Journal of Digital Convergence
Vol. 19. No. 8, pp. 205-217, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.8.205

재구성된 영지식 증명을 활용한 탈중앙형 자기 주권 신원의 안전한 비식별화 및 데이터 주권 관리

조강우[1], 전미현[1], 신상욱[2*]
[1]부경대학교 정보보호학과 대학원생, [2]부경대학교 IT융합응용공학과 교수

Secure De-identification and Data Sovereignty Management of Decentralized SSI using Restructured ZKP

Kang-Woo Cho[1], Mi-Hyeon Jeon[1], Sang Uk Shin[2*]
[1]Graduate Student, Dept. of Information Security, Pukyong National University
[2]Professor, Dept. of IT Convergence and Application Eng., Pukyong National University

요 약 탈중앙형 SSI(Self Sovereign Identity)가 새로운 디지털 신원 식별 기술의 대안으로 등장하였으나 이는 데이터 거래의 고유 알고리즘 특성으로 인해 효율적인 비식별화 기법이 제안되지 않았다. 본 논문에서는 SSI의 탈중앙형 동작을 보장하기 위해 ZKP(Zero Knowledge Proof)의 검증 결과를 검증인 측에서 외부에 제공 가능한 형태로 재구성함으로써 식별자를 제거하지 않는 비식별 기술을 제안한다. 또한, 이는 검증 참여 각 개체에 대한 차등 주권 관리 개념을 제안하는 것으로 재구성된 비식별 데이터를 정보주체의 동의 없이 제공할 수 있다. 결과적으로 제안 모델은 탈중앙형 SSI 환경에서 국내 개인정보보호법을 만족하고, 안전하며 효율적인 비식별 처리 및 주권 관리를 제공한다.

주제어 : 탈중앙화, 자기 주권 신원, 자격 증명, 비식별화, 영지식 증명

Abstract Decentralized SSI(Self Sovereign Identity) has become an alternative to a new digital identity solution, but an efficient de-identification technique has not been proposed due to the unique algorithmic characteristics of data transactions. In this study, to ensure the decentralized operation of SSI, we propose a de-identification technique that does not remove identifiers by restructuring the verification results of ZKP (Zero Knowledge Proof) into a form that can be provided to the outside by the verifier. In addition, it is possible to provide restructured de-identification data without the consent of data subject by proposing the concept of differential sovereignty management for each entity participating in verification. As a result, the proposed model satisfies the domestic personal information protection law in a decnetralized SSI, in addition provides secure and efficient de-identification processing and sovereignty management.

Key Words : Decentralization, Self-Sovereign Identity, Credential, De-Identification, Zero-Knowledge Proof

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2019R1I1A3A01060652), and a part of the project titled 'Future fisheries food research center', funded by the Ministry of Oceans and Fisheries, Korea.
*Corresponding Author : Sang Uk Shin(shinsu@pknu.ac.kr)
Received May 10, 2021 Revised August 6, 2021
Accepted August 20, 2021 Published August 28, 2021

1. 서론

중앙 집중 형태의 온라인 신원 인증 기법은 1990년대부터 현재까지 신원 식별 및 검증의 주요 기술로 자리매김하였다. 하지만 SPoF(Single Point of Failure) 및 성능 병목 현상 등 각종 중앙 집중형 문제점이 지속적으로 보고되어 디지털 신원 식별 분야에서는 더 이상 적합하지 않게 되었다[1].

이에 따라 새로운 온라인 신원 인증 기법의 수요가 급증하였다. 전자서명법 개정안에서는 기존 제도의 폐지를 명시한 바 있으며, 이에 따라 공인인증서는 공인 효력을 상실하게 되었다[2]. 이를 중점으로 2020년 12월 10일 시행된 개정 전자서명법에 의하여 기존 PKI(Public Key Infrastructure) 기반 구조에서 벗어난 연구들이 등장하였으며, 이러한 제도적 변화는 기존 중앙 집중 형태를 탈피하는 블록체인 기반 탈중앙형 디지털 신원 식별 솔루션의 연구로 이어졌다[3].

상기 논의된 사항을 종합하여 고려하였을 때, SSI(Self-Sovereign Identity) 기술은 탈중앙 환경에서 자기 주권형 신원 서비스를 확립하는 연구로 중앙 집중 형태의 문제점을 다수 보완할 수 있다[4-6]. 하지만 SSI의 고유 알고리즘 특성은 국내 개인정보보호법 등에서 요구하는 비식별화 및 목적 외 제 3자 제공 등을 만족하기 매우 어려운 실정이다. 또한, SSI에 비식별화 및 접근제어를 적용하는 연구는 국내외를 비롯하여 거의 이루어지지 않았으며, 과도기적 성향을 보인다.

본 논문에서는 이러한 문제점을 보완하기 위해 SSI의 ZKP(Zero-knowledge proof) 검증 과정을 개선한 비식별화 모델을 제안한다. 이는 통상적인 SOVRIN 기반 탈중앙형 SSI의 자격 증명에 대한 발행 및 검증 과정에 별도의 거래 증명 증거를 포함하는 것으로 다자 간 신원 데이터 거래의 신뢰성을 확보한다. 또한, 검증인은 증명인으로부터 영지식으로 검증한 VP(Verifiable Presentation)를 증명인의 동의 없이 제3자에 안전하게 제공하기 위해 해당 검증 사실을 VC(Verifiable Credential)로써 직접 발행한다. 본 논문에서 이를 재구성 데이터라 정의하며, 이는 신원 속성 정보를 포함하지만 증명인의 식별자를 검증인의 식별자로 대체하여 정보주체와 정보의 연결성을 차단하는 동작으로 비식별화를 달성한다. 마지막으로, 각 개체가 접근하는 데이터에 대한 차등 주권 레벨을 부여하는 것으로 접근 제어를 달성하여 원본 데이터와 재구성 데이터를 구분하고 데이터 추론을 방지한다. 본 논문을 통해 탈중앙형 SSI의 신원 데이터를 안전한 비식별 데이터로 가공하며, 정보주체의 신원을 훼손하지 않는 동시에 목적 외 데이터 외부 공유의 원활한 달성을 목적으로 한다.

본 논문의 구성은 다음과 같다. 2장에서 비식별화 기술 개요 및 지침 동향 분석, 탈중앙형 SSI의 배경지식을 제시하고 3장에서 제안 모델의 보안 위협, 가정 및 구체적인 프로세스를 기술한다. 4장에서는 제안 모델의 기술적, 법리적 타당성을 판단하고 나아가 실제 검증 시나리오에 대입하여 효율성을 실증한다. 마지막으로 5장에서 본 논문의 결론을 제시한다.

2. 배경 지식

2.1 데이터 비식별화

비식별화는 가명화와 익명화를 포괄하는 개념으로 본질적으로 단일 대응성(Single out), 연결성(Linkability), 추론 허용성(Inference)의 세 가지 주요 성질 중 일부 혹은 전부를 제거하는 것을 의미한다. 세 가지 구성 요인을 모두 제거하는 것을 익명화, 연결성과 추론 허용성만을 제거하는 것을 가명화로 정의한다[7]. 또한, 개인정보보호법 제2조의 1항 나목에서 정의하는 합리적인 방법을 통해 재식별화가 불가능하도록 생성된 비식별 데이터는 법령상 개인정보에 해당하지 않으며 그와 반대로 재식별화가 가능한 비식별 데이터는 법령의 보호 대상으로 본다[8].

비식별화는 무작위화 방법과 일반화 방법으로 분류할 수 있다[9]. 무작위화 방법은 식별자를 제거하거나 대체하여 원본 데이터의 신뢰성을 임의로 크게 저하시킴으로써 단일 대응성, 연결성 등의 경계를 모호하게 설정하는 방법으로, White Noise Addition, Replacement, Subtitution 등의 기법이 존재한다. 일반화 방법은 데이터 자체를 수정하는 방법으로, 일련의 기준에 따라 데이터값을 범주화한 후 보편적인 범위로 확장한다. 즉, 일반화된 데이터가 특정 개인을 지시할 수 없도록 하는 방법이며 k-anonymity, l-diversity, t-closeness의 요구사항을 기반으로 설계된 Aggregation 기법 등이 존재한다.

결과적으로, 다양한 조치를 통해 생성한 비식별 데이터는 단일 대응성, 연결성, 추론 허용성 등을 방지하여야 하며 아울러 합리적인 방법으로 타 정보와의 결합을 통해 재식별될 수 없어야 한다.

2.2 데이터 비식별화 지침 동향 분석

EU의 GDPR(General Data Protection Regulation)

에서 제시된 개인정보의 패러다임은 비식별화에서 기인한다. GDPR은 Article 4의 5항에서 비식별화의 기준으로 가명처리를 채택하였음을 기술하였고, 이와 같은 가명처리는 추가적인 정보의 사용 없이 더 이상 특정 개인정보주체에게 연계될 수 없는 방식으로 개인정보를 처리하는 것임을 규정하고 있다[10]. 즉, 추가적인 식별자 없이 개인을 구분할 수 없는 정보는 가명처리된 정보로 간주하며, 이는 원본 개인정보와는 다른 효력을 갖는 가공된 개인정보의 일부분으로 취급된다. 또한, 데이터의 강력한 비식별화를 기반으로 GDPR Article 7의 1항에서 개인정보처리 시 정보주체의 완벽한 동의를 보장하거나 Article 16 및 17의 1항에서 정정권과 삭제권을 보장하는 등 기존 지침과는 확연히 다른 다양한 요구사항을 정립하고 있다[11, 12].

이러한 변화에 따라 미국은 개인정보를 분류하여 식별정보의 경우 민감정보일 때 사전동의를, 비식별정보일 때는 사후동의를 받도록 개정하였다. 그로 인해 데이터의 주된 거래는 연방거래위원회(Federal Trade Commission, FTC)에서 관리하며, 안전하게 비식별화된 데이터라 하더라도 기업 간 거래를 용인하지 않는 대신 FTC에서 승인한 데이터 중개상을 통해 유통하는 방향으로 발전하였다. 일본의 경우 개인정보보호법을 개정하여 익명가공정보 개념을 도입하였다. 이는 개인정보처리 기준 및 유관 법령 다수를 GDPR에 맞추어 전체적으로 개정하였으며 2018년 7월 GDPR의 적정성 평가를 통과하였다. 이로 인해 EU와 상이한 개인정보처리 기준을 사용하는 미국과는 달리, 적정성 평가를 통과한 일본 내 기업은 EU 내에서 별다른 심사 없이 서비스할 수 있다[13].

우리나라 역시 개인정보 데이터 처리에 따른 변화에 발맞추었다. 2020년 8월 5일 발효한 정보통신망법·개인정보보호법·신용정보법(이하 데이터 3법) 개정은 결과적으로 개인정보보호 주체의 통일, 비식별 정보 활용의 확대, 개인정보 자기 주권, 개인정보 규제 체계 재정비 등을 목적으로 둔다.

2.3 탈중앙형 SSI(Self Sovereign Identity)

2.3.1 SSI의 개요

탈중앙형 SSI는 DID(Decentralized IDentity) 기술의 일종으로, TTP(Trusted third party)를 요구하지 않는 상호 비신뢰 환경에서 분산화된 신원 자격 증명 서비스를 제공한다. 또한, 정보주체에 의한 주도적인 정정권, 삭제권 등의 폭넓은 자기 주권을 보장할 수 있다[14-17]. SSI의 구성 요소는 식별자(Identifier)와 신원(Identity)으로 구분되며, 신뢰할 수 있는 안전한 저장소에 신원을 저장한 후 이를 지시하는 탈중앙형 식별자를 검증하여 신원 식별을 수행한다. SSI의 식별자는 DIDs(Decentralized IDentifiers)를 통해 탈중앙형 동작을 구현한다[18]. DIDs resolver의 일반적인 형태는 다음과 같다.

did : sov : xx-yy-zz

Fig. 1은 SSI 동작의 거시적인 개요를 나타낸다. SSI의 신원은 최초 실질적인 정보주체인 증명인(Holder)의 자격 주장(Claim)에서 기인한다. 하지만 이는 다른 검증 참여자에 의해 유효하지 않기 때문에 발행인(Issuer)의 전자 서명을 통해 유효성을 입증한다. 이러한 과정을 신원 자격 증명(Credential)의 발행이라 하며, 이를 기반으로 VC가 생성된다[19]. 복수의 VC를 지닌 증명인은 실질적으로 검증에 사용될 속성만을 종합하여 VP를 생성한다. 생성된 VP는 ZKP의 Challenge 기반 검증 기법을 통해 검증인(Verifier)에게 제출된다[20-22]. 검증인은 제출된 VP를 통해 증명인의 주장 및 발행인의 전자 서명을 확인하고 결격 사유가 없는 경우 VP를 신뢰할 수 있다.

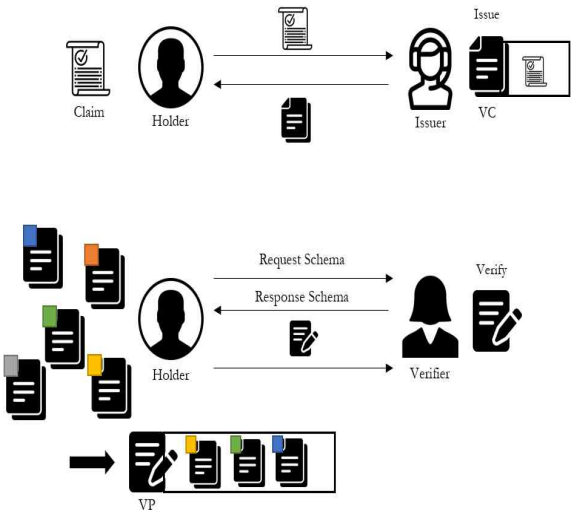

Fig. 1. Overview of the SSI

2.3.2 SSI의 신원/식별 검증 절차

본 항에서는 SSI 관련 연구 중 가장 대중화된 연구인 Hyperledger Indy 기반의 SOVRIN을 예시로 SSI의 식별 절차 및 ZKP 검증 절차에 대하여 보다 상세하게 논의한다[23].

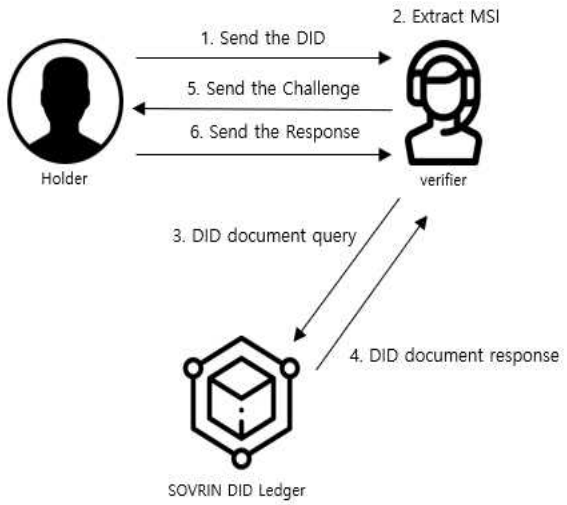

Fig. 2. A process of the DID authentication

먼저 Fig. 2와 같이, 두 참여자가 참여하는 증명이 발생하였을 경우 증명인이 검증인에게 자신의 합당한 신분을 증명하기 위해 최초 DID를 전달한다. 이를 제공받은 검증인은 DID의 MSI(Method Specific Identifier)를 추출하여 SOVRIN의 DID 분산 원장에 접근한 후, MSI가 지시하는 위치의 DID document를 획득한다. 검증인은 획득한 공개키로 사전에 공유되지 않은 난수를 암호화하여 Challenge를 생성한 후 증명인에게 전달한다. 증명인은 자신이 지닌 개인키로 Challenge를 복호화하여 난수를 획득하고, 이를 검증인에게 제시하는 것으로 자신이 해당 DID의 주체임을 주장할 수 있다.

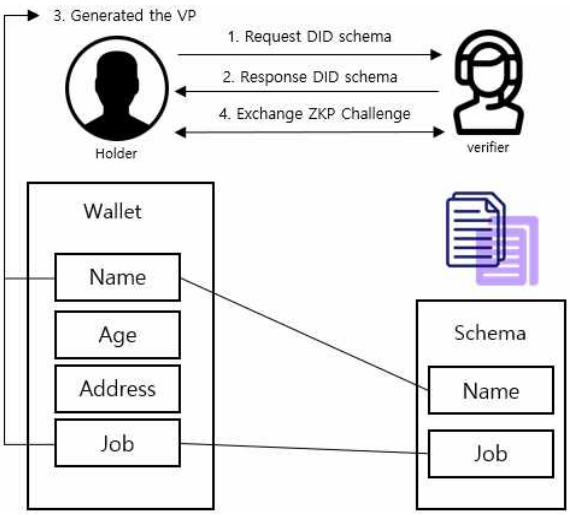

Fig. 3. A process of the SOVRIN verification

Fig. 3은 SOVRIN 모델에서 ZKP를 활용하여 증명인이 제출한 VP를 검증하는 기존 절차를 나타낸다. 최초, 신원 데이터 제공자로써 증명인은 자신의 Claim을 이용해 사전 발행된 VC를 안전한 전자 지갑에 보관하고 있음을 가정한다. 검증인은 자신이 증명인의 요청을 수행하기 위해 필요한 최소한의 Credential을 정의한 DID Schema를 증명인에게 전달한다. 이를 확인한 증명인은 보유한 VC 중 검증인이 요구하는 Credential만을 조합하여 VP를 생성한다. Fig. 3의 예시는 검증인의 Schema가 Name과 Job을 요구하기 때문에 증명인의 전자 지갑에서 이를 추출하여 VP를 생성함을 보인다. 해당 거래에서 생성된 VP는 오직 증명인-검증인 간의 약속된 Credential 조합으로 산출되었기 때문에 다른 검증에 해당 VP를 재활용할 수 없다는 것이 특징이다. 증명인은 생성된 VP를 ZKP 검증이 가능한 형태로 검증인에게 제공한다. 원본 데이터를 거래하지 않고도 해당 데이터의 보유 사실을 검증할 수 있는 ZKP의 특성으로 검증인은 자신이 요구했던 Credential 요소를 증명인이 보유하고 있음을 검증하는 것으로 신원 데이터 거래 절차를 종료한다.

3. 재구성 데이터 비식별화

3.1 보안 위협

SSI는 식별자의 탈중앙형 동작을 통해 TTP의 존재 유무에 관계없이 안전한 신원 데이터 관리를 제공한다. 또한, 자신의 Claim을 통해 신원 데이터를 발행한 후 해당 데이터에 대한 삭제권, 정정권 등의 자기 주권을 보장받는다. 이는 VP 생성을 통해 자신의 명백한 동의를 기반으로 최소한의 정보만을 선택적으로 제공할 수 있으며 ZKP 검증을 통해 데이터의 안전한 거래 및 기밀성의 목적을 달성한다.

SSI 신원 데이터 트랜잭션에서 탈중앙성 보장, 최소 정보 제공, 유출 및 추론 방지 등의 우수한 장점을 지닌다. 하지만 이러한 특성은 개인정보의 제3자 제공 및 이를 위한 비식별화 조치 관점에서 아래와 같은 문제점이 존재한다. Table 1은 본 절의 요약으로, 기존의 SOVRIN 환경에서 비식별화 및 데이터 외부 공유를 수행할 경우 발생 가능한 위협 모델을 제시한다.

- Threat 1 : SSI 개인정보에서의 식별자는 신원 데이터 지시 및 탈중앙형 동작을 보장하는 요소이다. 따라서 식별자를 삭제할 경우 SSI의 탈중앙 성질을 상

Table 1. Threat models of the proposed model

	Threat model	Details
Threat 1	De-identification to delete an identifier is not applicable	The identifier in SSI cannot be deleted because it is in charge of decentralized operation, and separate de-identification is required that does not delete the identifier.
Threat 2	Dishonest or honest-but-curious entity	An entity falsifies de-identification data of undetermined source or deceives another entity with non-existent data.
Threat 3	Transaction of de-identification data without Opt-In	In the absence of reliable access management policy between verifier and others, th problem of impossibility to grant reliability for restructure VC

실하기 때문에 비식별화 기법 중 식별자를 훼손하는 무작위화 방법을 적용하기 어렵다.

- Threat 2 : 정보처리위탁자에 해당하는 자가 비식별 데이터를 제3자에게 공유하기 위해서는 비식별 데이터의 출처 신뢰를 보장하여야 한다. 이 과정에서 정직하지 않거나 혹은 정직하지만 호기심이 많은 검증인이 출처가 불분명한 비식별 데이터를 위조하거나 기만할 가능성이 존재한다.
- Threat 3 : SSI 환경에서 신원 데이터에 대한 출처 신뢰 및 탈중앙형 동작을 보장할 수 있는 비식별화 기술이 존재함을 가정하더라도, 이를 검증인이 제3의 참여자에게 제공하는 과정에서 보안 취약점을 수반한다. 기존 SSI 구조는 모든 데이터 거래에 있어 정보주체의 명백한 동의를 요구하기 때문에 개인정보보호법 제28조의2를 만족하기 어렵다.

3.2 가정

본 논문에서 제안하고자 하는 재구성 데이터 비식별화는 보안 관점에서의 안전성 검토를 위해 다음과 같은 가정을 수행한다.

- 데이터 트랜잭션에 참여하는 모든 참여자들은 신뢰할 수 있는 DID를 공개된 분산 원장에 등록하였다.
- 증명인은 검증인이 요구하는 VC를 제시할 수 있으며, 발행된 VC를 관리하기 위한 안전한 로컬 저장소를 가지고 있다. 또한, 해당 저장소에 접근하기 위한 개인키는 유출되지 않았다.
- 증명인과 제3의 참여자 사이에서 신원 데이터의 정보처리위탁자에 해당하는 검증인은 정직하지 않거나 정직하지만 호기심이 많을 수 있다.

3.3 제안 모델

본 절은 3.1절에서 기술한 보안 위협을 해결하기 위해 SSI 신원 데이터에 대한 안전한 재구성 데이터 생성 및 제공, 관리의 관점으로 분류하여 논한다. 제안 모델은 각 Actor 간 거래 증명 증거를 추가하며, 신원 데이터를 취급하는 정보처리위탁자가 직접 재구성된 비식별 데이터를 생성한다. 또한, 데이터의 식별자를 대체하는 것으로 원본 데이터의 정보주체를 지시하지 않도록 고안되었다. 이를 통해 수동적인 수준에 그쳤던 기존의 비식별화를 개선하며, 각 개체는 거래 증명 증거를 기반으로 이를 공증하여 신뢰성을 보장할 수 있다. 재구성된 비식별 데이터는 식별자를 삭제하는 대신 다른 Actor의 식별자로 대체하는 동작을 통해 DID를 활용한 비식별화 및 탈중앙형 동작을 모두 보장할 수 있도록 설계된다. 마지막으로 재구성 데이터의 주권 관리 과정에서는 일련의 데이터 거래에서 참여 개체들의 역할에 따라 데이터의 주권을 차등 부여함으로써 개인정보보호의 안전성을 제공한다.

Table 2는 제안 모델 및 의사 코드에서 사용하는 구성 요소의 세부 사항을 요약하여 나타낸 표이다.

Table 2. Symbols of the proposed model

Symbol	Details
$Blinded\,secret$	Result of mixing $Link\,secret$, PK, PKr, RN
$Link\,secret$	Secret information to prove ownership of ZKP VC
PK	Public key for VC verification
PKr	Public key for VC revocation
RN	Random number that only the holder knows
$H(Bs)$	SHA256 digest of $Blinded\,secret$ (Transaction proof)
Metadata	Data for VC issuance
ZKP_{VC}	Result of ZKP for original VC
R_VC	Restructured VC

3.3.1 재구성 데이터 생성 및 외부 공유

Fig. 4는 제안 모델에서 재구성 데이터의 생성 및 제3자로 제공하는 기법의 절차를 나타내었다. DID를 이용한 상호 신원 검증은 사전에 안전하게 수행되었음을 가정한다. Fig. 5는 재구성 데이터 생성 프로세스(Process

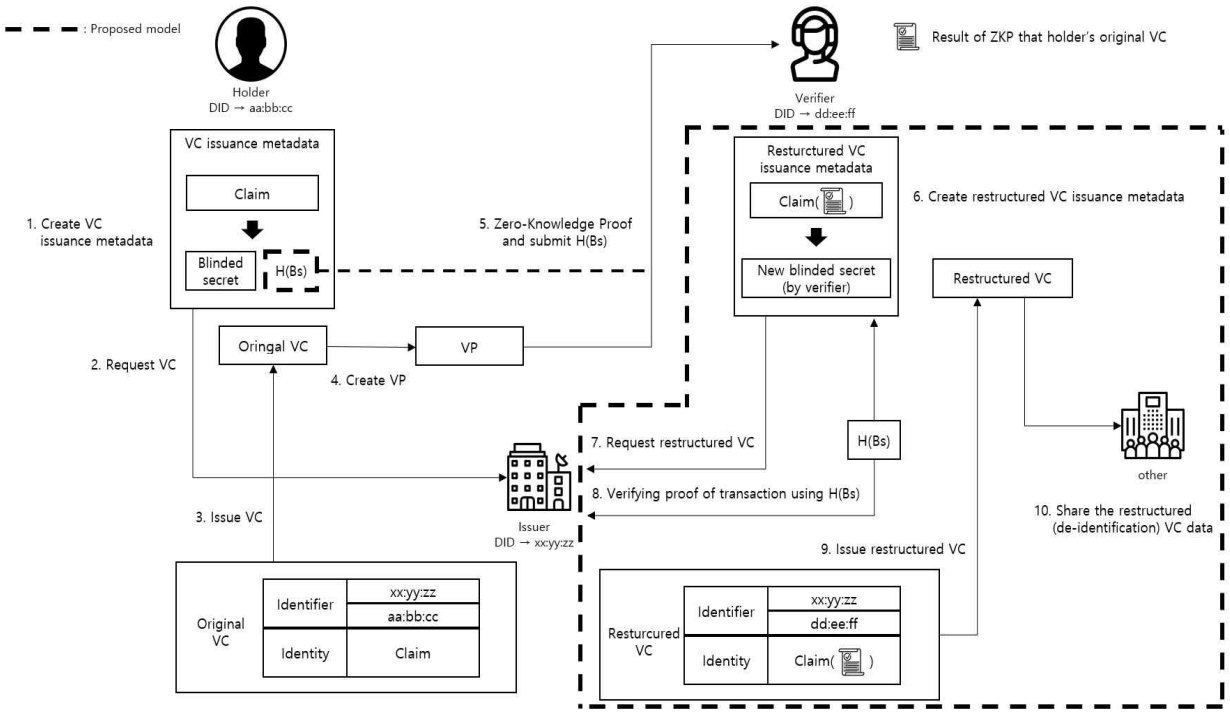

Fig. 4. Process of the proposed model

Algorithm 1. Generation of the restructured data

Entity Holder, Verifier, Issuer
Require ZKP_{VC}, $H(Bs)$

1 **Create** R_VC issuance info. by Verifier
2 Blinded Secret = R_VC's blinded secret
3 Claim = ZKP_{VC}
4 DID = Verifier's DID
5 **End Create**
6 Send R_VC issuance info Verifer -> Issuer
7 **Verify** $H(Bs)$ by issuer
8 Request $H(Bs)$ = Issuer -> Verifier
9 Response $H(Bs)$ = Verifier -> Issuer
10 **if** Verifier{$H(Bs)$}==Issuer{($H(Bs)$)} **then**
11 R_VC = Issue(R_VC)
12 **Else**
13 **Reject** Issue(R_VC)
14 **End if**
15 **Return** R_VC
16 **End Verify**

Fig. 5. Pesudo code of the generation process

6~8)의 부분적인 의사 코드를 나타내며, 상세 절차는 다음과 같다.

1. 최초, ZKP의 VC 발행 단계에서 자신의 Claim을 VC로 발행 요청하기 위한 $Blinded\,\mathrm{secret}$을 생성한다. 이는 발행을 요청할 발행인의 Schema를 기준으로 작성되며, $Link\,\mathrm{secret}$ 및 PK, PKr, RN을 포함하여 SOVRIN에서 수행하는 일반적인 $Blinded\,\mathrm{secret}$ 생성 절차를 따른다. 이는 추후 $Link\,\mathrm{secret}$에 대응될 수 있으며, 증명인만이 알고 있는 RN을 포함하기 때문에 $Link\,\mathrm{secret}$의 소유주(증명인)와 $Blinded\,\mathrm{secret}$이 지시하는 VC의 소유권 실증을 돕는다.
2. 증명인은 추가적으로 추후 3자 거래 증명 증거로 사용할 $Blinded\,\mathrm{secret}$의 SHA256 해시 다이제스트 $H(Bs)$를 생성한다. 증명인은 검증인과의 신원 데이터 검증에 사용할 $Link\,\mathrm{secret}$ 및 RN, $Blinded\,\mathrm{secret}$, $H(Bs)$를 안전한 개인 저장소에 보관한 후 $Blinded\,\mathrm{secret}$과 $H(Bs)$를 발행인에게 전달한다.
3. 이를 전달 받은 발행인은 VC 발행 절차를 수행하며, 발행된 VC를 증명인에게 전달한다.
4. 증명인은 해당 VC를 이용해 검증인이 요구하는 Credential 요소를 집합한 VP를 생성한다.
5. 증명인-검증인 간 ZKP를 수행한다. 해당 검증은 SOVRIN에서 제공하는 일반적인 VP 검증 절차를 따르지만, 추가적으로 증명인이 보유한 $H(Bs)$를 검증인에게 제출한다는 차이점이 존재한다.
6. VP에 대한 검증을 성공적으로 수행하였을 경우,

검증인은 자신이 요구하는 Credential 요소를 증명인이 보유하고 있다는 사실을 알 수 있다. 검증인은 해당 보유 사실을 Claim으로 하는 VC를 발행하는 것으로 비식별 재구성 VC를 생성할 수 있다.

7. VP 보유 사실에 대한 Claim을 VC로 발행하기 위해 검증인은 자신이 검증한 VP에 포함된 발행인 DID를 확인하고, 동일한 발행인에게 재구성 VC 발행을 요청한다.
8. 발행인은 검증인이 실제로 증명인과 VP 검증을 수행한 참여자 여부를 판단할 수 있어야 한다. 이는 검증인이 정직하지 않거나 정직하지만 호기심이 많은 경우 이 과정에서 발행인에게 악의적인 재구성 VC를 요청할 수 있기 때문이다. 검증인은 발행인에게 신뢰를 부여하기 위해 증명인에게 추가적으로 전달 받은 $H(Bs)$를 발행인에게 제시한다. $H(Bs)$를 생성할 수 있는 참여자는 $Blinded\,\mathrm{secret}$를 생성한 증명인이며, 보유할 수 있는 참여자는 사전에 발행 정보를 공유한 증명인과 발행인이다. 따라서 검증인이 이를 보유하고 있음은 증명인과의 상호 작용을 통해 $H(Bs)$를 전달받았음을 의미하며, 이는 그 자체로 증명인-검증인 간의 VP 검증을 수행하였다는 거래 증명 증거로써 동작한다.
9. 검증인이 증명인과 정상적인 VP 검증 및 거래를 수행한 참여자임을 판단한 발행인은 검증인의 Claim에 대한 재구성 VC를 발행한다.
10. 검증인은 발행된 비식별 재구성 VC를 원본 신원 데이터의 비식별 데이터로써, 공익 목적의 제3자에게 제공할 수 있다.

Table 3는 증명인이 검증인과의 검증 과정에서 사용한 VC 및 검증인이 증명인의 VC 보유 사실을 기반으로 발행한 재구성 VC의 차이점을 나타낸다. 검증인의 재구성 VC는 증명인이 제출한 VC를 기반으로 생성되기 때문에 포함된 Credential의 내용은 동일하다. 하지만 증명인의 DID가 검증인의 DID로 대체되었기 때문에 탈중앙형 동작을 훼손하지 않으면서 증명인과 개인정보의 연

Table 3. Comparison of the VC

VC	Identifier	Identity
Original VC	aa:bb:cc (holder)	Credential
Restructure VC	dd:ee:ff (verifier)	Credential

Algorithm 2. Sharing of the restructured data

Entity Verifier, Other
Require R_VC

```
1 Request R_VC by Other
2  If Available(Request) then
3   Response R_VC = Verifier{R_VC}
4  Else
5   Reject Request
6  Return Claim(ZKP_VC)
7  End if
8 Verify R_VC by Other
9  GetDID_Issuer = Issuer's DID
10 GetDID_Verifier = Verifier's DID
11 GetVerify = R_VC (DID_Issuer,
     DID_Verifier)
12 End Verify
```

Fig. 6. Pesudo code of the sharing process

관성을 제거하는 것이 가능하다. 이는 정보주체가 검증인으로 이전되는 결과를 도출한다. 즉, 재구성 VC는 증명인을 지시하지 않기 때문에 개인정보보호법 제 28조의 2에서 규정하는 '특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하지 않은 가명정보'로써 동작한다. Fig. 6는 재구성 VC의 제3자 외부 제공(N차 공유) 프로세스를 나타낸 의사 코드이며, 세부적인 절차는 다음과 같다.

1. 검증인은 ZKP 검증을 통해 획득한 정보(증명인의 정보 보유 사실)를 증명인의 동의 없이 제3자의 외부인에게 제공할 수 있는 상태이다.
2. 외부인이 공익 목적으로 증명인의 비식별 데이터에 대한 접근을 요청하는 경우, 정보처리위탁자에 해당하는 검증인은 DID로 자신을 지시하는 재구성 VC를 제시한다. 이 경우, 검증인은 재구성 데이터의 증명인으로, 외부인은 제3의 검증인으로써 SSI 네트워크 환경에서 VP 검증의 역할을 수행한다.

제안 모델의 결과물인 재구성 데이터(R_VC)는 증명인이 지닌 VC 원본을 어떠한 개체에게도 노출하지 않는 구조이기 때문에 외부로 유출되지 않는다. 대신 증명인의 VC 보유 사실만을 이용해 생성된 재구성 VC는 검증인을 정보주체로 하여 식별자를 대체(Replacement)한 비식별 데이터임과 동시에 증명인의 동의 없이 검증인의 동의만으로 제3자에게 제공할

수 있다. 이 경우 검증인이 재구성 VC의 정보주체가 되어 2차 검증인이 되는 제3자에게 ZKP 검증을 다시 수행할 수 있다. Credential에 포함된 Claim 정보는 N차 공유가 이루어지지만, 식별자가 다르기 때문에 동일 VP에 대한 재공유가 아닌 재구성 VC를 기반으로 생성된 별도의 재구성 VP에 대한 검증이 이루어진다. 제안 모델에서는 상기 서술한 특수한 형태의 데이터 거래 알고리즘을 도입하는 것으로 VC 재사용에서 기인하는 ZKP의 Prior agreement 문제점을 해결한다.

3.3.2 재구성 데이터 차등 주권 레벨링

제안 모델에서 검증인으로부터 발행된 재구성 VC는 제3자 외부 공유를 위해 비식별화 되어 안전하게 거래할 수 있는 비식별 정보로 동작한다[24]. 제안 모델은 SSI에서 신원 데이터 거래 환경에 참여하는 각 개체를 레벨 단위로 세분화하여 각 참여자의 데이터 주권을 차등 관리한다. Table 4는 최초 정보주체인 증명인이 보유한 VC와 이를 기반으로 하여 생성된 재구성 VC를 중점으로 SSI 네트워크에 참여하는 각 개체가 접근할 수 있는 차등 주권 레벨링을 나타낸다.

SSI의 자기 주권형 동작을 보장하기 위해 정보주체는 자신의 Credential에 대한 모든 정보를 보유해야만 한다. 따라서 증명인은 자신의 VC를 생성하기 위한 모든 정보의 접근 권한을 지닌다. 즉, 정보주체로서의 최상위 주권을 행사할 수 있다. 발행인은 VC 발행을 위한 정보에 접근 권한을 지닌다. 따라서 VC 발행 정보인 증명인의 Claim, PK 및 거래 증명 증거로 사용될 $H(Bs)$ 등에 대한 접근 권한을 부여 받지만 $Blinded\,\mathrm{sec}ret$, PKr 및 증명인의 로컬 저장소에 대한 개인키 등에 접근할 수 없다. 검증인은 증명인이 제시하는 VP 검증 및 재구성 VC를 생성하기 위한 최소한의 정보만 접근할 수 있는 권한이 부여된다. 즉. 검증인은 증명인의 Claim, VC의 원본 및 $Blinded\,\mathrm{sec}ret$ 등의 발행 정보에 주권을 갖지 않으며, R_VC에서의 Claim의 역할을 대신하기 위한 ZKP_{VC} 및 거래 증명 정보 $H(Bs)$에 대해서만 권한을 지닌다. 검증인으로 인해 발행된 R_VC를 제공받는 외부인(제3자)은 실질적으로 검증 과정에 참여하지 않기 때문에 가장 축소된 차등 권한을 부여 받는다. 따라서 외부인은 그 어떤 원본 데이터 및 생성 데이터에 접근할 수 없으며, 오직 검증인이 제공한 재구성 비식별 데이터인 R_VC에 대해서 정보 접근, 삭제권 등의 주권을 지닌다.

4. 분석 및 응용 시나리오

4.1 기술적 분석

본 절에서는 3.1절에서 제시한 위협 모델을 SOVRIN 및 제안 모델에 적용하여 비교하는 것으로 보안 관점에서의 기술적 분석을 진행하며, 해당 내용을 Table 5를 통해 요약하였다.

기존 SSI 모델의 가장 범용적인 연구인 SOVRIN은 Credential에 대한 검증 및 거래 과정에 있어 각 위협 모델에 대해 다음과 같은 문제점을 보인다.

- Threat 1 : SOVRIN은 식별자를 삭제하는 비식별화를 수행하였을 경우 탈중앙형 동작을 보장할 수 없다. 따라서 식별자를 삭제하지 않는 비식별화 기술을 요구하지만, SOVRIN 구조는 이러한 비식별 기술이 존재하지 않는다.
- Threat 2 : SOVRIN은 VC에 증명인 및 발행인의 식별자 정보를 포함하는 것으로 검증인으로 하여금 신뢰할 수 있는 출처 증명을 포함한다. 하지만 데이터 검증에 ZKP를 사용하기 때문에 제3자 제공시 데이터 신뢰성을 훼손하는 Prior agreement 문제점에 도달한다. 따라서 정보처리위탁자에 해당하는 검증인이 제3의 외부인에게 비식별 데이터를 공유할 경우 출처에 대한 신뢰를 충족할 수 없으며, 정직하지 않

Table 4. Differential sovereignty management of the proposed model

Level	Subject	Original identity	Issuance metadata	Identifier	ZKP Challenge	Restructure VC
0	Holder	■	■	■	■	
1	Issuer		■	■		
3	Verifier			■	■	■
4	Other					■

거나 정직하지만 호기심 많은 정보처리위탁자에 의한 데이터 위조 및 기만 공격에 여전히 취약하다.

- Threat 3 : 식별자를 제거하지 않으면서 동시에 정보처리위탁자에 대한 보안 위협을 해결할 수 있는 비식별화 기술이 제안되더라도, 이를 정보주체의 동의 없이 처리할 수 있는 근거가 충분하지 않다. SOVRIN의 개인정보는 정보주체에 대한 강력한 자기 주권을 보장하며, 모든 데이터의 거래는 정보주체의 명백한 동의에 근거하기 때문에 정보처리위탁자가 정보주체의 동의 없이 비식별 데이터를 처리하는데 어려움이 따른다.

한편, 동일한 위협 모델을 제안 모델에 적용하였을 경우 이를 해결하는 기술적 근거는 다음과 같이 정리할 수 있다.

- Threat 1 : 제안 모델은 데이터의 비식별 처리를 위해 식별자를 제거하는 대신, 새로운 정보주체가 될 정보처리위탁자의 식별자로 대체하여 SSI의 탈중앙형 동작을 여전히 보장한다. 또한, 정보처리위탁자에 의해 재구성된 비식별 데이터는 정보주체가 제공한 개인정보인 Credential에 대한 신뢰할 수 있는 검증 정보를 포함하지만, 정보주체를 지시하는 식별자가 대체됨으로써 비식별화를 위한 단일 대응성, 연결성, 추론성 제거를 달성한다.
- Threat 2 : 제안 모델은 상호 비신뢰 관계의 블록체인 네트워크에서 실질적으로 VC 검증에 참여하는 증명인-발행인-검증인 간의 신뢰 결정을 보장하기 위해 거래 증명 증거를 추가하였다. 오직 증명인-발행인만이 알고 있는 거래 증명 증거를 검증인과 공유하는 동작을 통해 원본 데이터의 거래가 증명인의 명백한 동의에 의하여 수행되었음을 증명하고, 발행인으로 하여금 적법한 검증인임을 판단할 수 있도록 동작한다.
- Threat 3 : 제안 모델은 안전하게 비식별 처리 된 재구성 데이터를 정보처리위탁자가 제3의 외부인에게 정보주체의 동의 없이 제공하기 위해 차등 주권 레벨링 개념을 도입하였다. 개인정보에 대해 가장 강력한 주권을 행사하여야 할 정보주체는 원본 신원 데이터에 대한 주권을 보장 받는다. 반면, 비식별화 된 재구성 데이터에 대한 실질적인 주권은 정보처리위탁자에게 존재한다. 정보주체의 명백한 동의 없이 데이터 거래가 불가능한 SSI 환경에서 동의 없는 데이터를 거래를 실현하기 위해 정보주체 대신 정보처리위탁자의 동의를 통해 거래할 수 있는 비식별 데이터를 발행할 수 있다.

4.2 법리적 분석

본 절은 2.2절에서 기술한 국내 비식별 처리 유관 법률에 근거하여 제안 모델의 법리성을 분석한다.

개인정보보호법 제2조제1항의2에서는 가명처리를 '개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보 없이 특정 개인을 알아볼 수 없도록 처리하는 것'으로 규정한다. 제안 모델에서 가명처리 된 데이터는 정보처리위탁자로부터 생성된 재구성 VC로, 이는 개인정보 중 특정 개인을 식별할 수 있는 일부 정보인 식별자를 재설정하여 비식별 처리를 달성한다. 또한, 원본 신원 데이터의 제공은 정보주체의 명백한

Table 5. Comparison of SOVRIN and the proposed model

	SOVRIN	Proposed model
Threat 1	Decentralization that relies on identifiers	Eliminate single out, linkability, inference through identifier replacement
Threat 2	Data cannot be shared externally due to ZKP's Prior agreement	Ensuring the trust of externally provided data using proof of transaction
Threat 3	Data cannot be shared without the consent of the data subject due to Opt-In	Secure sharing of non-identification data by differential sovereignty
Personal info. protection law Article 2	Generate non-identification data that removes identifiers	Generate non-identification data that does not remove identifiers
Personal info. protection law Article 17	External data sharing by data subject's compulsory Opt-In (Dissatisfied)	External data sharing by data consignor's Opt-In (Satisfied)
Personal info. protection law Article 35, 36	No consideration of access control to non-identifying data	Control access to non-identifying data and ensure self-sovereignty over original data

동의에 근거하기 때문에 동법 제15조를 만족하며, 공익 목적의 재구성 비식별 데이터 제공은 정보주체의 동의 없이 정보처리위탁자의 동의만으로 가능하므로 동법 제17조를 만족함을 확인할 수 있다. 아울러 차등 주권 레벨링을 통해 실제 개인정보의 원본 VC에 접근할 수 있는 참여자를 정보주체로 제한함으로써 무분별한 개인정보 열람을 방지한다. 이는 동법 제35조 및 제36조에 해당하는 정보주체의 권리인 정정권, 삭제권을 보장한다. 특히나 동법의 제2조제1항의2 및 제28조, 제35조, 제36조의 조항은 2020년 8월 시행된 개정 개인정보보호법에서 새롭게 추가된 개인정보의 비식별화, 자기 주권에 관한 내용을 포함하고 있다는 점에서 제안 모델은 차세대 신원 식별 기술의 비식별 처리 및 접근 권한 요건을 법리적으로 충족함을 확인할 수 있다. 마지막으로, 제안 모델은 재구성 데이터에 대한 권한을 지닌 정보처리위탁자가 제3자에게 공유할 경우 제3자가 요구하는 VC만을 선택하여 재구성 VP로 생성할 수 있기 때문에 개인정보 최소 제공 원칙에 해당하는 동법 제39조의5를 만족한다. 본 절에 대해, SOVRIN과 제안 모델의 비교 내용을 Table 5에 제시하였다.

4.3 응용 시나리오

본 절에서는 3장에서 기술한 제안 모델을 실제 SSI 검증 시나리오에 적용하는 것으로 실전 문제 응용 가능성을 평가한다. 본 시나리오에서 SSI 검증 과정 참여자는 증명인(구직자)–발행인(학교)–검증인(회사)–외부인(연구기관)으로 구성되며 검증인과 외부인은 각각 구인 활동과 통계 연구를 위해 증명인의 연령 및 학력 정보를 요구하는 것으로 가정한다. 제안 모델을 적용한 시나리오의 개요는 Fig. 7에 제시하였으며, 프로세스는 다음과 같다.

1. 증명인은 검증인이 검증을 위해 요구하는 Credential을 확인한다. 본 시나리오에서는 검증인이 증명인의 연령 및 학력 정보를 요구함을 가정한다.
2. 해당 Credential에 알맞은 VC를 획득하기 위해 졸업증명서 Claim 및 이에 대한 $Blinded\,\mathrm{secret}$, $H(Bs)$를 생성한다.
3. 증명인은 이를 발행인에게 전달하여 VC 발행을 요청한다.
4. 발행인은 증명인이 제출한 정보를 검토하여 정상적인 요청일 경우 졸업증명서 VC를 발행한 후 증명인에게 반환한다.
5. 졸업증명서 VC는 검증인이 요구한 정보보다 많은 정보를 포함할 수 있다. 따라서 증명인은 개인정보 최소 제공 원칙을 만족하기 위해 졸업증명서 VC 중 검증인이 요구하는 연령 및 학력에 대한

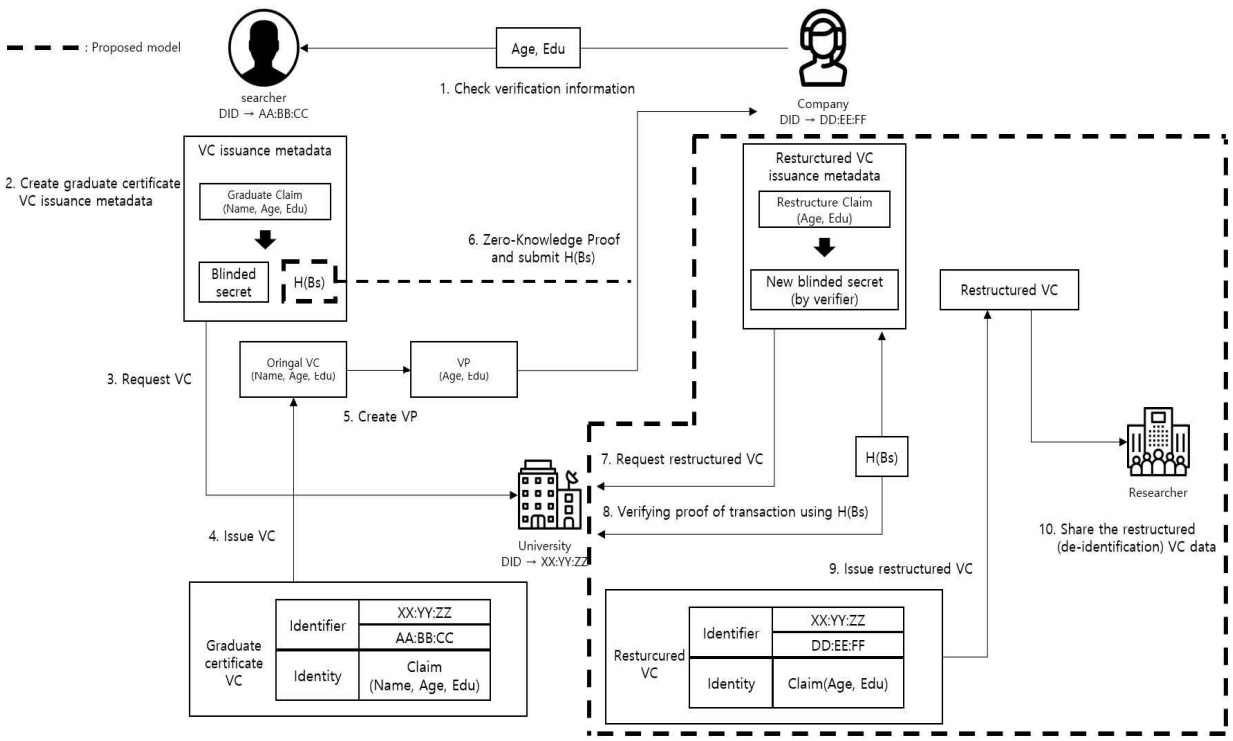

Fig. 7. Application scenario of the proposed model

Table 6. Differential sovereignty management of the scenario

Level	Subject	Original Age & Education	Issuance metadata	Identifier	ZKP Challenge	Restructure Age & Education
0	Searcher	■	■	■	■	
1	University		■	■		
3	Company			■	■	■
4	Researcher					■

Credential을 취합하여 VP를 생성한다.

6. 증명인-검증인 간 VP의 ZKP Challenge를 실행한다. 이 과정에서 증명인은 차후 거래 증명 증거로 사용할 $H(Bs)$를 검증인에게 전달한다.
7. 검증인은 ZKP Challenge에 성공한 이후 증명인의 나이, 학력에 대한 Credential 보유 사실을 인지한다. 추후 이를 비식별화하여 외부인에게 공유하기 위해 증명인의 Claim으로 생성한다. 또한, 발행인에게 해당 Claim을 기반으로 하는 VC의 발행을 요청한다.
8. 발행인은 검증인이 실제 증명인과 VP 검증을 진행한 당사자인지 판단하기 위해 $H(Bs)$를 요구하여 검증한다.
9. 검증인이 정상적인 $H(Bs)$를 제출한 경우 검증인의 재구성 VC 발행을 승인한다.
10. 검증인은 생성한 재구성 데이터를 해당 VC 검증에 참여하지 않은 제3의 외부인에게 제공할 수 있다.

본 시나리오에서, 검증인이 생성한 재구성 VC는 증명인의 나이 및 학력 Credential에 대한 원본이 아니지만, 신뢰할 수 있는 ZKP 검증 결과를 기반으로 재구성하였기 때문에 사본의 역할을 수행할 수 있다. 동시에, 원본 졸업증명서 VC에 포함되었던 이름을 삭제하고 식별자를 대체하였기 때문에 외부인에게 특정인을 지시하지 않는 비식별 데이터로 제공하는 것이 가능하다. 해당 과정에서 사용된 모든 정보에 대한 접근 권한은 Table 6와 같이 차등적으로 관리된다. 결과적으로, 외부인은 식별자를 특정할 수 없는 신원 미상의 나이 및 학력에 대한 신뢰할 수 있는 단순 연구 목적의 Credential을 획득한다.

본 시나리오 검증을 통해 해당 모델이 실제 SSI 검증 환경에서 비식별 데이터의 생성, 거래 및 공유의 모든 단계에서 안전한 비식별화를 보장하는 것을 확인할 수 있다. 또한, 차등 주권 레벨링에 의한 증명을 통해 외부 연구기관이 출처 신뢰 가능한 통계 표본을 획득하였음을 실증할 수 있다.

5. 결론

SSI는 탈중앙형 동작 및 개인정보의 자기 주권, ZKP를 활용한 기밀성 등을 보장하는 것으로 급격하게 변화하는 각국 개인정보보호 유관 법령의 다양한 요구사항을 효율적으로 달성한다. 하지만 기존 디지털 신원 식별 솔루션과는 상이한 특유의 식별 및 검증 절차에 있어 효율적인 비식별 처리와 데이터 트랜잭션 기술이 제안되지 않았다.

본 논문에서는 이러한 문제점을 해소하고자 SSI의 동작 환경에 맞춘 개인정보 데이터 비식별화 솔루션을 제안하였다. 그 결과 원본 VC와 동일한 효력을 가지면서 식별자의 연결성을 제거한 재구성 VC를 생성할 수 있으며, 이에 대한 신뢰성을 부여하기 위한 거래 증명 증거 정보를 VC 발행 과정에 포함하였다. 아울러 원본 VC와 재구성 VC의 접근 권한을 각 참여자에 대해 차등 관리함으로써 SSI의 자기 주권형 동작을 보장하는 범위에서 안전하고 효율적인 비식별 데이터 생성 및 거래 프로세스를 제안하였다. 이는 효율적인 비식별화를 저해하는 내/외부 보안 위협을 기술적으로 해결할 수 있으며, 국내 개인정보보호법에서 정의하는 다양한 규정을 법리적으로 충족할 수 있음을 검증하였다.

본 논문은 재구성 데이터 비식별화 기술의 개념 정립 및 모델 제안 단계에 있으며, 비식별 데이터의 가공 및 거래 기술에 추가적인 연구를 요구한다. 현재의 연구 단계에서는 정보주체의 동의 없이 제3자에게 개인정보를 제공한 경우, 이와 같은 사실을 정보주체에게 안전하게 고지하는 문제를 해결할 수 없다. 또한, 정보주체의 삭제권 행사로 인해 원본 VC가 삭제된 경우 이에 연관된 재구성 VC를 유기적으로 삭제할 수 없기 때문에 해당 한계

점에 대한 지속적인 개선이 추후 연구 과제로 남아있다.

REFERENCES

[1] C. Bruner, U. Gallersdörfer, F. Knirsch & D. Engel, F. Matthes, (2020) DID and VC : Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. *en-trust*, 01-06. DOI : 10.1145/3446983.3446992

[2] Ministry of Science and ICT. (2021). *Digital Signature Act* (Online). https://law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%EC%A0%84%EC%9E%90%EC%84%9C%EB%AA%85%EB%B2%95&x=0&y=0#liBgcolor0

[3] A Mühle, A Grüner, T. Gayvoronskaya & C. Meinel. (2020) A survey on essential components of a self-sovereign identity, *Elsevier Computer Science Review. 30,* 80-85. DOI : 10.1016/j.cosrev.2018.10.002

[4] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan & K. K. R. Choo. (2020). Blockchain-based identity management systems : A review. *Journal of Network and Computer Applications. 166(102731).* 01-11. DOI : 10.1016/j.jnca.2020.102731

[5] A. Tobin & D. Reed. (2016). *The inevitable rise of self-sovereign identity*. The Sovrin Foundation.

[6] Q. Stokkink & J. Pouwelse. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, 1336-1342. DOI : 10.1109/Cybermatics_2018.2018.00230

[7] J. S. Kim. (2020). Research on the Use of Pseudonym Data - Focusing on Technical Processing Methods and Corporate Utilization Directions -. Journal of The Korea Institute of Information Security & Cryptography, 30(2), 253-262. DOI : 10.13089/JKIISC.2020.30.2.253

[8] Personal Information Protection Committee, (2020). *Enforcement Decree of the Personal Information Protection Act* (Online). https://law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95&x=0&y=0#liBgcolor0

[9] H. S. Lee & J. H. Song. (2016). *A Research on De-identification Technique for Personal Identifiable Information*. Seongnam : Software Policy Research Institute(SPRi).

[10] Council of the European Union. (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).*

[11] S. Wachter. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review. 103(1),* 5-8. DOI : 10.1016/j.clsr.2018.02.002

[12] G. Kondova & J. Erbguth. (2020). Self-sovereign identity on public blockchains and the GDPR. *35th Annual ACM Symposium on Applied Computing.* 342-345. DOI : 10.1145/3341105.3374066

[13] J. B. Lee. (2018). A study on the Implications of Japanese Personal Information Protection Legislation and Improvement of Korean Legislation in the GDPR Era. *KANGWON LAW REVIEW 55.* Chuncheon : Institute of Comparative Legal Studies. DOI : 10.18215/kwlr.2018.55..95

[14] P. Windley & D. Reed. (2018). *SOVRIN™ : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust.* The Sovrin Foundation.

[15] C. Lundvist, R. Heck, J. Torstensson, Z. Mitton & M. Sena. (2017). *Uport: A platform for self-sovereign identity draft version.* Delft : Blockchain Lab, 21 Feb, 2017.

[16] C. Fei, J. Lohkamp, E. Rusu, K. Szawan & K. Wangner, (2018). *Jolocom: Self-sovereign and decentralised identity by design.* White paper.

[17] J. Roos. (2018). *Identity Management on the Blockchain, Seminar Innovation Internet Technologies and Services Departments of Informatics.* Munich : Technical University of Munich.

[18] D. Reed, M. Sporny & M. Sabadello, (2020) *Decentralized Identifiers (DIDs) v1.0.* W3C Working Draft (Online). https://www.w3.org/TR/did-core/

[19] M. Sporny, G. Noble, D. Longley, D. C. Burnett & B. Zundel. (2019). *Verifiable Credential Data Model 1.0.* W3C Editor's Draft (Online). https://www.w3.org/TR/vc-data-model/

[20] S. Goldwasser, S. Micali & C. Rackoff. (1989). The Knowledge Complexity of Interactive Proof Systems, *SIAM Journal on computing 18(1).* 186-208. DOI : 10.1137/0218012

[21] M. Blum, P. Feldman & S. Micali. (2019). Non-interactive zero-knowledge and its applications. *Providing Sound Foundations for Cryptography: On the work of Shafi Goldwasser and Silvio Micali.* 329-349. DOI : 10.1145/3335741.3335757

[22] A. Gabizon. (2017). *Explaining SNARKs.*. ELECTRONIC COIN CO. (Online), https://electriccoin.co/?s=explaining%20SNARKs%20Part%20&is_v=1

[23] P. J. Windley. (2016) *How Sovrin Works*. The Sovrin Foundation. (Online). https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf.

[24] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos & S. Guerreiro. (2020). SSIBAC: Self-Sovereign Identity Based Access Control. *IEEE.* 01-09.
DOI : 10.5283/epub.44043

조 강 우(Kang-Woo Cho) [학생회원]

· 2020년 2월 : 부경대학교 정보통신공학과 (학사)
· 2020년 3월 ~ 현재 : 부경대학교 정보보호학과 석사과정
· 관심분야 : 개인정보보호, 블록체인, DID
· E-Mail : kwcho899@pukyong.ac.kr

전 미 현(Mi-Hyeon Jeon) [학생회원]

· 2021년 2월 : 부경대학교 IT융합응용공학과 (학사)
· 2021년 3월 ~ 현재 : 부경대학교 정보보호학과 석사과정
· 관심분야 : 블록체인, IoT, 클라우드
· E-Mail : jmh3850@pukyong.ac.kr

신 상 욱(Sang Uk Shin) [정회원]

· 1995년 2월 : 부경대학교 전자계산학과 (학사)
· 1997년 2월 : 부경대학교 전자계산학과 (석사)
· 2000년 2월 : 부경대학교 전자계산학과 (박사)
· 2000년 4월 ~ 2003년 8월 : 한국전자통신연구원 선임연구원
· 2003년 9월 ~ 현재 : 부경대학교 IT융합응용공학과 교수
· 관심분야 : 암호 프로토콜, 블록체인, 디지털 포렌식, IT융합보안
· E-Mail : shinsu@pknu.ac.kr