Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.981

GDPR 준수 가능한 블록체인 기반 접근제어 시스템

임 준 호,[1†] 천 지 영,[2] 노 건 태,[3] 정 익 래[4‡]
[1,4]고려대학교 (대학원생, 교수), [2]이화여자대학교 (교수), [3]서울사이버대학교 (교수)

GDPR Compliant Blockchain Based Access Control(GCBAC)

Joon Ho Lim,[1†] Ji Young Chun,[2] Geontae Noh,[3] Ik Rae Jeong[4‡]
[1,4]Korea University (Graduate student, Professor), [2]Ewha Womans University (Professor), [3]Seoul Cyber University (Professor)

요 약

블록체인 기술은 탈중앙화된(decentralized) 분산원장(distributed ledger)과 합의 기반 구조를 바탕으로 높은 보안 수준을 제공할 수 있다는 장점이 있다. 이와 같은 블록체인 기술의 활용도 증진을 위해서는 헬스 케어, 전자상거래 등 개인정보 처리가 필요한 분야에서의 활용 방안 모색이 필요하다. 이를 위해서는, 블록체인 기반 시스템에서도 유럽 연합(EU) 개인정보보호 규정(GDPR, General Data Protection Regulation)으로 대표되는 개인정보보호 관련 법규 및 규정을 준수할 수 있어야 한다. 그러나, 블록체인의 자체 특성상 기록된 자료에 대한 불변성과 탈중앙성 때문에 기존 개인정보보호 규정의 요구사항을 블록체인상에서 기술적으로 구현함에 어려움이 있다. 본 논문에서 우리는 카멜레온 해시(chameleon hash)와 속성 기반 암호화(Attribute Based Encryption, 이하 ABE)를 활용하여 GDPR에서 요구하는 개인정보 주체의 권리를 보장 가능한 다중 체인(multi-chain)기반 접근제어 시스템을 제시한다. 끝으로 우리의 시스템에서는 기밀성과 무결성을 유지한 가운데, 개인정보 처리가 가능함을 보안 분석을 통해 보인다.

ABSTRACT

Blockchain technology can provide a high level security based on a decentralized distributed ledger and consensus-based structure. In order to increase the utilization of blockchain technology, it is necessary to find a way to use it in fields that require personal data processing such as health care and e-commerce. To achieve this goal, the blockchain based system should be able to comply with data privacy regulations represented by European Union(EU)'s GDPR(General Data Protection Regulation). However, because of the properties of the blockchain like the immutability and decentralized recorded data, it is difficult to technically implement the requirements of the existing privacy regulations on the blockchain. In this paper, we propose a multi-chain based access control system that can guarantee the rights of the personal data subject required by GDPR by utilizing Chameleon Hash and Attribute Based Encryption (ABE). Finally, we will show through security analysis that our system can handle personal data while maintaining confidentiality and integrity.

Keywords: Blockchain, GDPR, Access Control, ABE(Attribute Based Encryption), Chameleon Hash, Smart Contract

I. 서 론

Satoshi Nakamoto의 Bitcoin[6]으로부터 최초 제기된 블록체인의 개념은 기존 중앙화된 시스템을 탈피하여, 시스템에 존재하는 각 노드별 분산 원장(distributed ledger)을 유지함으로써 탈중앙성,

Received(10. 07. 2020), Modified(11. 13. 2020), Accepted(11. 16. 2020)

† 주저자, pcrjh@korea.ac.kr
‡ 교신저자, irjeong@korea.ac.kr(Corresponding author)

데이터의 무결성 및 불변성을 확보할 수 있는 안전한 시스템 구축의 가능성을 보여주었다. 블록체인에서 새로운 데이터의 기록은 시스템 구성원의 합의(consensus)를 동반해야만 가능하기 때문에 독단적인 데이터 게재 및 수정은 불가하다는 보안상 장점을 가진다.

위와 같은 블록체인의 장점을 기존 또는 새롭게 파생된 산업 구조에 도입 및 활용하여 보안성을 강화시키기 위한 다양한 방안들이 제시 및 연구되었다. 대표적으로 거래 기록의 무결성이 중요시되는 전자상거래, 사물인터넷(Internet of Things, 이하 IoT) 기반의 헬스 케어[20], 스마트 시티[21] 등의 분야가 있다. 특히, 다양한 기기 및 센서로부터 수집된 데이터를 활용하는 IoT 네트워크 환경에서는 높은 보안 수준을 유지하기 위하여, 각 기기가 생성한 데이터에 대한 섬세한(fine-grained) 접근제어(access control)가 요구되는데, 블록체인을 기반으로 접근제어 체계를 구축하면 블록체인 자체의 특성으로부터 높은 신뢰성 및 가용성을 확보할 수 있다[14,18].

이처럼 다양한 분야에서 블록체인이 실질적으로 도입 및 활용되기 위해서는 단순 기술적 구현뿐 아니라, 기존 사회의 법규 및 규정을 준수할 수 있는 실제 활용 가능한 시스템 제시가 동반되어야 한다. 특히, 대다수의 분야가 헬스 케어나 스마트 시티 환경처럼 개인정보 처리를 포함하고 있기 때문에 블록체인의 향후 활용 가능성 증대를 위해서는 개인정보보호 규정을 준수 가능한 모델 제시가 반드시 필요하다.

대표적인 개인정보보호 규정에는 유럽연합(EU)의 개인정보보호 법령(General Data Protection Regulation, 이하 GDPR)이 있다[7]. GDPR은 개인정보 주체의 권리를 확보하고, 기업의 책임성 강화 및 개인정보보호 방안 수립 등을 위한 전반적인 내용을 다루고 있으며, 위반시 과징금 부가 등의 강력한 행정처분을 부가하고 있다[8,9].

그러나, 블록체인 자체의 특성과 개인정보보호 규정 간에는 충돌요소가 일부 존재하여 GDPR의 요구사항을 블록체인상에서 기술적으로 구현하는데 어려움을 겪고 있다. 예를 들어, 블록체인에 기록된 자료는 수정, 삭제가 불가하다는 무결성 및 불변성을 갖고 있는데, 이는 개인정보 주체가 요구하는 경우 기존에 저장된 개인정보 주체의 개인정보를 삭제할 수 있어야 한다는 GDPR 제17조 '삭제권' 조항과 충돌된다. 또한, GDPR 제18조 '처리제한권'에 의거 개인정보는 인가된 사용자만 접근, 처리할 수 있도록 기밀성(confidentiality)을 만족해야 하는데 블록체인상에 순수 개인정보를 기재하면 블록체인 구성원 모두에게 개인정보가 공개되기 때문에 개인정보보호 규정과 충돌을 야기할 수 있다.

위와 같은 문제를 블록체인상에서 해결하기 위한 다양한 연구[1,4,5,10,11,14]가 제시되었으나, 기존의 연구들은 카멜레온 해시(chameleon hash)[23]를 활용하여 블록체인상에서 '삭제권'을 구현할 수 있는 방안 연구[5,11]에 집중되었다. 때문에 GDPR의 요구사항을 포괄적으로 구현 가능한, 즉 정보 주체(data subject)의 권리를 전반적으로 보장할 수 있는 블록체인 시스템 제시 사례는 극히 드물다[10].

또한, 블록체인상의 데이터를 수정시 특정 구성원에 의존된 중앙화된 데이터 수정 구조를 갖거나[11, 14], 블록체인 외의 오프체인상에 존재하는 요소를 활용[10]함으로써, 블록체인 활용에 따른 탈중앙화된 시스템으로부터 얻게 되는 보안 이점을 상실할 수 있다는 한계를 보여주었다. 따라서, 앞으로 제시되는 블록체인 기반 개인정보 처리 시스템은 가능하면 블록체인 외적 구성요소에 대한 의존성을 최소화하여 블록체인 시스템의 탈중앙성을 유지하는 방안을 강구해야 한다.

본 논문에서 우리는 카멜레온 해시 및 속성 기반 암호화(Attribute Based Encryption, 이하 ABE)를 활용하여 GDPR에서 요구하는 정보 주체의 권리를 온전히 보장할 수 있는 다중 블록체인(multi-chain) 기반 접근제어 시스템을 제시한다. 우리의 시스템은 Li, Jiguo의 ABE 기법[3]을 활용하여 정보 주체의 개인정보에 대한 처리제한권(GDPR 제18조)을 구현함과 동시에, 컨트롤러(Data Controller)라는 신규 블록체인 노드 개념을 추가하여, 블록체인상에 게재된 데이터의 접근 권한 수정이 필요한 경우, DC 노드들에 의한 합의 과정을 요구함으로써, 블록체인 외부 요소의 개입을 최소화하였다. 끝으로, 우리의 시스템은 블록체인 활용에 따른 무결성을 유지한 가운데, 개인정보 처리가 가능함을 보안 분석을 통해 보인다.

II. 배경 지식

2.1 블록체인(Blockchain)

블록체인은 거래(transaction)라는 일련의 데이터를 블록에 담아 해시 연산 기반의 체인 형태로 연결하여 구성원들간에 동일한 원장을 저장 및 유지하는 데이터 저장 기술이다. 따라서, 블록체인상에 등재된 데이터는 모두에게 공개되어 검증 가능성과 투명성을 갖고 있으며, 블록체인 내 데이터를 수정하려면 기존 블록들의 연결성을 유지하는 해시 성질을 깨야하기 때문에 일반적으로 무결성을 유지할 수 있다(예외적으로, 수정 가능한 블록체인 구조에서는 통제된 환경에서 블록 내용 수정이 가능하다. 2.5 참고). 또한, 블록체인상에 데이터를 게재하려면 기존 노드들에게 검증을 받고, 정의된 합의 프로토콜(consensus protocol)을 충족시켜야하기 때문에 악의적인 일부 사용자의 부정당한 행위는 시스템 구성원 모두에게 감지 및 예방될 수 있다.

블록체인은 네트워크의 개방성에 따라 Bitcoin[6]이나 Ethereum[12]과 같은 누구나 시스템에 참여 가능한 퍼블릭(public) 블록체인과 사전에 허가된(permissioned) 사용자만 접근 가능한 프라이빗(private) 블록체인, 그리고 중간 형태의 Hyperledger Fabric(HLF)[13]과 같은 다수의 조직이 참여하는 컨소시엄(consortium)블록체인이 있다. 본 논문에서 우리는 퍼블릭 블록체인과 컨소시엄 블록체인에 한정하여 기술하기로 한다.

2.1.1 스마트 컨트랙트(Smart Contract)

스마트 컨트랙트는 블록체인 시스템에서 가동되는 탈중앙화된 프로그램이다. 튜링 완전성(turing-complete)을 만족하는 프로그래밍 언어로 작성된 스마트 컨트랙트는 블록체인 분산원장 내에서 사용자가 생성한 거래로부터 항상 동일한 결과값을 산출하는 결정론적인(deterministic) 특성을 갖고 있다. 이를 활용하면 블록체인상에서 사용자간 합의를 이행할 수 있으며, 처리된 합의 내용은 분산원장에 기록되어 블록체인 구성원 모두에게 공개되기 때문에, 구성원 모두로부터 검증받을 수 있다(auditability).

2.2 GDPR

2018년 5월 25일부로 법적 효력을 갖게된 유럽연합(EU)의 GDPR은 위반시 과징금 등 강력한 행정처분이 부과 가능하며, 유럽을 대상으로 사업을 하는 경우에도 법령 적용 대상이 될 수 있다. GDPR의 3가지 역할군은 다음과 같다.

- **정보 주체(Data Subject, DS)** : 생산된 개인정보의 소유자
- **컨트롤러(Data Controller, DC)** : 개인정보 처리의 목적 및 방법을 결정하며, 정보 주체의 개인정보가 적법하고, 공정하며, 투명하게 처리되도록 관리 및 입증할 책임을 가진다.
- **프로세서(Data Processor, DP)** : 컨트롤러를 대신하여 지정된 개인정보 처리방법에 의거하여 개인정보를 처리한다.

또한, GDPR에서 정보 주체의 권리를 보장하기 위하여 기술적 구현이 요구되는 핵심 조항을 정리하면 아래 6가지와 같다.

- **정보 주체의 동의(consent)** : 개인정보 처리는 정보 주체의 동의를 획득한 경우에만 적법하다(제6조 1항).
- **정정권** : 정보 주체는 부정확한 개인정보를 정정하도록 컨트롤러에게 요청할 권리를 가진다(제16조).
- **삭제권** : 정보 주체는 개인정보를 삭제하도록 컨트롤러에게 요청할 권리를 가지며, 컨트롤러는 지체없이 삭제할 의무를 가진다(제17조). 또한, 국내 개인정보 보호법 제21조에서는 정보 보유기간이 경과하거나 처리 목적이 달성된 개인정보는 파기하도록 정하고 있다.
- **처리 제한권** : 정보 주체는 컨트롤러에게 개인정보 이용 제한을 요청할 수 있다(제18조).
- **설계 및 기본설정에 의한 개인정보보호** : 컨트롤러는 정보 주체의 권리를 보호하기 위해, 개인정보 보호 원칙을 효율적으로 이행하도록 기술 및 관리적 조치를 강구해야 한다(제25조).
- **처리활동의 기록** : 컨트롤러 또는 프로세서가 진행한 처리활동의 기록을 보존해야 한다(제30조).

2.3 카멜레온 해시

일반적인 암호학적 해시는 충돌 저항성(collision resistance)을 만족한다. 카멜레온 해시는 충돌 저항성을 만족하면서도 트랩도어를 알고 있는 정당한 사용자가 입력 충돌쌍을 쉽게 찾을 수 있다는 추가적인 성질을 가진다.

본 논문에서 우리는 키 노출 문제(key exposure problem)에 안전한 카멜레온 해시[23]를 사용하며, 다음 4개의 알고리즘으로 구성된다.

1) CH.KeyGen(k) : 보안 상수 k를 입력받아 공개 파라미터 hk와 트랩도어 tk를 생성한다.

2) CH.Hash(hk,m,r) : 공개 파라미터 hk, 메시지 m, 난수 r을 입력받아 해시 값 $CH_{m,r}$을 생성한다.

3) CH.Ver(hk,m,r,$CH_{m,r}$) : 공개 파라미터 hk와 메시지 m, 난수 r, 해시 값 $CH_{m,r}$을 입력받아 CH.Hash(hk,m,r)=$CH_{m,r}$을 만족하면 True, 그렇지 않으면 False를 출력한다.

4) CH.Col(tk,m,r,$CH_{m,r}$,m′) : 트랩도어 tk, 메시지 m, 난수 r, 해시 값 $CH_{m,r}$, 새로운 메시지 m'을 입력받아 CH.Hash(hk,m,r) = CH.hash(hk,m′,r′)을 만족하는 r'을 출력한다.

2.4 속성 기반 암호화(Attribute-based Encryption, ABE)

ABE는 속성(attribute) 집합과 접근 구조(access structure)를 사용하여 암호 기법에 접근 제어를 결합한 암호시스템이다. ABE는 속성 집합과 접근 구조를 어디에 부여하는지에 따라 비밀키 정책 ABE(Key-Policy ABE, 이하 KP-ABE)와 암호문 정책 ABE(Ciphertext-Policy ABE, 이하 CP-ABE)[17]로 나뉜다. KP-ABE는 비밀키에 접근 정책이, 그리고 암호문에 속성 집합이 부여되고, CP-ABE는 비밀키에 속성 집합이, 그리고 암호문에 접근 정책이 부여된다. CP-ABE의 경우 암호화를 하는 사용자가 암호문에 접근 정책을 부여하여 암호화를 하면, 이 정책에 부합하는 속성 집합을 포함한 비밀키를 가진 사용자만이 암호문을 복호화할 수 있다. 본 논문에서 우리는 GDPR의 정보 주체가 실시간 생성하는 개인정보 데이터에 권한이 있는 프로세서만 접근하여 사용할 수 있도록 CP-ABE를 활용하여 접근제어 시스템을 구성한다. CP-ABE는 다음 4개의 알고리즘으로 구성된다.

1) ABE_SystemSetup(γ) : 시스템 파라미터 γ를 입력 받아 TA의 마스터키 MK와 공개키 PK를 생성한다.

2) ABE_KeyGen(MK,S_j) : TA의 마스터키 MK와 j번째 사용자의 속성 집합 S_j를 입력받아 j번째 사용자의 비밀키 SK_j를 생성한다.

3) ABE_Encrypt(PK,M,A) : 공개키 PK, 메시지 M, 접근 정책A를 입력받아 암호문 CT를 생성한다.

4) ABE_Decrypt(SK_j,CT) : j번째 사용자의 비밀키SK_j와 암호문 CT를 입력받아 메시지 M을 얻는다.

본 논문에서는 개인정보와 접근 정책 업데이트를 위해 Jiguo Li의 CP-ABE[3]를 활용하여 시스템을 구성한다. Jiguo Li의 CP-ABE[3]에서는 AM(Attribute Manager)이라는 시스템 구성원을 포함하여 암호문 생성시 해당 속성을 만족하는 그룹 값이 포함된 그룹키로 암호화하는 과정을 추가하였다. 위 구조 덕분에 Jiguo Li의 CP-ABE[3]에서 사용자의 비밀키 철회 과정은 TA(Trusted Authority)의 개입 없이 AM만으로 수행 가능하다.

본 논문에서는 사전에 지정된 블록체인 노드(DC)에게 AM 기능을 수행하도록 설계함으로써, 개인정보 처리시 TA라는 중앙화된 요소의 도움 없이 블록체인 시스템 구성요소만으로 운용되도록 설계하였다(4.5 세부절차 참조). Jiguo Li의 CP-ABE는 다음 5개의 알고리즘으로 구성된다.

1) ABE_SystemSetup(γ) : 시스템 파라미터 γ를 입력받아 TA는 공개 파라미터 PP와 TA의 마스터키 MK를 생성한다. AM들은 합의 과정을 동반하여 AM의 마스터키 MMK와 공개키 PK를 생성한다.

2) ABE_KeyGen(PP,MK,MMK,PK,S_j) : 공개 파라미터 PP, TA와 AM의 마스터 키 (MK,MMK), 공개키 PK, j번째 사용자가 만족하는 속성 집합 S_j를 입력받아 j번째 사용자의 비밀키

SK_j를 생성한다.

3) ABE_Encrypt(PK,M,A) : 공개키 PK, 메시지 M, 접근 정책A를 입력받아 암호문 CT를 생성한다.

4) ABE_Decrypt(CT, SK_j) : 암호문 CT, j번째 사용자의 비밀키 SK_j를 입력받아 메시지 M을 얻는다.

5) ABE_Revoke(V_j,MMK,PK,SK_{V_j},CT_{V_j}) : j번째 사용자의 철회되는 속성 값 V_j, AM의 마스터키MMK, 공개키 PK, 철회되는 속성 값 V_j를 만족하는 사용자들의 비밀키 SK_{V_j} , 속성 V_j와 관련된 암호문 CT_{V_j}를 입력받아 수정된 DC의 마스터키 MMK', 수정된 공개키 PK', 수정된 비밀키 SK_{V_j}', 수정된 암호문 CT_{V_j}'로 업데이트한다.

본 논문의 시스템에서 ABE_Encrypt()과정을 제외한 DC가 참여하는 모든 과정에서는 단일 DC에 의한 독단적 역할 수행이 불가하며, 반드시 합의 과정이 동반되어야 한다.

2.5 수정 가능한 블록체인 (Redactable Blockchain)

수정 가능한 블록체인은 블록체인에 올라간 데이터를 권한이 있는 집단들의 합의를 통해 수정할 수 있는 구조로 되어 있으며, 기존의 해시 함수 대신 카멜레온 해시를 활용하여 블록을 구성하는 방식으로 이루어져 있다[11]. 카멜레온 해시 기반의 수정 가능한 블록체인의 각 블록은 Fig.1과 같은 구조를 가진다.

Fig.1의 예시처럼 블록의 거래내용이 업데이트 되더라도 해당 블록의 거래에 대한 해시 값은 카멜레온 해시 함수를 사용하기 때문에 변하지 않도록 구성할 수 있다. 트랩도어를 가진 권한이 있는 사용자가 트랩도어를 이용하여 변경된 거래내용에 대한 난수

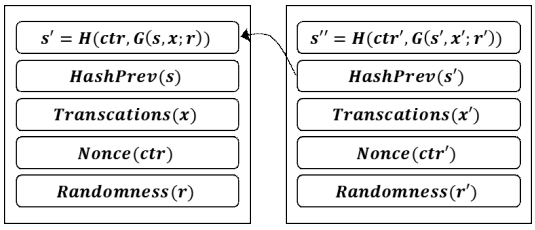

Fig. 1. The structure of redactable blockchain

값을 조정함으로써 해시 값을 그대로 유지할 수 있게 된다. 따라서 블록 간 연결성을 유지한 가운데 블록체인 내용을 업데이트할 수 있다.

본 논문에서 사용되는 Key-chain과 Data-chain(4.4 참조)은 개인정보와 접근 정책 업데이트를 위해 카멜레온 해시 기반의 수정 가능한 블록체인 구조를 이용한다.

III. 관련연구

블록체인상에서 개인정보를 처리하기 위하여 다양한 해결방안이 제시되었다. Giuseppe Ateniese 등[11]은 카멜레온 해시를 활용하여 블록체인 블록을 구성함으로써 필요시 내용을 수정, 삭제 가능한 블록체인 구조를 제시하여 GDPR 제17조 '삭제권'을 블록체인상에서 구현할 수 있는 가능성을 제시하였다. 이후 Kondapally Ashritha 등[5]은 비밀공유 기법(secret-sharing)을 활용하여 카멜레온 해시 트랩도어 값이 노출되는 문제를 해결하고자 하였으나, 블록체인상에 게재된 개인정보에 누구나 접근 가능하기 때문에 개인정보의 접근제어와 개인정보 이용에 따른 사전 동의 획득 방안을 제시하지 못한다.

Wirth Christian 등[1]과 Nguyen Binh Truong 등[10]은 블록체인의 스마트 컨트랙트를 활용한 개인정보 주체의 동의 획득 방안을 제시하였다. 그러나, Wirth Christian 등[1]의 기법은 개인정보 또는 인증서를 공개된 블록체인상에서 전달하기 때문에 정보유출(data leakage)의 위험성이 존재하며, [10]에서는 개인정보를 별도 보관하는 외부 자원 서버(resource server)라는 블록체인 외부 영역에 개인정보를 저장시킴으로써 위탁받은 개인정보의 무결성, 신뢰성 문제를 발생시킬 수 있다. [1]과 [10]은 공통적으로 블록체인 외부 요소가 시스템에 포함되어 블록체인 시스템 활용에 따른 탈중앙성에 기반한 보안 이점을 경감시킬 수 있다는 한계를 보여주었다.

한세진 등[4]과 Guangsheng Yu 등[14]은 ABE를 활용하여 블록체인상에 게재된 정보에 대한 접근제어를 구현하였다. 그러나, GDPR의 프로세서가 블록체인에 기록된 개인정보를 활용하였다는 사용내역 또는 정보 주체로부터의 동의 사실을 기록으로 남길 수 없어, 위·변조 불가한 GDPR 제30조(처리활동의 기록)를 만족하는 감사 기록을 생성할 수 없다는 한계를 보여주었다.

Table 1. GDPR-Compliance comparison related to blockchain based personal data treating system

	[11]	[5]	[1]	[10]	[4], [15]	Our Protocol
Art.6	X	X	○	○	X	○
Art.16	○	○	X	△	X	○
Art.17	○	○	X	△	X	○
Art.18	X	X	X	○	○	○
Art.25	X	X	○	○	○	○
Access Control	X	X	○	○	○	○

GDPR 구현 관점에서 관련연구를 비교하면 Table 1과 같으며 GDPR상에서 정보 주체의 권리를 대변하는 조항들을 전반적으로 준수 가능한 시스템 연구는 부재함을 알 수 있다. 또한, [10]의 경우 GDPR의 요건을 충족할 수 있으나, 블록체인 구성요소가 아닌 외부요소를 포함시킴으로써 블록체인의 탈중앙성을 저하시키는 것을 확인할 수 있다. 본 논문에서 우리는 블록체인 외부요소의 개입을 최소화시킨 가운데, GDPR관련 핵심조항을 기술적으로 구현 가능한 시스템을 제시한다.

IV. 시나리오

Ⅳ장에서는 개인정보 인증, 처리, 인가를 다루는 실제 시스템 시나리오를 제시하고, GDPR의 요구사항을 기술적으로 구현함에 있어 발생 가능한 문제점들에 대하여 설명한다.

4.1 기존 시나리오

현재 개인정보를 취급하는 대다수의 서비스들은 OAuth 2.0 표준[15]을 준수하여 API(또는 서비스)의 인증 및 개인정보 처리 권한을 부여하고 있다. OAuth 2.0의 개인정보 처리 과정(Fig.2)에서 등장하는 역할군은 다음과 같다.

- **Resource Owner** : 생산된 개인정보의 소유자(end-user) 또는 객체(entity)이며, 개인정보 처리를 원하는 Client에게 Resource Server에 저장된 본인의 개인정보에 접근을 허가할 수 있다(GDPR의 정보 주체에 해당).
- **Client** : 개인정보를 취급하는 API 또는 서비스로 Resource Owner로부터 개인정보 사용 허가를 사전에 획득해야 한다(GDPR의 프로세서에 해당).
- **Resource Server** : 개인정보 저장 서버
- **Authorization Server** : Client를 대신하여 개인정보 처리 인가 업무를 수행한다. Resource Owner로부터 인증받은 Client에게 Access Token을 발급한다. (개인정보 처리 유무에 따라 GDPR의 컨트롤러 또는 프로세서에 해당).

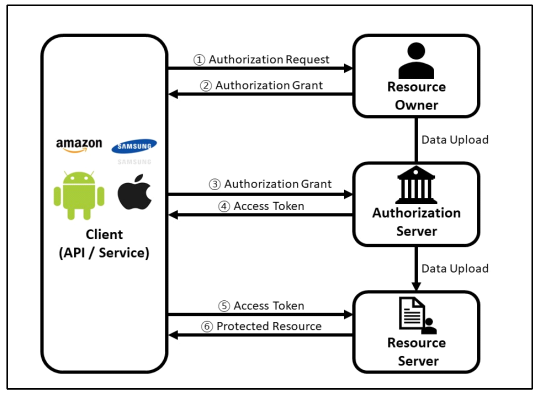

Fig. 2. Personal data flow in OAuth 2.0

Samsung Payment와 같은 금융 결제 서비스를 예시로 들면 세부절차는 다음과 같다. 고객의 거래 내용(개인정보)을 기반으로 서비스를 제공하는 신용카드 업체 A(Client)는 Samsung Payment 사용 고객(Resource Owner)으로부터 ① 거래내역(개인정보)을 조회 및 처리할 수 있는 권한을 요구한다. ② 개인정보 처리 승인 권한을 획득한 Client는 Samsung Payment 서비스 제공자(Authorization Server)에게 ③ Access Token 발급을 요구한다. ④ Client의 인증 정보를 확인한 Authorization Server는 Client에게 Access Token을 발급하고, ⑤⑥ Client는 Access Token을 활용하여 거래내역 DB(Resource Server)에 접근하여 개인정보를 처리한다.

4.2 당면과제(Challenge)

4.1에서 제시한 OAuth 2.0 표준은 권한 위임(delegation), 인증, 인가 및 접근통제 기능을 구

현할 수 있으나, Authorization Server라는 중앙화된(centralized) 요소를 활용함에 따라 GDPR의 관점에서 다음과 같은 문제를 야기할 수 있다[22]. 첫째, Authorization Server는 Access Token 발급 업무 수행 시 Resource Owner가 요구하는 조건대로 GDPR의 컨트롤러로서의 역할을 수행해야 한다. 그러나 악의적인 Authorization Server는 Client의 요구에 반하는 비인가 Access Token을 Client에게 발급하여 개인정보 유출 문제를 발생시킬 수 있다. 또한, 위 구조에서 Client는 단순 처리 결과를 신뢰할 수밖에 없기 때문에, 개인정보의 적법한 처리에 대한 투명성(transparency) 및 검증(auditability) 문제가 발생할 수 있다. 둘째, Authorization Server는 Client의 요구대로 적법하게 개인정보를 처리하였음을 Client 또는 감사기관에 항상 입증할 수 있어야 한다(GDPR 제30조). 따라서 Authorization Server는 위·변조 불가한 처리 기록을 생성 및 유지할 수 있는 능력을 구비해야 한다.

4.3 제안 시스템 Overview

본 논문에서 우리는 블록체인 기반 접근제어 시스템을 활용하여 4.2에서 언급한 문제의 해결방안을 제시한다. 정보 주체의 개인정보와 이를 열람하기 위한 키 값은 각각 Data-chain과 Key-chain이라는 서로 다른 블록체인 분산원장에 기록된다. High-level 관점에서 개인정보 처리 구조는 다음과 같다(Fig.3).

- **(준비단계)** : ① TA(Trust Authority)와 컨트롤러(DC)는 시스템 내 모든 프로세서(DP)에게 사용자별 만족하는 속성(attribute)을 고려하여 ABE 비밀키 값을 생성하여 부여한다.
- **(개인정보 업로드)** : ② 정보 주체(DS)는 DC의 도움을 받아 본인의 암호화된 개인정보를 Data-chain에, 개인정보 암호화에 사용된 키 값(CK)을 속성 기반 암호화하여 Key-chain에 업로드한다. 이때, 속성 기반 암호화에는 DS가 원하는 접근 정책(access policy)이 포함된다.
  ③ DS가 속성 기반 암호화에 포함시킨 접근 정책을 만족하는 DP는 부여받은 ABE 비밀키를 활용하여 Key-chain상의 속성 기반 암호화된 CK을 복호화하여 획득한다. ④ DP는 획득한 CK을 활용하여 Data-chain의 암호화된 개인정보를 복호화하여 획득한다.

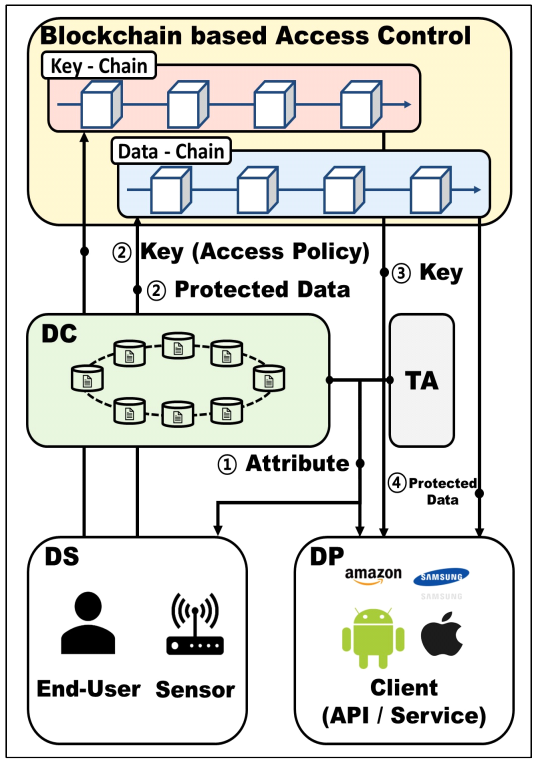

Fig. 3. High-level personal data flow in blockchain based access control system

본 논문의 시스템은 4.2에서 설명한 기존 개인정보 처리 시스템에서 발생 가능한 보안문제를 해결 가능하다. DS의 개인정보는 DS가 원하는 접근 정책이 설정되어 DC에 의해 거래 형태로 변환되어 블록체인상에 게재된다. 따라서 DC가 생성한 모든 결과값은 구성원 모두에게 공개되어 검증받을 수 있기 때문에 악의적인 위·변조 행위나 잘못된 개인정보 접근 인가행위를 방지할 수 있다. 또한, DC는 블록체인상에 게재된 값들을 근거로 DS의 요구대로 개인정보를 적법하게 처리하였음을 DS 또는 감사기관에 입증할 적법한 근거를 확보할 수 있다(GDPR 제30조).

4.4 세부 시스템 설명

본 논문의 시스템은 [14]와 같이 Key-chain과 Data-chain라는 두개의 블록체인 분산원장을 운용

하여 개인정보(데이터)와 개인정보 접근 정책 및 로그 기록을 분리하여 관리한다.

- **Key-chain** : Key-chain은 퍼블릭 또는 HLF[13]와 같은 컨소시엄 블록체인 형태로 구현 가능하다. Key-chain에서는 Ethereum[12]의 스마트 컨트랙트(HLF[13]의 체인코드)와 4.5에서 설명한 수정 가능한 블록을 게재할 수 있다. Key-chain에는 Data-chain에 기록된 개인정보를 획득할 수 있는 권한과 개인정보 요청 및 처리 로그가 기록된다. 개인정보 획득 권한은 속성 기반 암호화된 CK와 $Token$형태로 구현되며, 개인정보 요청 및 처리 로그는 DS의 스마트 컨트랙트(Add_{DS})에 대한 입·출력 거래 형태로 기록된다.
- **Data-chain** : 실제 암호화된 개인정보가 저장되는 공간으로, 컨소시엄 블록체인 형태로 구성된다. GDPR 제17조 '삭제권'을 '절대적 삭제' 개념으로 해석하여 수정 가능한 블록체인 구조를 활용한다. 만일 DS가 개인정보 삭제 또는 정정을 요청하는 경우, DC들에 의한 합의 프로토콜을 동반하여 Data-chain상의 내용을 삭제 또는 수정한다.

시스템에 등장하는 역할군은 GDPR에 명시된 역할군(DS, DC, DP)을 포함하여 다음과 같다. DS와 DC간 통신은 안전하다고 가정한다.

- **정보 주체(DS)** : 개인정보 주체로서 본인을 대변하는 스마트폰 또는 개인정보를 수집하는 의료센서와 같은 센서 형태로 구현된다. DC노드를 활용하여 개인정보를 블록체인상에 게재하고, 접근 정책 설정, 개인정보 삭제/수정 의뢰가 가능하다.
- **컨트롤러(DC)** : DS와 사전 계약 관계를 바탕으로 개인정보를 대신 처리하는 존재로 기업 자체 또는 서비스로 구현된다. 각 DC는 블록체인 시스템에서 TA에 의해 사전 지정된 노드 형태로 구현되며, 고연산 수행 능력(high computing power)을 지닌다. DC 상호간에는 합의를 수행하기 위한 비밀 채널(secure-channel)이 구성되어 있다고 전제한다. DS를 대신하여 암호화된 개인정보 게재, 접근제어 설정, 개인정보 또는 접근제어 조건 변경(ABE 속성 값 변경)업무를 수행한다.
- **프로세서(DP)** : 자체 개인정보 수집 및 관리 능력이 없는 기업 또는 서비스로 구현된다. DC에서 관리중인 DS의 개인정보 처리 접근 정책을 만족하면 DS의 동의하에 개인정보를 획득할 수 있다.
- **TA** : 가장 높은 보안수준(the highest security level)을 가진 존재로써 시스템 구성원의 인증, 속성 관리, 시스템 감사를 담당한다. 최초 준비단계에서는 DC와 연계하여 ABE 키 값을 생성한다. 시스템 내 모든 구성원의 신원을 알고 있으며, 블록체인 기록을 바탕으로 부정행위 발생 유무를 감시하는 감사기관으로서의 역할을 수행한다.
- **Miner** : 본 시스템에서 Miner는 악의적 행위로부터 안전한 Key-chain 유지를 담당한다. DS의 요청으로 DC가 생성한 거래를 작업증명(proof-of-work), 지분증명(proof-of-stake)과

Table 2. Notation

Notation	
M	• Message
PP	• ABE public parameter
γ	• ABE system parameter
MK	• ABE TA's master key
MMK	• DC's manager master key
PK/SK_j	• ABE public key/j'th DP's private key
PK_B/SK_B	• Public/Private key pair used in blockchain
S / S_j	• Attribute set / DP j's attribute set
att_i	• i'th attribute ($\in S$)
A / A_s	• Access policy / Access policy with secret value s
k	• Chameleon hash security parameter
hk_K/hk_D	• Chameleon hash key of Key-chain / Data-chain
tk_K/tk_D	• Chameleon trap-door of Key-chain / Data-chain
CK	• Conversation key to encrypt M
$Token$	• The key to encrypt M with CK
CT	• ABE ciphertext of a conversation key
CT_x	• ABE ciphertext containing attribute x
$\mathbb{CT}$	• Ciphertext of M
$I_{(x,y)}$	• Index of a transaction located in x'th block, y'th transaction
$t_{(i,j)}$	• i'th block's j'th transaction
Add_{DS}	• DS's smart contract address
r	• Random number for Chameleon hash
V_j	• j'th DP's revocated attributes
Enc/Dec	• Symmetric encryption / decryption
$Encrypt/Decrypt$	• Public key encryption / decryption

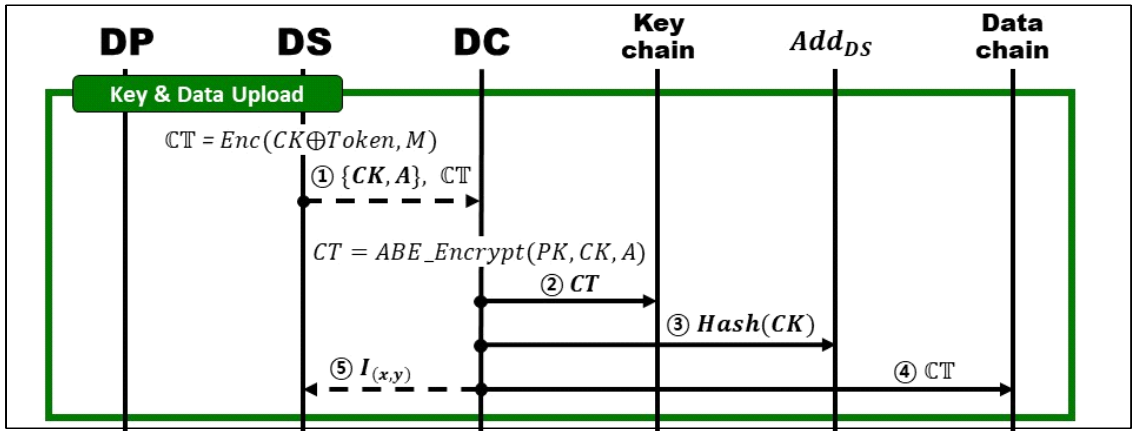

Fig. 4. Sequence diagram of data upload phase

같은 합의 프로토콜에 기반하여 블록을 생성한다.

4.5 세부절차

본 논문 시스템의 세부과정은 크게 최초 준비과정, 개인정보가 유통 및 처리되는 개인정보 업로드·수신 과정, 블록체인상에 기록된 개인정보 및 접근정책 업데이트 과정까지 총 3가지 과정으로 이루어진다. 이때, 블록체인을 기반으로 소통하는 과정은 $Append()$를 통하여 이루어진다. $Append()$란 블록체인 거래를 생성하여 기록하는 과정으로, $Append(M)$은 M이 포함된 블록체인 거래를 생성하여 Key-chain 또는 Data-chain상에 기록하는 과정을 의미한다.

4.5.1 최초 준비과정

최초 준비과정은 Fig.5와 같이 진행되며 세부설명은 다음과 같다.

최초 시스템의 구성은 TA에 의하여 시작된다. TA는 $Systemsetup()$을 통하여 DC가 속성 기반 암호화를 수행할 수 있도록 지원한다. ① TA가 시스템 가입을 희망하는 DP를 검증 후, DP별 속성(att_i)을 고려하여 DC가 속성 기반 비밀키를 생성할 수 있도록 SK_j'을 생성하여 DC들에게 전달한다. ② SK_j'을 전달받은 DC들은 DC간 비밀 채널을 활용하여 각 사용자별 속성 기반 비밀키(SK_j)를 합의에 기반하여 생성 후, 각 DP에게 전달한다.

DC간 합의 과정은 다양한 규칙 준수가 가능하나, 본 논문에서는 HLF의 PBFT(Practical Byzantine Fault Tolerance)[24]을 활용하여 Fig.6과 같이 합의를 도출한다. PBFT에서는 시스템에 참여하는 총 노드의 수가 n개라 할 때, $(n-1)/3$개 이하의 노드가 악의적인 행위를 하더라도 합의를 도출할 수 있다.

Algorithm 1 : Initialization Phase

▷ **Define :** $\Leftarrow$ // Secure channel

▷ **ABE.Initialization**

1 $(PP, MK) \leftarrow TA.ABE\_Systemsetup(\gamma)$;
2 $TA.Broadcast(PP)$;
3 $(MMK, PK) \leftarrow DC.ABE\_Systemsetup()$;
4 $DC.Broadcast(PK)$;
5 $\{SK_j'\} \leftarrow TA.ABE\_KeyGen(PP, MK, S_j)$;
6 $DC \Leftarrow TA.Send(SK_j')$; // ①
7 $SK_j \leftarrow DC.ABE\_KeyGen(SK_j')$; // ②
8 $DP \Leftarrow DC.Send(SK_j)$;

Fig. 5. Algorithm 1 : Initialization Phase

4.5.2 개인정보 업로드·수신

DS는 본인의 개인정보 처리를 허락한 DC를 통하여 개인정보를 업로드하고, DP는 DS에게 본인이 개인정보를 처리할 조건을 만족함을 증명하고, DS의 동의를 획득함으로써 개인정보를 처리할 수 있다(세부절차 Fig.4,7,8). 각 DS는 사전에 Key-chain에 본인의 스마트 컨트랙트(Add_{DS})를 등록하여 DP의 개인정보 활용 요청 메시지와 이에

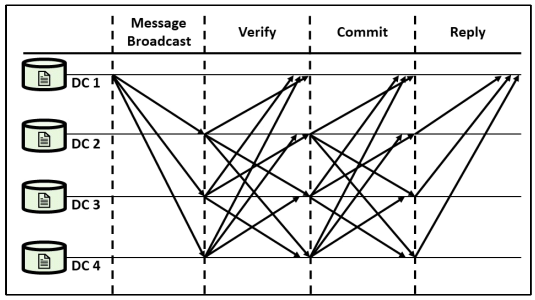

Fig. 6. PBFT Consensus procedure among DC

대한 처리 결과를 Key-chain에 기록한다. 세부절차(Fig.8)는 다음과 같다.

- **개인정보 업로드** : ① DS는 본인의 개인정보(M)를 ($CK \oplus Token$)을 키 값으로 활용하여 대칭키 암호문($\mathbb{CT}$)을 생성한다. ② DS는 CK를 원하는 접근 정책(A)와 $\mathbb{CT}$를 포함하여 사전 계약된 DC에게 전달한다. ③ DC는 DS의 요구대로 속성 기반 암호문(CT)을 생성한다. ④ DC는 속성 기반 암호문(CT)을 Key-chain에, ⑤ $Hash(CK)$를 DS의 스마트 컨트랙트(Add_{DS})에, ⑥ 암호화된 개인정보($\mathbb{CT}$)를 Data-chain에 기재한다. ⑦ DC는 Data-chain상에 $\mathbb{CT}$가 업로드된 위치 정보($I_{(x,y)}$)를 DS에게 알려준다. 이때, DC는 DS의 요구에 따라 개인정보를 처리할 의무가 있으며, 개인정보 처리 기록이 모두 블록체인에 기록되기 때문에 DC의 악의적 행위를 방지하고, DC의 개인정보 처리 내역을 공개 감사 및 검증할 수 있다.
- **개인정보 수신** : ⑧ DP는 본인의 속성 기반 비밀키(SK_j)를 활용하여 Key-chain상에 등재된 CT를 복호화하여 CK를 획득한다. ⑨ DP는 DS의

Algorithm 2 : Data Upload & Retrieve Phase

▷ **Data Upload**

1 $(CK, Token) \leftarrow DS.Generate(\ )$;
2 $\mathbb{CT} \leftarrow DS.Enc(CK \oplus Token, M)$; // ①
4 $DC \Leftarrow DS.Send(\{CK, A\}, \mathbb{CT})$; // ②
5 $CT \leftarrow DC.ABE\_Encrypt(PK, CK, A)$; // ③
6 $Key\ chain \leftarrow DC.Append(CT)$; // ④
7 $Add_{DS} \leftarrow DC.Append(Hash(CK))$; // ⑤
8 $Data\ chain \leftarrow DC.Append(\mathbb{CT})$; // ⑥
9 $DS \leftarrow DC.Send(I_{(x,y)})$; // ⑦

▷ **Data Retrieve**

10 $CK \leftarrow DP.ABE\_Decrypt(SK_j, CT)$; // ⑧
11 $Add_{DS} \leftarrow DP.Append((Hash(CK), PK_B)$; // ⑨
12 $CT' \leftarrow DS.Encrypt(PK_B, Token)$; // ⑩
13 $DP \leftarrow DS.Append(CT', I_{(x,y)})$; // ⑪
14 $Token \leftarrow DP.Decrypt(SK_B, CT')$; // ⑫
15 $M \leftarrow DP.Dec(CK \oplus Token, \mathbb{CT})$; // ⑬

Fig. 8. Algorithm 2 : Upload & Retrieve Phase

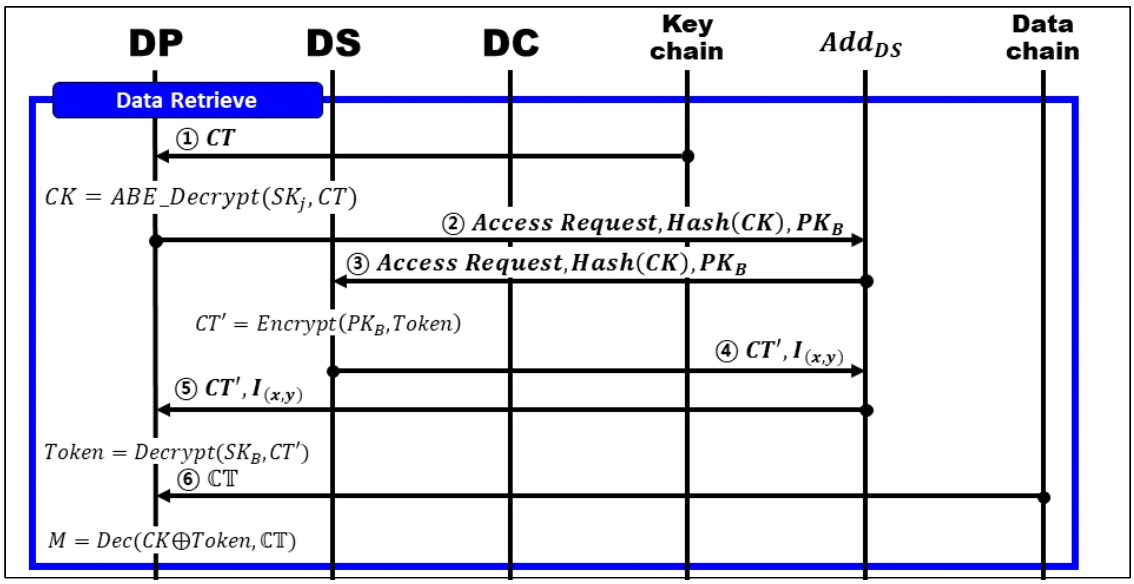

Fig. 7. Sequence diagram of data retrieve phase

스마트 컨트랙트(Add_{DS})를 경유하여 DS에게 $Hash(CK)$와 Key-chain에서 사용하는 DP 본인의 공개키 PK_B를 포함하여 개인정보 처리 요청(request message)을 거래 형태로 발송한다. ⑩ DP의 요청을 동의한 DS는 수신받은 PK_B로 $Token$을 암호화(CT')하고, ⑪ $I_{(x,y)}$와 함께 Add_{DS}을 경유하여 DP에게 전달한다. ⑫ DP는 본인의 개인키 SK_B로 전달받은 값을 복호화하여 $Token$을 획득한다. ⑬ 이후, DP는 Data-chain 상에서 $I_{(x,y)}$을 바탕으로 암호화된 개인정보 $\mathbb{CT}$를 찾아 ($CK \oplus Token$)으로 복호화하여 M을 획득한다.

4.5.3 개인정보, 접근 정책 업데이트

본 논문 시스템에서는 개인정보 및 접근 정책의 업데이트를 위하여 Key-chain과 Data-chain 모두 카멜레온 해시 연산 기반의 수정 가능한 블록체인 구조를 사용한다. Fig.10과 같이 Key-chain에는 CK를 속성 기반 암호화한 CT가, Data-chain에는 CK와 $Token$으로 암호화된 개인정보 $\mathbb{CT}$가 기록된다. 각 블록에 포함된 거래는 난수 r과 카멜레온 해시 연산 결과값이 같이 저장되며, 만일 DC에 의한 해시 충돌쌍 계산이 필요한 경우, DC들은 수정이 필요한 거래를 찾아서 $CH.Col(\,)$연산을 통하여 수정된 기록에 대응하는 난수 값을 계산할 수 있다. 이때, $CH.Col(\,)$과정은 오직 Key-chain과 Data-chain의 트랩도어(tk_K,tk_D)를 알고 있는 DC에 의해서만 수행 가능하며, 반드시 DC간 합의과정이 동반되어야만 블록체인 데이터를 수정 가능하다.

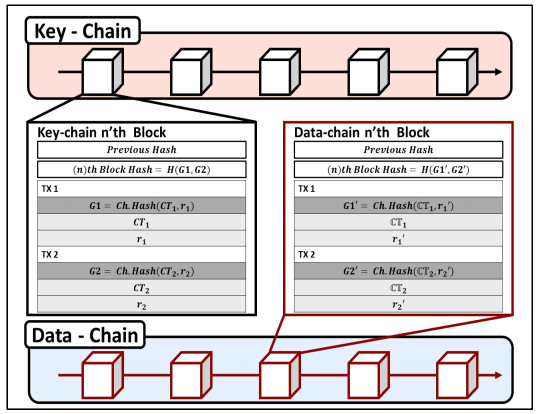

Fig. 10. Block structures of Key-chain and Data-chain

업데이트 과정은 Fig.9와 같이 총 3가지로 구성되며, 세부절차(Fig.11, 12)는 다음과 같다.

• **최초 준비과정** : 최초 시스템 구성간 ① TA는

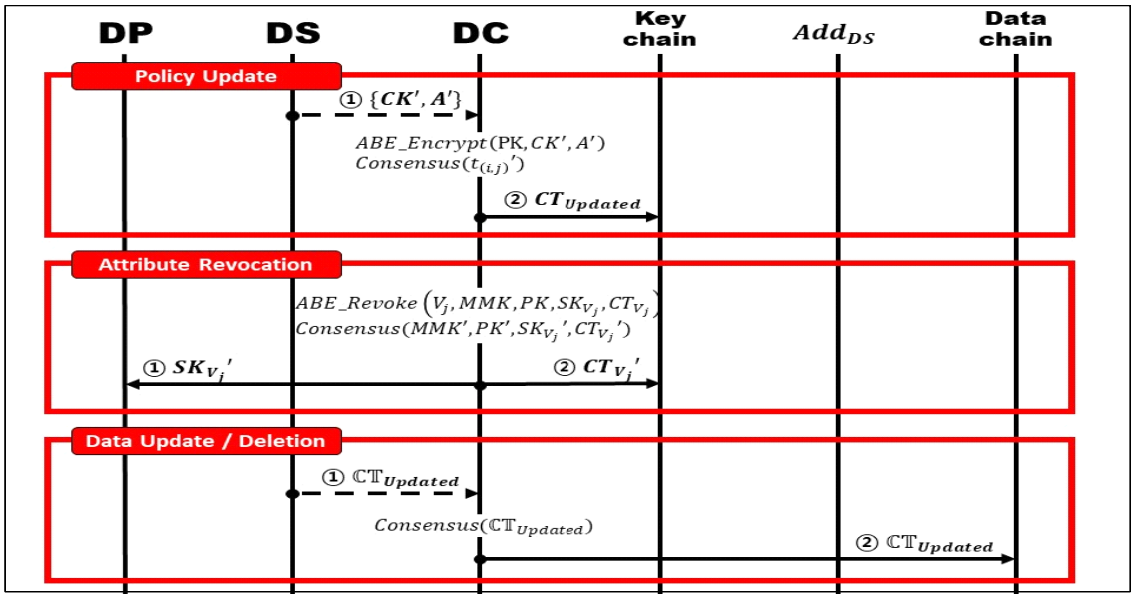

Fig. 9. Sequence diagram of Update phase

$CH.KeyGen()$을 통하여 DC가 카멜레온 해시 연산을 수행할 수 있도록 Key-chain과 Data-chain의 hk와 tk를 각각 생성한다. ② 이후, TA는 DC에게 (tk_K, tk_D)를 전달한다.

- **접근 정책 업데이트** : DS가 기존에 게재한 본인의 개인정보 접근 정책 변경($A \rightarrow A'$)을 희망하는 경우, ① DS는 DC에게 신규 정책(A')을 전달하여, 기존 Key-chain에 게재된 CT을 A'을 포함한 속성 기반 암호문으로 업데이트할 것을 요청한다. ② 이를 수신한 DC는 $CT_{Updated}$을 생성하고, ③ 보유한 tk_k을 활용하여 카멜레온 해시 충돌쌍을 계산하고($CH.Col(tk_k, CT, r, CT_{Updated})$, $CT_{Updated}$가 포함된 신규 거래($t_{(i,j)}'$)를 생성하여 다른 DC들에게 전달하여 Key-chain의 기존 거래$t_{(i,j)}$를 대체할 것을 제안한다. ④ DC간 합의 $Consensus(t_{(i,j)}')$를 통과한 신규 거래($t_{(i,j)}'$)는 모든 블록체인 노드들에게 전파되어 Key-chain 상의 기존 거래$t_{(i,j)}$을 대체하게 된다. 이때, Key-chain의 내용이 변경되어도 블록체인의 연결성은 유지된다(2.5 수정 가능한 블록체인 참조).
- **속성 업데이트** : DP가 기존 보유한 속성이 변경된 경우로, DP가 기존에 보유한 속성 기반 비밀키(SK_j)를 변경해야 한다. ⑤ j번째 DP의 속성(V_j)이 철회되는 경우, DC들은 j번째 DP의 변경된 비밀키(SK_j')와 DC의 신규 마스터키(MMK'), 신규 공개키 (PK'), 속성 V_j와 관련된 기존 암호문에 대응하는 신규 암호문 (CT_{V_j}')을 DC간 합의(Fig.12 line 6-9)를 동반하여 생성한다. 합의를 통과한 결과값에 대하여, ⑥ DC는 j번째 DP에게 변경된 비밀키(SK_j')를 전달하고, ⑦ 신규 공개키 PK'을 전파한다. ⑧ 기존 Key-chain상에 CT_{V_j}가 포함된 거래는 신규 암호문 CT_{V_j}'로 수정된다(Fig.12 line 5와 동일).
- **개인정보 수정/삭제** : DS가 기존 Data-chain에 기록된 개인정보(M)를 수정 또는 삭제하고 싶은 경우, ⑨ 변경된 값(M')을 기존 개인정보(M) 암호화에 사용된 ($CK \oplus Token$)을 활용하여 암호화 후($\mathbb{CT}_{Updated}$), DC에게 전달한다. 이를 수신한 DC는 DC간 합의(Fig.12 line 6-9)를 동반하여 Data-chain상에 기존 $\mathbb{CT}$가 포함된 블록 내용을 수정한다.

Algorithm 3 : CH Initialization Phase

▷ **Define :** $\Leftarrow$ // Secure channel
▷ **CH.Initialization**
1 $(hk_K, tk_K) \leftarrow TA.CH.KeyGen(k)$;
2 $(hk_D, tk_D) \leftarrow TA.CH.KeyGen(k)$; // ①
3 $TA.Broadcast(hk_K, hk_D)$ and $DC \Leftarrow TA.Send(tk_K, tk_D)$; // ②

Fig. 11. Algorithm 3 : CH Initialization Phase

Algorithm 4 : CH Update Phase

▷ **Define**
1 $t_{(i,j)}' \leftarrow Overwrite(t_{(i,j)}, CT_{Updated}, tk)$;
▷ **Access policy Update phase**
3 $DC \Leftarrow DS.Send(CK, A')$; // ①
4 $CT_{Updated} \leftarrow DC.ABE\_Encrypt(PK, CK, A')$; // ②
5 $t_{(i,j)}' \leftarrow DC.Overwrite(t_{(i,j)}, CT_{Updated}, tk_k)$;
6 While $Consensus(t_{(i,j)}')$ do
7 $DC.Verify(t_{(i,j)}')$;
8 if $t_{(i,j)}'$ *is valid* then
9 alarm and exit
// $line\ 5-9$: ③
10 $Keychain \leftarrow DC.Append(t_{(i,j)}')$; // ④
▷ **Attribute revocation phase**
11 $(MMK', PK', SK_{V_j}', CT_{V_j}') \leftarrow ABE\_Revoke(V_j, MMK, PK, SK_{V_j}, CT_{V_j})$; // ⑤
12 $DP \Leftarrow DC.Send(SK_{V_j}')$; // ⑥
13 $DC.Broadcast(PK')$; // ⑦
14 $Keychain \leftarrow DC.Append(CT_{V_j}')$; // ⑧
▷ **Personal data update / deletion phase**
15 $\mathbb{CT}_{Updated} \leftarrow DS.Enc(CK \oplus Token, M')$;
16 $DP \Leftarrow DS.Send(\mathbb{CT}_{Updated})$ and $Datachain \leftarrow DP.Append(\mathbb{CT}_{Updated})$;
// $line\ 15-16$: ⑨

Fig. 12. Algorithm 4 : CH Update Phase

V. 시스템 분석

5.1 GDPR 준수

본 논문의 시스템은 앞서 2.2에서 제시한 정보 주체(DS)의 권리를 구현하는 GDPR 조항을 모두 구

현 가능하다.

- **처리 제한권** : DS의 개인정보 처리는 오직, DS가 Key-chain상에 속성 기반 암호문CT에 포함한 접근 정책 A를 만족하는 DP만 처리 가능하다(Fig.8 ⑧).
- **정보 주체의 동의(consent)** : DP가 DS의 개인정보를 최종적으로 Data-chain의 $\mathbb{CT}$로부터 획득하기 위해서는 DS의 스마트 컨트랙트(Add_{DS})로부터 $Token$과 개인정보의 위치가 기재된 $I_{(x,y)}$를 획득해야만 한다. 이때 DS가 DP에게 발송하는 $Token$과 $I_{(x,y)}$는 개인정보 처리 이용을 동의함을 의미한다(Fig.8 ⑪).
- **정정권 / 삭제권** : DS의 개인정보(M) 또는 개인정보 처리 권한(A)에 대한 수정 요청은 DC간 합의를 동반한 수정 가능한 블록체인 구조를 통하여 구현 가능하다. 시스템 내 구성원의 속성 변경에 따른 키(SK_j) 업데이트 또한 가능하다(Fig.12 ⑤-⑧).
- **설계 및 기본설정에 의한 개인정보보호** : 본 논문의 블록체인 시스템에서는 유통되는 개인정보에 대한 기밀성, 무결성을 충족 가능하다(5.2 참고).
- **처리활동의 기록** : 본 논문의 개인정보 처리 시스템에서는 개인정보 업로드, 조회, 인증, 인가 및 접근제어 일체에 관한 건이 모두 블록체인의 분산원장(Key-chain, Data-chain, Add_{DS})에 거래 형태로 기록된다. 기록된 모든 거래 내용은 GDPR에서 요구하는 항시 제공 가능한 감사 자료로 활용 가능하며, 블록체인 시스템의 보안 이점에 따라 기록 위·변조 공격으로부터 안전하다.

5.2 보안 분석

본 논문 시스템의 공격 모델(attack model)은 크게 시스템 외부 공격자(external adversary)와 내부 공격자(internal adversary)로 구분되며 시스템 내 블록체인에 기록된 개인정보를 탈취 또는 악의적인 수정을 통하여 시스템의 기밀성, 무결성을 저하시키는 것을 목표로 하고 있다.

외부 공격자는 블록체인상에 기록된 공개된(public)정보를 조회하여 개인정보 또는 키 값을 탈취하여 기밀성을 저하시키려 한다. 내부 공격자는 다음과 같이 (1) 과거 DS의 접근 정책(A)을 충족 가능하였으나 현재는 속성이 철회된 DP, (2) DS의 요구사항에 반하는 개인정보 인가·처리를 도모하는 악의적인(malicious) DC로 구분된다.

- **기밀성** : 블록체인(Key-chain, Data-chain, Add_{DS})에 기재된 모든 정보는 블록체인 네트워크에 접속 가능한 사용자 모두에게 공개된다. 해시 연산, 대칭키 암호 등 암호학적 원리(cryptographic primitives)가 모두 안전(secure)하다는 전제하에, 외부 공격자는 블록체인 시스템을 모니터링함으로써 얻게 되는 정보들($CT, Hash(CK), CT'$)로부터 개인정보(M) 또는 이를 획득하기 위한 키 값($CK, Token$)을 얻을 수 없다.
  Fig.7에서 내부 공격자 중 속성이 철회된 DP는 본인의 갱신된 속성 기반 비밀키를 활용하여 기존에 조회 가능한 CT를 복호화시킬 수 없으며, 만약 속성 철회 발생 이전 시점에 본인의 속성 기반 비밀키를 활용하여 Key-chain으로부터 CK를 얻었다 하여도, Data-chain상의 $\mathbb{CT}$를 복호화하기 위하여 추가적으로 필요한 $Token$을 모르기 때문에 개인정보 M을 획득할 수 없다.
- **무결성** : 본 논문의 블록체인 시스템은 블록체인 합의 프로토콜과 분산원장에 기록된 개인정보 처리 내역(log)에 기반하여 안전성이 유지된다. 또한, 개인정보(M) 또는 접근 정책(A) 업데이트는 오직 카멜레온 해시 연산의 트랩도어(tk_K, tk_D)를 알고있는 사전 지정된 DC에 의해서 합의과정(Fig.12 ③)을 동반한 통제된 환경에서만 이루어진다. 이때, 트랩도어를 알지 못하는 일반 사용자(DS, DP)들에게는 카멜레온 해시 함수가 기존 해시함수와 마찬가지로 충돌 저항성을 만족하기 때문에[23] 트랩도어에 대한 접근 관리만 이루어지면 카멜레온 해시 사용에 따른 무결성 침해 문제는 발생하지 않는다.

DS의 개인정보를 처리함에 있어 악의적인 DC가 DS의 요구에 반하는 접근 정책(A)을 포함하는 속성 기반 암호문(CT)을 생성함으로써 악의적 개인정보 인가를 통한 개인정보 유출을 도모할 수 있다. 그러나, 블록체인상에 해당 정보가 기록되어 TA 및 시스템 구성원들로부터 항시 감시받기 때문에, 잘못된 개인정보 접근제어 처리에 따른 개인정보 유출을 예

방할 수 있다.

또한, Fig.9,12의 업데이트 과정에서 악의적 DC는 최초 TA로부터 획득한 카멜레온 해시 연산의 (tk_K, tk_D)를 기반으로 악의적 블록체인 데이터 수정 또는 삭제 공격을 진행할 수 있다. 그러나, 최종적으로 블록체인상의 데이터를 수정하기 위해서는 사전에 지정된 DC간의 합의 프로토콜의 요구 조건을 충족해야한다. 따라서, 시스템상의 악의적 DC에 의한 잘못된 거래를 생성하더라도 합의 과정을 통과할 수 없기 때문에 변조 공격으로부터 블록체인 시스템을 보호할 수 있다.

또한, 본 논문의 개인정보 처리 시스템은 블록체인 외부 요소의 개입을 최소화하였다. 본 논문 시스템의 TA는 최초 준비과정(Fig.5)에서 DP별 속성 부여 및 감사기관으로서의 역할 수행 외에 다른 과정에서 개입하는 소요는 없다. 따라서, [1]과 [10]의 시스템처럼 블록체인 외부 구성요소(외부 저장서버 등)를 활용함에 따른 유통되는 개인정보 및 처리결과에 대한 신뢰성 문제를 해결할 수 있다.

5.3 연산 효율성 분석

본 절에서는 본 논문에서 제안한 시스템의 연산 효율성을 과정별로 분석한다. 여기서 $1\times ABE.Encrypt$와 같은 표현은 $ABE.Encrypt$ 연산이 한 번 일어났음을 정의한다. 분석된 표는 아래 Table 3과 같다.

개인정보 또는 접근 정책 업데이트 과정에서는 블록체인 시스템 내 데이터의 무결성 유지를 위하여 DC에 의한 합의 프로토콜 진행이 요구된다. 시스템 내 존재하는 DC 노드의 수(n)가 많을수록 시스템의 안전성은 높아지나, 블록체인 합의 과정간 요구되는 연산($Verify$) 수행량이 많아지므로 시스템 설계 목표에 따라 적정 수준의 DC 노드 수(n) 지정이 요구된다. 특히, 속성 기반 암호화 및 카멜레온 해시 연산은 고연산 수행 능력을 지닌 DC 노드에 의해 수행되며, 카멜레온 해시 연산은 DS의 개인정보 삭제권/정정권 요구시에만 수행되므로 지속 가능한(sustainable) 개인정보 처리 시스템을 구축할 수 있다.

본 논문의 시스템은 컨소시엄 블록체인 환경으로 DC 노드간 PBFT[24] 합의 프로토콜을 통하여 블록체인을 유지한다. 따라서, 높은 연산 수행량을 요구하는 비트코인[6]의 작업증명(초당 약 7개 거래 생성)보다 높은 거래 생성 및 검증 속도를 유지할 수 있다(HLF v1.1 기준, 초당 140개 이상 거래 생성)[25]. 만일 Key-chain을 퍼블릭 블록체인으로 구현하여 비트코인 또는 이더리움과 같은 기존 운용중인 퍼블릭 블록체인으로 구현하는 경우, Key-chain의 거래 생성속도는 해당 블록체인 시스템의 거래 생성 속도에 수렴한다.

Table 3. The number of required computations per phase

Phase	Computation Efficiency
Initialization	• $(1\times ABE\_Systemsetup) + (2\times Broadcast) + (1\times ABE\_KeyGen) + (2\times Send)$
Data Upload	• $(1\times Generate) + (1\times Enc) + (1\times ABE\_Encrypt) + (2\times Send) + (3\times Append) + (1\times XOR) + (1\times Hash)$
Data Retrieve	• $(1\times ABE\_Decrypt)+(1\times Dec) + (1\times Encrypt) + (1\times Decrypt) + (2\times Append) + (1\times XOR) + (1\times Hash)$
CH Initialization	• $(2\times CH.KeyGen) + (1\times Broadcast) + (1\times Send)$
Access Policy Update	• $(1\times Send) + (1\times ABE\_Encrypt) + (1\times CH.Col) + (n\times Verify) + (1\times Append)$
Attribute Revocation	• $(k\times ABE\_Revoke) + (k\times Append) + (1\times Send) + (1\times Broadcast)$
Personal Data Update	• $(1\times Enc) + (1\times CH.Col) + (n\times Verify) + (1\times XOR) + (1\times Send) + (1\times Broadcast)$
Note	• k : The number of ciphertexts (CT_{V_j}) related to the revocated attribute(V_j) • n : The number of DC nodes

VI. 결 론

본 논문에서 우리는 다중 체인을 기반으로 GDPR에서 요구하는 정보 주체의 권리를 기술적으로 구현 가능한 개인정보 처리 시스템을 새롭게 제시하였다. 본 논문의 시스템에서는 기존 중앙화된 개인정보 처리 시스템이 GDPR로 대표되는 개인정보보호 규정 준수에 있어, 중앙화된 개인정보 처리·인가 서버 활용에 따라 발생 가능한 개인정보 처리의 무결

성 및 신뢰성 문제를 블록체인을 활용하여 해결 가능함을 보여주었다. 또한, 본 논문의 시스템에서 유통되는 개인정보는 속성 기반 암호화 및 스마트 컨트랙트를 활용하여 엄격한 접근제어가 구현된 가운데 개인정보 처리 기록이 블록체인의 분산원장에 기록됨으로써 시스템 구성원들로부터 감시 가능하도록 설계하였다.

향후 이어지는 연구에서는 분산원장에 거래 내용 기록간 소요되는 시간이 일반 중앙화된 시스템과 비교하여 느리다는 점 등을 고려하여 블록체인 시스템을 개인정보 처리 분야에서 실질적으로 활용하기 위해서 요구되는 성능 확보를 위한 추가적인 노력이 이어져야할 것이다.

References

[1] Wirth Christian and Michael Kolain. "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data," Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET), May. 2018

[2] Choi, Yong-hyuk and Hun-yeong Kwon. "A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information," Journal of the Korea Institute of Information Security & Cryptology 28.6, pp.1607-1621, June. 2018

[3] Jiguo Li, Wei Yao, Jinguang Han, Yichen Zhang, and Jian Shen. "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," IEEE Systems Journal 12.2, pp.1767-1777, March. 2017

[4] Sejin Han, Suntae Kim, and Sooyoung Park. "A GDPR based Approach to Enhancing Blockchain Privacy," The Journal of The Institute of Internet, Broadcasting and Communication 19.5, pp.33-38, October. 2019

[5] Kondapally Ashritha, Sindhu M and Lakshmy KV. "Redactable Blockchain using Enhanced Chameleon Hash Function," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, June. 2019

[6] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf/, 2008

[7] GDPR.EU, "What-is-gdpr" https://gdpr.eu/what-is-gdpr/, 2020

[8] BBC, "Google hit with £44m GDPR fine over ads" https://www.bbc.com/news/technology-46944696, 2019

[9] BBC, "British Airways faces record £183m fine for data breach" https://www.bbc.com/news/av/embed/p06kjsw5/48905907, 2019

[10] Nguyen Binh Truong and Gyu Myoung Lee. "Gdpr-Compliant Personal Data Management: A Blockchain-Based Solution," IEEE Transactions on Information Forensics and Security 15, pp.1746-1761, October. 2019

[11] Giuseppe Ateniese, Bernardo Magri, Daniele Venturi and Ewerton R.Andrade. "Redactable Blockchain - or - Rewriting History in Bitcoin and Friends," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 111-126, April. 2017

[12] Gavin Wood. "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper 151. pp.1-32, November. 2017

[13] Christian Cachin. "Architecture of the hyperledger blockchain fabric," Workshop on distributed cryptocurrencies and consensus ledgers, Vol. 310, no.4, July. 2016

[14] Guangsheng Yu, Xuan Zha, Xu Wang, Wei Ni, Ping Yu, J.Andrew Zhang, Ren Ping Liu and Y.Jay Guo. "Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems," IEEE Transactions on Engineering Management, pp.1-18, January. 2020
[15] Hardt, Dick. "Rfc 6749: The oauth 2.0 authorization framework," Internet Engineering Task Force (IETF) 10 : 2070-1721, 2012
[16] Jones, Michael, and Dick Hardt. "RFC 6750-The OAuth 2.0 Authorization Framework: Bearer Token Usage," Internet Engineering Task Force (IETF), 2012
[17] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption," SP'07, IEEE symposium on security and privacy, pp.321-334, May. 2007
[18] Oscar Novo. "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal Vol.5, No.2, pp.1184-1195, April. 2018
[19] Ke Huang, Xiaosong Zhang, Yi Mu, Fatemeh Rezaeibagha, Xiaojiang Du and Nadra Guizani. "Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain," IEEE Transactions on Industrial Informatics, Vol.16, NO.4, pp.2677-2686, April. 2019
[20] Aurelie Bayle, Mirko Koscina and David Manset. "When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry," 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp.788-792, December. 2018
[21] Pradip Kumar Sharma and Jong Hyuk Park. "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems 86, pp.650-655, April. 2018
[22] Daniel Fett, Ralf Küsters and Guido Schmitz. "A comprehensive formal security analysis of OAuth 2.0," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp.1204-1215, October. 2016
[23] Giuseppe Ateniese and Breno de Medeiros. "On the Key Exposure Problem in Chameleon Hashes," International Conference on Security in Communication Networks, Springer, Berlin, Heidelberg, pp.165-179, 2004
[24] Miguel Castro and Barbara Liskov. "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Transactions on Computer Systems (TOCS), Vol.20, No.4, pp.398-461, November. 2002
[25] Parth Thakkar, Senthil Nathan, and Balaji Viswanathan. "Performance benchmarking and optimizing hyperledger fabric blockchain platform," 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems(MASCOTS), pp.264-276, September. 2018

〈저 자 소 개〉

임 준 호 (Joon Ho Lim) 학생회원
2014년 2월: 육군사관학교 정보과학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 블록체인, 개인정보 보호

천 지 영 (Ji Young Chun) 종신회원
1997년 2월: 이화여자대학교 수학과 졸업
2006년 2월: 고려대학교 정보보호학과 석사
2011년 8월: 고려대학교 정보경영공학과 박사
2011년 9월~2019년 12월: 고려대학교 정보보호연구원 연구교수, 시간강사
2012년 8월~2014년 3월: University of Illinois at Urbana-Champaign 박사후 연구원
2020년 1월~현재: 이화여자대학교 엘텍공과대학 컴퓨터공학전공 특임교수
〈관심분야〉 정보보호 프로토콜, 데이터 보안, 프라이버시 향상 기술

노 건 태 (Geontae Noh) 종신회원
2008년 2월: 고려대학교 산업시스템정보공학과 졸업
2010년 2월: 고려대학교 정보경영공학과 석사
2014년 8월: 고려대학교 정보보호학과 박사
2014년 9월~2017년 2월: 고려대학교 정보보호연구원 박사후 연구원, 연구교수
2017년 2월~현재: 서울사이버대학교 빅데이터·정보보호학과 조교수
2020년 3월~현재: 서울사이버대학교 빅데이터·AI센터 센터장
〈관심분야〉 암호 이론, 데이터 보안, 프라이버시 향상 기술

정 익 래 (Ik Rae Jeong) 정회원
1998년 2월: 고려대학교 전산학과 졸업
2000년 2월: 고려대학교 전산학과 석사
2004년 8월: 고려대학교 정보보호학과 박사
2006년 3월~2008년 2월: 한국전자통신연구원 암호기술연구팀 선임연구원
2008년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호 이론, 프라이버시 향상 기술 (PET), 데이터베이스 보안, 생체인증