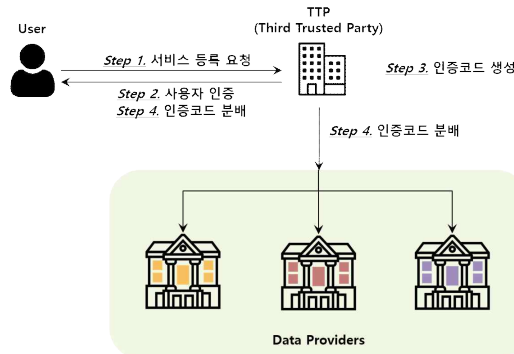
3.2 표기법

본 제안 사항에서 사용하는 Parameter에 대한 표기법은 아래 <Table 1>과 같다.

<Table 1> Notation

Parameter	Description
$code_{Auth}$	The authorized code from TTP
N_x	The random number from x
S_i	The statement of i
p	prime number
g	integer number from 1 to p-1

3.3 마이데이터 서비스 등록단계



(Fig. 2) Registration Process

Step 1. 서비스 등록 요청

사용자는 TTP에게 서비스 등록 요청을 수행하며, 사용자는 데이터 제공을 원하는 데이터 제공자를 선정하여 TTP에게 전달한다.

Step 2. 사용자 인증

TTP는 사용자를 인증하여 검증을 수행한다.

Step 3. 인증코드 생성

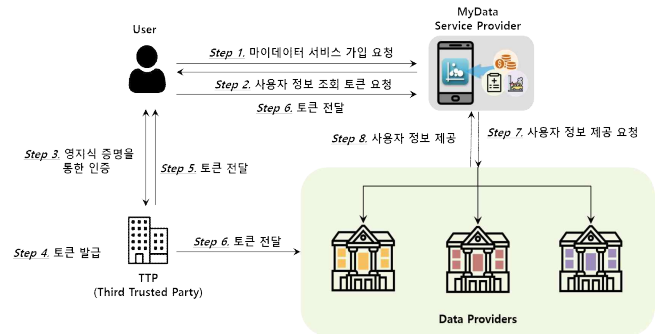
TTP는 검증이 완료되면, 사용자의 요청을 바탕으로 각 기관과 사용자에게 대응되는

$code_{Auth}$ 을 생성한다.

Step 4. 인증코드 분배

생성한 $code_{Auth}$ 을 사용자로부터 요청 받은 기관들과 사용자에게 분배한다.

3.4 마이데이터 서비스 인증단계



(Fig. 3) Verification Process

Step 1. 마이데이터 서비스 가입 요청

사용자는 마이데이터 서비스 제공자에게 가입을 요청한다.

Step 2. 사용자 정보 조회 토큰 요청

마이데이터 서비스 제공자는 데이터 제공자에게 정보를 조회하기 위한 토큰을 사용자로부터 요청한다.

Step 3. 영지식 증명을 통한 사용자 인증

사용자는 사용자 정보를 요청하기 위한 토큰을 발급하기 위해 TTP에게 토큰 발급 요청을 수행한다. 이 때, TTP는 토큰 발급을 요청하는 사용자의 인증을 수행한다. 인증과정은 아래와 같다. 이후, 사용자는 아래 수식에 따른 값을 생성한다.

① N_{user} 생성

② $S_{code_{Auth}} = g^{code_{Auth}} \bmod p$ 생성

③ $S_{N_{user}} = g^{N_{user}} \bmod p$ 생성

④ $(code_{Auth} + N_{user}) \bmod (p-1)$ 생성

TTP는 사용자가 인증코드($code_{Auth}$)를 소유하고 있는지 검증하기 위하여 $[0, 1]$ 중 랜덤하게 선택하여 사용자에게 전달한다. 사용자는 TTP로부터 전달받는 랜덤 값에 따라 아래 수식을 만족하는 값을 생성하여 TTP에게 전달한다. 이때, 전달받은 랜덤 값이 0이면 ①을 시행하고 1이면 ②를 시행한다.

① N_{user} 전달

② $(code_{Auth} + N_{user}) \bmod (p-1)$ 전달

TTP는 전달한 랜덤 값에 따라 전달받은 증명 값을 검증한다. 검증식은 다음과 같으며, 전달받은 랜덤 값이 0이면 ①을 시행하고 1이면 ②를 시행한다.

$$① S_{N_{user}} = g^{N_{user}} \bmod p$$

$$② S_{code_{Auth}} \times S_{N_{user}} = g^{(code_{Auth} + N_{user}) \bmod (p-1)} \bmod p$$

만약, 검증식이 성립하지 않으면 사용자가 아니라고 판단하여 종료하며 그렇지 않으면 인증과정을 반복한다.

Step 4. 토큰 발급

사용자와의 인증이 완료되면, TTP는 사용자의 정보조회가 가능한 토큰을 발급한다.

Step 5. 토큰 전달

TTP는 발급된 토큰을 사용자와 데이터 제공자에게 전달한다.

Step 6. 토큰 전달

사용자는 TTP로부터 전달받은 토큰을 마이데이터 서비스 제공자에게 전달한다.

Step 7. 사용자 정보 제공 요청

마이데이터 서비스 제공자는 사용자로부터 전달받은 토큰을 통해 데이터 제공자에게 정보를 요청한다.

Step 8. 사용자 정보 제공

데이터 제공자는 TTP로부터 전달받은 토큰과의 일치여부를 통해 마이데이터 서비스 제공자에게 사용자 정보를 제공한다.

IV. 안전성 분석

4.1 사용자 인증정보 노출방지

본 제안 사항에서는 Zero-Knowledge Proof를 이용하여 사용자의 인증정보인 인가코드 노출 없이 증명 값을 통해 인가코드의 소유 여부를 확인하였다. 따라서, 마이데이터 서비스 제공자는 이산대수 문제의 어려움에 따라 인가코드를 확인할 수 없다. 이를 통해, 마이데이터 서비스 제공자가 인가코드를 악의적으로 유출하여 이용할 수 없으며, 인가코드를 변조하거나 이용함으로써 허가되지 않은 데이터의 열람이 불가능하다.

4.2 사용자 위장 공격 방지

공격자는 증명 값 전달 과정에서 인가코드를 소유하고 있음을 위장할 수 있다. 하지만 공격자는 TTP의 요청값을 수용할 수 없다. 이는, 공격자는 TTP가 전달한 랜덤값이 0일 때는 이를 위장할 수 있지만 1일 때는 인가코드의 미소유로 해당 값을 생성할 수 없다. 따라서, 공격자는 랜덤값이 1일 경우가 한 번이라도 포함될 경우 해당 증명단계를 검증할 수 없다.

V. 결론

본 논문에서는 마이데이터 서비스 등록단계와 마이데이터 서비스 인증단계를 통해 Zero-Knowledge Proof를 활용한 마이데이터 서비스 제공 방안을 제안하였다. 마이데이터 서비스가 다양해지고 증가함에 따라 데이터 제공자와의 개별 인증과 마이데이터 서비스 제공자에 대한 신뢰 문제에 대응하기 위해 본 제안이 도움이 될 것으로 판단된다.

향후에는 마이데이터 서비스를 안전하게 제공하기 위해 마이데이터 서비스를 분석하고 안전하게 제공할 수 있는 방안을 제안하고자 한다.

[참고문헌]

- [1] 삼정KPMG 경제연구원, “데이터 경제의 시작, 마이데이터 : 금융 산업을 중심으로”, SamJung INSIGHT, Vol. 68, 2020.
- [2] 금융위원회, “소비자 중심의 금융혁신을 위한 금융분야 마이데이터 산업 도입방안”, Jul. 2018.
- [3] 권민경, “국내외 마이데이터 도입 현황 및 시사점”, 자본시장연구원, Feb. 2019.
- [4] Oded Goldreich and Yair Oren, “Definitions and Properties of Zero-Knowledge Proof Systems”, Journal of Cryptology, Vol. 7, No. 1, 1994.