The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 1, pp.55-60, Feb. 29, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.1.55
JIIBC 2020-1-7

BACS : 퍼블릭 블록체인 접근 통제 시스템에 관한 실험적 연구

BACS : An Experimental Study For Access Control System In Public Blockchain

한세진[*], 이선재[**], 이도현[***], 박수용[****]

Sejin Han[*], Sunjae Lee[**], Dohyeon Lee[***], Sooyoung Park[****]

요 약 본 논문에서는 퍼블릭 블록체인에서 개인정보를 안전하게 보호하기 위한 방법으로, 암호기법을 이용한 접근통제 시스템을 제안한다. 제안 시스템은 거래 데이터 중에서 개인정보에 해당하는 부분을 선별하여 이를 접근정책에 따라 암호화한 다음 블록체인에 저장하고, 적정한 권한을 가진 사람만이 복호화하도록 설계된다. 성능과 확장성을 향상시키기 위하여 암호스킴을 블록체인과 연동하는 오프-체인 네트워크에 구현한다. 따라서 암호 연산에 따른 성능저하가 미미하고, 기존 블록체인 네트워크의 구성을 보존하면서도 새로운 접근통제를 반영할 수 있어 확장성이 높다. 암호화 스킴은 속성기반암호화(ABE:Attribute-Based Encryption)에 기반한다. 그러나 통상적인 ABE와 달리 정보의 속성인 보유기간을 접근구조에 포함하여 개인정보 보호규제에서 요구하는 정보의 잊혀질 권리를 제공한다. 한편 ABE의 처리 성능문제를 보완하기 위해 대칭키 방식을 혼용한 것도 본 논문의 특징이라 할 수 있다. 제안 시스템을 공개형 블록체인인 클레이튼을 이용하여 구현하고 성능 평가를 통해 타당성을 증명하였다.

Abstract In this paper, we propose an access control system using cryptography as a method to protect personal data in public blockchain. The proposed system is designed to encrypt data according to the access policy, store it in the blockchain, and decrypt only the person who satisfy the access policy. In order to improve performance and scalability, an encryption mechanism is implemented outside the blockchain. Therefore, data access performance could be preserved while cryptographic operations executed Furthermore it can also improve the scalability by adding new access control modules while preserving the current configuration of blockchain network. The encryption scheme is based on the attribute-based encryption (ABE). However, unlike the traditional ABE, the “retention period”, is incorporated into the access structure to ensure the right to be forgotten. In addition, symmetric key cryptograpic algorithms are used for the performance of ABE. We implemented the proposed system in a public blockchain and conducted the performance evaluation.

Key Words : Access Control, Attribute-Based Encryption, AES-CBC, Blockchain, DCPABE, Personal data, Public Key, Private Key, Right to be forgotten

[*]준회원, 서강대학교 컴퓨터공학과 박사과정
[**]준회원, 서강대학교 컴퓨터공학과 석사과정
[***]준회원, 서강대학교 컴퓨터공학과 석사과정
[****]정회원, 서강대학교 컴퓨터공학과 정교수
접수일자: 2019년 11월 28일, 수정완료: 2020년 1월 4일
게재확정일자: 2020년 2월 7일

Received: 28 November, 2019 / Revised: 4 January, 2020 / Accepted: 7 February, 2020
[****]Corresponding Author: sypark@sogang.ac.kr
Department of Software Engineering, Sogang University, Korea.

Ⅰ. 서 론

블록체인 기술은 4차 산업혁명을 이끌 주요 기술로 주목 받고 있다. 특히 탈중앙화 모델로서, 높은 수준의 데이터 무결성을 제공하기 때문에 암호화폐[1][2], 자동화된 스마트 계약[8][4], IoT와 결합한 스마트기기, 헬스케어, 유통망 등과 같은 분야[3]에서 각광 받고 있다. 그러나 네트워크의 참여와 이탈이 자유로운 공개형 블록체인에서는 데이터가 모두에게 공개되기 때문에 개인정보를 입력하게 될 경우 프라이버시가 보장되지 않는다는 문제점이 있다[5]. 특히 의료, 금융 등 민감한 개인정보 처리가 불가피한 분야에서는 심각한 문제가 될 수 있다.

본 논문에서는 공개형 블록체인에서 개인정보를 안전하게 보호하기 위한 방법으로 암호기법을 이용한 접근통제시스템을 제안한다. 제안 시스템은 거래 데이터 중에서 개인정보에 해당하는 부분을 선별하여 이를 접근정책에 따라 암호화한 다음 블록체인에 저장하고, 적정한 권한을 가진 사람만이 복호화할 수 있도록 한다. 성능과 확장성을 위하여 암호 기능을 블록체인과 연동하는 오프체인 네트워크에 별도로 구현하는 것이 특징이라 할 수 있다.

제안 시스템은 속성기반암호화(ABE : Attribute-Based Encryption) 스킴에 기반한다. 그러나 통상적인 ABE의 접근통제 구조가 정보주체의 속성을 기준으로 이루어지는 데 비하여, 제안 스킴은 정보의 속성, 즉, 보유기간을 포함하는 특징을 가진다. 따라서 자격조건에 따른 접근통제 뿐만 아니라 정보의 보관 만료기간에 따라서도 접근을 통제할 수 있다. 이는 국내외 개인정보보호법의 개인정보 보호원칙인 “잊혀질 권리”를 블록체인에서 구현했다는 점에서 의미가 있다. 한편 ABE의 처리 성능문제를 보완하기 위해 대칭키 방식을 혼용한 것도 본 제안의 특징이라 할 수 있다. 제안하는 시스템을 공개형 블록체인인 클레이튼의 스마트 컨트랙트를 이용하여 구현하였으며 성능 평가를 통해 타당성을 증명하였다.

Ⅱ. 관련 연구

1. 속성기반암호화

속성기반암호화(ABE:Attribute-Based Encryption)는 Sahai와 Waters에 의하여 2005년에 소개되었다[11]. ABE는 정보주체의 다양한 속성(직급, 소속 등)을 반영한 접근정책을 이용하여 데이터를 암호화 하고, 이용자가 가진 속성이 접근정책에 부합할 경우 암호문을 복호화 할 수 있도록 설계된다. 속성과 암호화/복호화키는 제3의 신뢰기관에 의해 발급된다.

2. 다중기관 속성기반암호화

현대 사회에서 개인은 오직 한 단체 또는 법인에 대한 속성으로 한정될 수 없을 만큼 다양한 기관과 연관되어 있다. 예를 들어, 어떤 개인이 대학 연구실의 “연구원” 속성과 병원 조직의 “의사” 속성을 동시에 가질 수 있다. Sahai와 Waters가 제안한 모델[12]에서는 모든 속성키를 단일 신뢰기관에서 처리하였기 때문에 키의 통합 처리가 어려울 뿐만 아니라 신뢰기관의 키 에스크로 문제가 존재한다. 이 문제를 해결하기 위하여 Chase 등은 다중기관에 의해 속성이 관리되는 다중기관 속성기반암호화(Multi-Authority ABE) 모델을 제시하였다[13]. 이 모델에서는 전체 속성집합을 K개의 서로 다른 속성 기관이 중첩 없이 나누어 처리하므로 단일 기관이 전체 키를 보유할 수 없다는 장점이 있고 키 에스크로 문제도 존재하지 않지만, 속성 기관을 여전히 단일 중앙기관이 관리하므로 단일 지점 의존도가 발생하는 문제가 있다. 뿐만 아니라 사전에 정의된 기관에서만 속성 기반 암호화를 수행할 수 있기 한계점 때문에 새로운 기관을 추가하면 암호화를 다시 수행해야하는 문제점이 존재한다.

3. 탈중앙 속성기반암호화

Lekwo 등은 앞서 연구된 다중기관 속성기반암호화 모델에서 중앙 기관을 제거하고, 누구나 전역 파라메터(Global Parameter) 값을 이용하여 속성기반암호화에 참여토록 하는 탈중앙 속성기반암호화(DCPABE : Decentralized Attribute-Based Encryption) 프로토콜을 제안 하였다[14]. 이 모델은 신뢰기관에 대한 의존도가 낮고 키 에스크로 문제가 존재하지 않는다는 장점이 있다. 다만, 암호 알고리즘이 합성수 기반의 위수(order)를 사용하므로 처리 속도가 낮고, 속성의 폐기(revocation)가 어렵다는 문제점이 존재한다.

4. 오프체인

오프체인은 블록체인 외부에 새로운 네트워크를 구성하여 블록체인의 성능 및 수수료 문제를 개선하는 방식이다. Joseph Poon등은 2015년 오프체인을 이용하여 블록체인의 한계를 극복하는 모델인 라이트닝 네트워크 제안하였다[15]. 이 모델은 오프체인에서 공개키암호 알고리즘을 이용하여 자산을 안전하게 거래하고 최종 거래만

메인 블록체인에 기록함으로서 합의 알고리즘 과정에서 발생하는 느린 거래속도와 비싼 수수료 문제를 해결하였다. 또한, 2018년 라이트닝 네트워크를 실제로 구현하여 블록체인 외부에 탈중앙 네트워크를 유지할 수 있다는 것을 입증하였다.

Ⅲ. Preliminaries

본 논문에서 사용하게 될 접근구조(access structures)와 겹선형함수(bilinear map)에 대해 알아본다.

1. 접근구조(Access Structures)

Definition $\{P_1,...P_n\}$를 속성들의 집합이라고 하자. 접근구조 A는 단조증가 집합이며, 다음과 같이 정의된다.

$A \subseteq 2^{P1,...Pn}$일 때, $\forall B, C$: 만약 $B \in A$ 이고 $B \subseteq C$라면, $C \in A$이다.

2. 겹선형 함수(Bilinear map)

Definition G_1과 G_2는 소수 p 위수를 갖는 곱셈 순환군이다. g는 G_1의 생성원이고, e는 다음 조건을 만족하는 함수로써 $e : G_1 X G_1 \rightarrow G_2$ 를 겹선형 함수라 한다.

·Bilinearity: $e(g^a, g^b) = e(g,g)^{ab}$ $(a,b \in Z_p^*)$

·Non-degeneracy : $e(g,g) \neq 1$

·Efficient computability : $e(g,g)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

Ⅳ. 제안 모델

본 논문에서는 오프체인 환경에서 다중기관 네트워크를 구성하여 블록체인 데이터의 접근 권한을 통제하는 블록체인 접근 통제 시스템(BACS : Blockchain-based Access Control System)을 제안한다.

1. 시스템 모델

BACS는 그림 1과 같이 BACS Relayer, 퍼블릭 블록체인(Klaytn) 그리고 사용자 웹 클라이언트로 구성된다. Relayer는 클라이언트와 블록체인간에 데이터를 중개하는 역할을 한다. 주요 동작은 ①클라이언트 입력 데이터를 Relayer에 전달하면 ② Relayer는 이를 암호화하여 블록체인의 스마트 컨트랙트에 전송하고, 스마트 컨트랙트는 이를 블록체인에 기록한다. ③ Relayer는 복호화를 위해 스마트 컨트랙트로부터 조회할 데이터를 전달받고 ④ 이를 복호화하여 클라이언트에 전달한다.

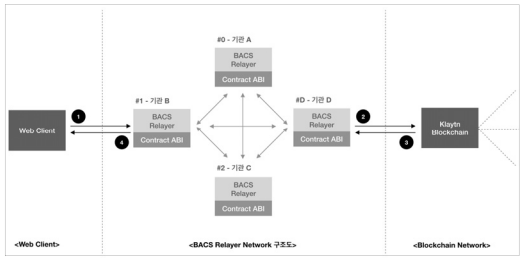

그림 1. 프레임워크
Fig. 1. Framework

2. 세부 기술

BACS 알고리즘은 II.2절에서 설명한 Lewko의 DCPABE를 블록체인에 효과적으로 결합한 것으로, 주요 차별점은 (1)처리 속도 개선을 위해 하이브리드 암호방식을 사용한 것과, (2)기존 접근구조에 정보의 속성(유효기간)을 추가한 확장된 접근구조를 도입한 점이다.

① 하이브리드 암호화

DCPABE는 합성수 위수를 갖는 암호 알고리즘을 이용하므로 암호 처리 속도가 낮은 문제점을 가지고 있다. 더욱이 접근정책에 포함되는 속성 개수가 증가할 경우 암호 처리 시간은 이에 비례하여 더욱 증가한다. 이를 해결하기 위해 우리는 고정 크기의 암호문을 생성하는 AES-256-CBC를 사용하여 데이터를 암호화하고, AES-CBC에 사용된 비밀키를 DCPABE로 암호화하여 키에 대한 접근을 통제하는 새로운 하이브리드[16] ABE를 제안한다. 그림 2는 제안하는 시스템을 도식화한 것이다.

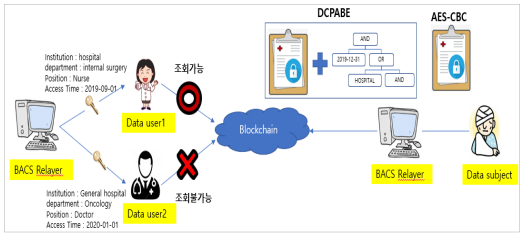

그림 2. BACS 동작 구조
Fig. 2. BACS flow

② 확장된 접근구조

이전에 연구된 모든 ABE가 주체(subject)의 속성으로 이루어진 접근구조를 사용하였으나, 이 경우 개인정보보호법에서 요구하는 데이터에 대한 보유기간 경과시의 삭제 기능을 구현하기 어렵다. 이에 우리는 주체뿐만 아니라 객체(object)에 대한 속성인 "보유기간" 을 기존 접근구조에 추가한 "확장된 접근구조"를 제안한다.

3. BACS 알고리즘

제안하는 알고리즘은 아래와 같이 5단계로 구성된다.

① $Global\,Setup(\lambda) \rightarrow GP$

파라미터 λ 를 이용하여 글로벌 파라미터(GP) 를 생성한다.

② $Authority\,Setup(GP) \rightarrow SK, PK$

GP와 속성집합을 이용하여 임의의 수 $a_i, y_i \in Z_N$에 대해 각 기관노드의 비밀키(SK), 공개키(PK)쌍를 (1)과 같이 생성한다.

$$PK = \left\{ e(g_1, g_2)^{a_i}, g_1^{\gamma_i} \forall\, i \right\}$$
$$SK = \left\{ \alpha_i, y_i \forall\, i \right\} \quad \cdots(1)$$

③ Encrypt(AS, GP, {PK}) → CT

메시지 M을 AES-CBC로 암호화하고 AES-CBC키를 GP, 확장된 접근구조(AS), 모든 기관노드 공개키 {PK} 및 임의의 수 s, $r_x \in Z_N$을 이용하여 (2)와 같이 암호화한다.

$$C_0 = Me(g_1, g_1)^8$$
$$C_{1,x} = (g_1, g_1)^{\lambda_x} e(g_1, g_1)^{a_{p(x)} r_x}$$
$$C_{2,x} = g_1^{r_x}$$
$$C_{3,x} = g_1^{y_{p(x)} r_x} g_1^{w_x} \forall\, x$$

($A_{x=}$= 접근행렬 A의 x번째 행, $\lambda_x = A_x \bullet v$, $w_x = A_x \bullet w$) $\cdots(2)$

④ $KeyGen(GID, A_i, T, SK, GP) \rightarrow K_{i,GID}$

GID, 속성집합 A_i, 접근시각(T), GP를 이용하여 사용자 개인키 $K_{Ai,GID}$를 (3)과 같이 생성한다.

$$K_{i,GID} = g_1^{\alpha_i} H(GID)^{y_i} \quad \cdots(3)$$

⑤ $Decrypt(CT, GP, K_{i,GID}) \rightarrow M$

글로벌 파라미터(GP) 개인키로 (4)와 같이 복호화 한다.

$$C_{1,x} \bullet e(H(GID), C_{3,x}) / e(K_{p(x),GID,C_{2,x}}) = e(g_1, g_1)^{\lambda_x} e(H(GID), g_1)^{w_x} \quad \cdots(4)$$

임의의 수 $c_x \in Z_N (\sum_x c_x A_x = (1,0,\ldots,0))$에 대해 (5)를 계산한다.

$$\prod_x (e(g_1,g_1)^{\lambda_x} e(H(GID),g_1)^{w_x})^{C_x} = e(g_1,g_1)^8 \cdots(5)$$

원문 메시지는 (6)과 같이 도출된다.

$$M = C_0 / e(g_1, g_1)^8 \quad \cdots(6)$$

V. 실험 및 평가

1. 실험 환경

Ubuntu OS 16.04 LS(1 Core, 2 GB Memory)에 퍼블릭 블록체인 클레이튼을 설치하고, 이 네트워크와 연동하는 별도의 오프체인 네트워크를 구성한다. 오프체인 네트워크에 노드를 구성하고 각 노드에 클라이언트와 블록체인을 중개하는 컴포넌트인 BACS Relayer를 설치한다. BACS Relayer는 클라이언트가 입력한 개인정보를 암호화하여 블록체인에 기록하고 반대로 블록체인에서 읽은 데이터를 복호화하여 클라이언트에게 전달하는 모듈이다. BACS Relayer 프로그램 구현을 위해 싱가포르 난양공과대학교의 SANDS[17] 팀에서 개발한 DCPABE 라이브러리와 Java 표준 암호화 라이브러리에서 제공하는 AES-256-CBC를 이용하였다.

2. 실험 방법

속성 키를 발급하는 다중 속성기관을 총 4개 구성하였고, 각각을 4대의 BACS Relayer 노드에 설치하였다. 각 노드는 8개, 21개, 23개, 14개의 속성 키(중복 없음)를 생성하고 이를 서로가 공유한다. 본 실험에서는 트랜젝션 길이와 접근정책에 포함된 속성갯수를 증가시키면서 BACS Relayer의 암호화 및 복호화에 소요되는 시간을 측정한다.

3. 성능 평가 결과

실험 결과, 표 1과 같이 330바이트의 트랜젝션을 암

호화 했을 때 514ms가 소요되었고 복호화하는 데는 79ms가 소요되었다. 데이터 사이즈를 680바이트까지 증가시켜도 처리 시간에는 큰 변화가 없음을 알수 있다. 반면 표 2에서와 같이 트랜젝션 사이즈를 150 바이트로 고정시킨 상태에서 속성 개수가 3개일 때 암호화에 608ms, 복호화에 78ms가 소요되었으나, 속성 개수를 정보의 보유기간 속성을 추가하여 30개로 증가시키자 암호화에 3,118ms, 복호화에 1,574ms가 소요되는 등 다소 긴 시간이 소요 되었다. 다만, 복호화 처리 시간은 암호화 처리 시간보다 상대적으로 짧은데, 이는 복호화 할 때는 접근정책의 조건식을 충족하기 위해 필요로 하는 속성 비밀키의 개수가 암호화 때보다 같거나 작기 때문이다. 예를 들어 (의사 OR 간호사)의 접근 정책을 가진 데이터의 경우 의사만으로도 복호화가 가능하다.

표 1. 트랜젝션 길이에 따른 성능 측정 결과
Table 1. Performance measurements as transaction size increase

Time(ms)	Transaction(Byte)		
	330	480	680
encryption	514	532	586
decryption	79	78	78

표 2. 속성 갯수에 따른 성능 측정 결과
Table 2. Performance measurements as the number of attributes increases

Time(ms)	The number of attributes			
	1	2	3	30
encryption	401	462	608	3,118
decryption	39	84	78	1,574

4. 개인정보 보호 평가

(1) 접근통제 및 보유기간

제안하는 BACS 알고리즘은 암호화된 정보를 복호화할 수 있는 조건을 복호자의 속성으로 설정하였기 때문에 해당 속성이 조건에 부합되는 경우에만 복호화할 수 있다. 속성에는 일반적인 소속과 직책 등을 나타내는 정보주체의 속성과 데이터의 보유기간을 나타내는 객체 속성이 포함되므로 이에 부합하지 않는 접근은 모두 차단된다.

(2) 기밀성 및 무결성

모든 데이터는 암호화되므로 기밀성이 보장되고, 또한 암호문은 정보의 변경이 불가능한 블록체인 분산원장에 기록되므로 무결성이 보장된다.

Ⅵ. 결 론

본 논문에서는 속성기반암호 스킴을 공개형 블록체인에 결합한 블록체인 접근제어 시스템을 제안하였다. 선행연구인 탈중앙 다중 속성기반암호화 모델에 암호문 사이즈를 고정화하는 대칭키 암호를 추가 적용하여, 트랜젝션 사이즈에 상관없는 고정적인 암복호화 처리 성능을 달성하였다. 또한 정보의 유효기간 속성을 접근정책에 추가하여 만기 도래시 접근을 차단토록 하였으나, 유효기간 속성을 반영하는 과정에서 속성의 개수가 크게 증가하고 결과적으로 암호화 속도가 증가하는 현상이 발생하는 문제점이 있었다. 이는 향후 연구에서 개선이 필요한 부분이다.

References

[1] Tasca, P., Hayes, A. and Liu, S, "The evolution of the bitcoin economy", Journal of Risk Finance, Vol. 19, No. 2, pp.94-126. 2018.
DOI: https://doi.org/10.1108/JRF-03-2017-0059

[2] [Online]
DOI:https://www.ibm.com/blockchain/financial-services

[3] Sang Guk Moon, Min Sun Kim, Hyun Joo Kim, "Design of an Intergrated University Information Service Model Based on Block Chain", Journal of the Korea Academia-Industrial cooperation Society, Vol. 20, No. 2, pp.43-50, 2019.
DOI:https://doi.org/10.5762/KAIS.2019.20.2.43

[4] Sheng ding, Jin Cao, Chen Li, Kai Fan, and Hui Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT", IEEE ACCESS, Vol.7, pp.38431-38441, 2019.
DOI: https://doi.org/10.1109/ACCESS.2019.2905846

[5] Young-Seek Chung, Jae-Sang Cha, "The Security Risk and Countermeasures of Blockchain based Virtual Currency Trading", Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 11, No. 1, pp.100-106, 2018.
DOI:https://doi.org/10.17661/jkiiect.2018.11.1.100

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash

system", 2008.

[7] [Online] https://proofofexistence.com

[8] Vitalik Buterin, "Ethereum White Paper", 2014..

[9] Heeyoul Kim, "Analysis of Security Threats and Countermeasures on Blockchain Platforms", Journal of KIIT. Vol. 16, No. 5, pp.103-112, pISSN 1598-8619, eISSN 2093-7571 103, 2018.
DOI:https://doi.org/10.14801/jkiit.2018.16.5.103

[10] Donghyeok Lee and Namje Park, "CCTV Video Privacy Protection Scheme Based on Edge Blockchain", Journal of KIIT. Vol. 17, No. 10, pp.101-113, pISSN 1598-8619, eISSN 2093-7571 101, 2019.
DOI:https://doi.org/10.14801/jkiit.2019.17.10.101

[11] V.Goyal, O.Pandey, A.Sahai, and B.Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", CCS '06 Proceedings of the 13th ACM Conference on Computer and Communications Security, pp.89-98, 2006.
DOI: https://doi.org/10.1145/1180405.1180418

[12] Chase M,"Multi-authority Attribute Based Encryption.", Vadhan S.P. (eds) Theory of Cryptography, TCC 2007, Lecture Notes in Computer Science, Vol 4392, 2007.
DOI: https://doi.org/10.1007/978-3-540-70936-7_28

[13] Melissa Chase and S.Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", CCS '09 Proceedings of the 16th ACM conference on Computer and communications security, pp.121-130, 2009.
DOI: https://doi.org/10.1145/1653662.1653678

[14] Lewko A., Waters B, "Decentralizing Attribute-Based Encryption:, Paterson K.G. (eds) Advances in Cryptology-EUROCRYPT 2011, EUROCRYPT 2011, Lecture Notes in Computer Science, Vol, 6632, 2011.
DOI: https://doi.org/10.1007/978-3-642-20465-4_31

[15] Joseph Poon and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payment", 2016.

[16] IETF RFC 5246.
DOI: https://tools.ietf.org/html/rfc5246

[17] SANDS team at the Nanyang Technological University, http://sands.sce.ntu.edu.sg/

저 자 소 개

한 세 진(준회원)

- 서강대학교 컴퓨터공학과 학사('98), 석사('01), 박사수료('18)
- KT 책임연구원('01~'11)
- 금융감독원 선임조사역('11~現)
- 관심분야 : 핀테크, 블록체인

이 선 재(준회원)

- 성신여자대학교 융합보안학과 학사('15)
- 서강대학교 컴퓨터공학과 석사('18~現)
- 관심분야 : 소프트웨어공학, 블록체인

이 도 현(준회원)

- 국가평생교육진흥원 컴퓨터공학과 학사
- 서강대학교 컴퓨터공학과 석사('19~現)
- 관심분야 : 소프트웨어공학, 블록체인

박 수 용(정회원)

- 서강대학교 컴퓨터공학과 학사('86), Florida State University 컴퓨터 및 정보과학 석사('88), George Mason University 정보기술학 박사('95)
- 서강대학교 컴퓨터공학과 교수('98~現)
- 관심분야 : 블록체인, 요구공학

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음 (IITP-2020-2017-0-01628*)