chapter 2

분산원장기술 시스템을 위한 보안기능 요구사항

박근덕 ‖ 서울외국어대학원대학교 조교수

I. 서론

4차 산업혁명 관련 신흥 기술로 주목받고 있는 분산원장기술(예; 블록체인 등)은 오픈소스(Open source) 기반 분산원장기술(DLT) 시스템(또는 플랫폼)으로 구현되어 다양한 애플리케이션(또는 서비스) 개발 시 널리 활용되고 있다. 최근 과학기술정보통신부와 한국인터넷진흥원(KISA)은 블록체인 발전전략(2018)의 일환으로 민간주도 국민 프로젝트를 추진하여 탈중앙화 기부 플랫폼 개발, 블록체인 기반 중고차 서비스 플랫폼 개발, 블록체인 ID/인증 네트워크 기반 금융, 통신, 교육 분야 서비스 개발 및 응용 확산 등 3개 과제를 선정하였고 2020년도에 각 사업자를 통해 시범 서비스를 운영할 계획이다. 또한, 국민들이 체감할 수 있고 편익이 높은 6개 분야에서 블록체인 공공분야 시범사업을[1] 행정기관 등과 진행하고 있다. 그리고 다수의 기업들도 국가간 송금 시스템, 지역화폐(또는 모바일 상품권) 거래 시스템, 온라인 지급결제 시스템 등 분산원장기술을 활용한 다양한 서비스를 개발 및 운영하고 있다.

앞에서 살펴본 바와 같이 공공 및 민간 분야에서 개발 및 운영하는 각종 서비스는 대부

* 본 내용은 박근덕 교수(☎ 02-2182-6000, jacepark926@gmail.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
1) 온라인 투표 시스템(중앙선거관리위원회), 전자문서 발급 인증 시스템(외교통상부), 축산물 이력관리 시스템(농림축산식품부), 부동산 거래 시스템(국토교통부), 해외 직구를 위한 개인 통관 시스템(관세청), 해운물류 시스템(해양수산부)

분 오픈소스 기반 분산원장기술 시스템(또는 플랫폼, 예; 하이퍼레저 패브릭, 이더리움 등)을 활용하고 있다. 이용자에게 제공되는 분산원장기술 기반 서비스는 기존의 중앙화된 시스템(Non-DLT system)과 분산원장기술 시스템을 포함하고 있어 서비스 운영 시 분산원장기술 시스템에서 발생할 수 있는 보안 위협 식별 및 대응이 절실히 필요하다.

본 고에서는 오픈소스 기반 분산원장기술 시스템의 보안 강화를 위해 제II장에서는 오픈소스 기반 분산원장기술 시스템에서 제공하는 보안 기능을 살펴본다. 제III장에서는 이용자에게 서비스를 제공하기 위한 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 잠재적인 보안 위협을 식별하고, 제IV장에서는 제III장에서 식별된 보안 위협에 대응할 수 있는 보안기능 요구사항을 제안한다. 마지막으로 제V장에서는 결론과 향후 일정을 설명한다.

II. 오픈소스 기반 분산원장기술 시스템

본 장에서는 오픈소스 기반 분산원장기술 시스템 중 대표적으로 널리 활용되고 있는 하이퍼레저 패브릭과 이더리움에서 기본적으로 제공하고 있는 보안 기능을 설명한다.

1. 하이퍼레저 패브릭

하이퍼레저 패브릭(Hyperledger Fabric)은 리눅스 재단(Linux Foundation)에서 개발 및 유지 관리하고 있는 오픈소스 기반 분산원장기술 시스템으로서 허가형(Permissioned, Private) 분산원장 네트워크와 스마트 계약(Smart Contract)을 제공하는 것이 특징이다[1].

하이퍼레저 패브릭에서 제공하는 보안 기능은 데이터 무결성, 신원 관리, 접근 통제, 암호화 등이 있다. 데이터 무결성 기능은 분산원장에 저장된 거래 데이터에 대한 무결성을 검사하는 기능을 제공한다. 신원 관리 기능은 아이디(ID) 또는 시스템 개체(Entities)의 등록, 변경 및 삭제 기능과 인증 및 권한 부여 기능을 제공한다[2]. 접근 통제 기능은 분산원장 네트워크를 채널 단위로 분리하여 각 채널에 대한 참여자의 접근을 통제할 수 있고, 스마트 계약(체인 코드) 코딩을 통해 구현함으로서 프라이빗(Private) 데이터에 대한 접근을 통제할 수 있다. 암호화 기능은 프라이빗 데이터를 일방향 암호화(해시) 또는 양방향

암호화할 수 있다. 또한, 피어(Peer)에서 파일시스템 암호화를 통해 분산원장 데이터를 암호화할 수 있고, 피어 간 전송 구간 암호화는 전송 계층 보안 프로토콜(Transport Layer Security: TLS)을 활용하여 암호화할 수 있다[3].

2. 이더리움

이더리움(Ethereum)은 이더리움 재단(Ethereum Foundation)에서 개발 및 유지 관리하고 있는 오픈소스 기반 분산원장기술 시스템으로서 허가형(Private, Consortium) 및 비허가형(Public) 분산원장 네트워크와 스마트 계약(Smart Contract)을 제공하는 것이 특징이다[4].

이더리움에서 제공하는 보안 기능은 데이터 무결성, 신원 관리 등이 있다. 데이터 무결성 기능은 분산원장에 저장된 거래 데이터에 대한 무결성을 검사하는 기능을 제공한다. 신원 관리 기능은 일반 계정(externally owned accounts)과 계약 계정(contract accounts)으로 구분된 계정을 등록, 변경 및 삭제하는 기능을 제공한다[5].

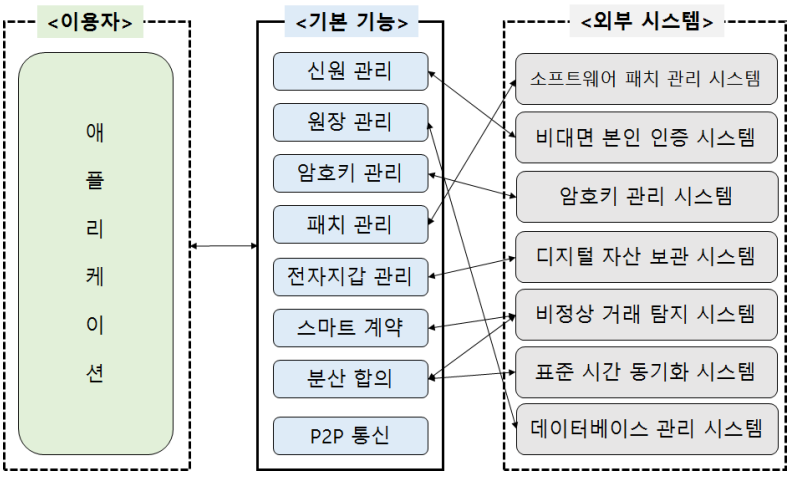
III. 분산원장기술 시스템에 대한 보안 위협

본 장에서는 이용자 애플리케이션을 구동하기 위해 오픈소스 기반 분산원장기술 시스템에서 제공하는 기능을 설명하고, 시스템 운영 시 발생할 수 있는 보안 위협을 식별한다.

1. 분산원장기술 시스템의 기본 기능

본 절에서는 이용자 애플리케이션을 구동하기 위해 오픈소스 기반 분산원장기술 시스템에서 제공하는 기본 기능을 설명한다.

분산원장기술 시스템은 이용자 애플리케이션 및 외부 시스템과 인터페이스를 가질 수 있고 신원 관리, 원장 관리, 암호키 관리, 패치 관리, 전자지갑 관리, 스마트 계약, 분산 합의, P2P 통신 등의 기본 기능으로 구성된다. 신원 관리 기능은 분산원장기술 시스템을 이용 및 운영하는 사용자를 인증하고 권한을 부여하는 것으로 외부 시스템인 비대면 인증 시스템(휴대폰 본인 인증, I-PIN 등)을 활용할 수 있다. 원장 관리 기능은 거래 데이터를



〈자료〉 서울외국어대학원대학교 자체 작성

[그림 1] 이용자 애플리케이션을 운영하는 분산원장기술 시스템

저장하고 있는 원장의 무결성을 주기적으로 점검하고 분산 합의, 스마트 계약 등에 의해 신규 원장을 추가하거나 검색하는 것으로 외부 시스템인 데이터베이스 관리 시스템을 활용하여 원장을 저장 및 검색할 수 있다. 암호키 관리 기능은 전자 서명, 데이터 암호화 등에 필요한 암호키의 생성, 분배, 접근, 파기 등을 처리하는 것으로서 외부 시스템인 암호키 관리 시스템을 활용할 수 있다. 패치 관리 기능은 분산원장기술 시스템을 구성하는 소프트웨어를 자동으로 업데이트 하는 것으로 외부 시스템인 소프트웨어 패치 관리 시스템을 활용할 수 있다. 전자지갑 관리 기능은 분산원장기술 시스템에서 제공할 수 있는 디지털 자산의 생성, 이용, 보관, 파기 등을 처리하는 것으로서 외부 시스템인 디지털 자산 보관 시스템(콜드 월렛 등)을 활용할 수 있다. 스마트 계약 기능은 이용자가 특정 조건에 만족하는 경우 자동으로 실행되는 계약을 이행하는 것으로 외부 시스템인 비정상 거래 탐지 시스템을 활용하여 이상 거래를 탐지할 수 있다. 분산 합의 기능은 신규 거래에 대한 검증과 신규 원장 생성, 공유, 검증 및 저장을 수행하는 것으로 외부 시스템인 비정상 거래 탐지 시스템을 활용하여 이상 거래를 탐지할 수 있고 또한 외부 시스템인 표준 시간 동기화 시스템을 활용하여 신규 거래 발생 시간을 정확하게 기록할 수 있다. P2P 통신 기능은 분산원장 네트워크에 참여하는 노드(컴퓨터) 간에 데이터 통신을 수행하는 것이다.

2. 분산원장기술 시스템에 대한 보안 위협

본 절에서는 이용자 애플리케이션을 구동하기 위해 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 보안 위협을 식별한다.

가. 이용자 익명성

거래의 당사자인 이용자의 신원 확인(Know Your Customer: KYC)을 이행하지 않아 익명의 이용자 간에 거래가 발생한 경우 해당 거래의 책임성을 보장할 수 없고, 또한 자금세탁 및 테러자금 조성 등에 악용될 수 있다.

나. 소프트웨어 위·변조

분산원장기술 시스템을 운영하기 위해 각 노드에 설치된 소프트웨어(스마트 계약 포함)가 악의적으로 위·변조되거나 악성 코드에 감염되면 분산원장 파괴, 서비스 지연을 초래하거나 이용자 손실이 발생할 수 있다.

다. 암호키 유출

거래 당사자인 이용자의 전자서명용 개인키를 유출하게 되면 타인에 의한 무단 거래로 인하여 이용자 손실이 직접적으로 발생하게 되고, 중요 데이터를 암호화한 암호키를 유출하게 되면 중요 데이터 유출에 따라 이용자의 2차 피해가 발생할 수 있다.

라. 비인가된 접근

분산원장에 대한 무단 접근, 스마트 계약 무단 실행, 분산원장 네트워크에 대한 무단 접근 등 비인가된 접근이 허용될 경우 서비스 중단 및 이용자 손실이 발생할 수 있다.

마. 데이터 유출 및 위·변조

분산원장 네트워크를 통해 노드 간에 거래 데이터, 원장 데이터 등을 전송 시 중간자 공격(Man-in-the-middle attack)에 의해 데이터 유출 및 위·변조가 발생할 수 있어 분산원장의 훼손 및 이용자의 2차 피해 등을 초래할 수 있다.

바. 시스템 장애

분산원장기술 시스템을 운영하기 위한 소프트웨어의 오류, 분산원장 네트워크에 참여하

는 노드의 시스템 자원(CPU, 메모리, 네트워크, 스토리지 등) 부족 등에 기인하여 서비스 지연을 초래할 수 있다.

사. 감사 기록 손실

분산원장기술 시스템 운영에 관한 기록, 이용자 행위에 관한 기록 등이 무단 변경 또는 삭제되어 보안사고 발생 시 책임 추적이 불가능할 수 있다.

3. 분산원장기술 시스템의 보안 위협 대응

본 절에서는 오픈소스 기반 분산원장기술 시스템(하이퍼레저 패브릭, 이더리움)에서 제공하는 보안 기능과 보안 위협 간의 대응 관계를 설명한다.

하이퍼레저 패브릭의 보안 기능 “데이터 무결성”은 보안 위협 “데이터 유출 및 위변조”, 보안 기능 “신원 관리”는 보안 위협 “이용자 익명성”, 보안 기능 “접근 통제”는 보안 위협 “비인가된 접근”, 보안 기능 ‘암호화’는 보안 위협 “암호키 유출”에 각각 일부 대응할 수 있으나, 보안 위협 “소프트웨어 위변조”, “시스템 장애” 및 “감사 기록 손실”에는 대응하기 어렵다.

이더리움의 보안 기능 “데이터 무결성”은 보안 위협 “데이터 유출 및 위변조”, 보안 기능 “신원 관리”는 보안 위협 “이용자 익명성”에 각각 일부 대응할 수 있으나, 보안 위협 “소프트웨어 위변조”, “암호키 유출”, “비인가된 접근”, “시스템 장애” 및 “감사 기록 손실”에는 대응하기 어렵다.

[표 1] 하이퍼레저 패브릭의 보안 기능과 보안 위협 간의 대응 관계

하이퍼레저 패브릭의 보안 기능	보안 위협						
	위협1	위협2	위협3	위협4	위협5	위협6	위협7
데이터 무결성					△		
신원 관리	△						
접근 통제				△			
암호화			△				

주 1) 위협1=이용자 익명성, 위협2=소프트웨어 위변조, 위협3=암호키 유출, 위협4=비인가된 접근, 위협5=데이터 유출 및 위변조, 위협6=시스템 장애, 위협7=감사 기록 손실

주 2) △ = 일부 대응

[표 2] 이더리움의 보안 기능과 보안 위협 간의 대응 관계

이더리움의 보안 기능	보안 위협						
	위협1	위협2	위협3	위협4	위협5	위협6	위협7
데이터 무결성					△		
신원 관리	△						

주1) 위협1=이용자 익명성, 위협2=소프트웨어 위변조, 위협3=암호키 유출, 위협4=비인가된 접근, 위협5=데이터 유출 및 위변조, 위협6=시스템 장애, 위협7=감사 기록 손실
주2) △ = 일부 대응

IV. 분산원장기술 시스템 보안 강화 방안

본 장에서는 이용자 애플리케이션을 운영하기 위한 오픈소스 기반 분산원장기술 시스템에서 발생할 수 있는 보안 위협에 대응하는 보안기능 요구사항을 도출한다. 그리고 공통평가기준에 근거한 보안기능 컴포넌트를 활용하여 보안기능 요구사항을 구현하기 위한 방안을 제안한다.

1. 보안기능 요구사항

가. 식별 및 인증

분산원장기술 시스템은 본인 확인 절차에 따라 이용자 또는 애플리케이션을 식별하고 인증하는 수단을 제공할 필요가 있다. 또한, 거래의 중요도에 따라 강화된 인증 수단(일회용 패스워드, 인증서 등)을 적용한다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(식별 및 인증 클래스, 평가대상(TOE) 접근 클래스)를 활용한다[10].

나. 보안 감사

분산원장기술 시스템은 이용자의 행위 이력을 기록하고 안전하게 보관하여 보안사고 발생에 대한 책임을 추적할 수 있는 수단을 제공할 필요가 있다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(보안감사 클래스, 평가대상의 보안기능성(TSF) 보호 클래스)를 활용한다[10].

다. 통신 보호

분산원장기술 시스템은 분산원장 네트워크에 참여하는 노드 간의 중요 정보 전송 시 안전한 통신 수단을 제공할 필요가 있으며, 또한, 분산원장기술 시스템과 외부 시스템 간의 중요 정보 전송 시 안전한 통신 수단을 제공할 필요가 있다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(통신 클래스, 평가대상의 보안기능성(TSF) 보호 클래스, 안전한 경로/채널 클래스)를 활용한다[10].

라. 암호 통제

분산원장기술 시스템은 이용자 간의 거래 시 전자서명, 중요 정보 전송 또는 저장 시 데이터 암호화 등을 위한 암호키를 안전하게 처리(생성, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(암호 지원 클래스)를 활용한다[10].

※ 국가·공공기관이 분산원장기술 시스템을 운영하는 경우, 「전자정부법」 및 시행령에 따라 국가정보원장이 승인한 암호 모듈(검증필 암호 모듈)을 사용하여야 한다[11],[12].

마. 접근 통제

분산원장기술 시스템은 비인가자가 중요 정보자산(분산원장, 스마트 계약, 분산원장 네트워크 등)에 무단으로 접근하는 것을 통제할 수 있는 수단을 제공할 필요가 있다[6]-[8]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(사용자 데이터 보호 클래스)를 활용한다[10].

바. 개인정보 보호

분산원장기술 시스템은 이용자의 개인정보가 유출 및 노출되지 않도록 안전하게 처리(수집, 이용, 보관, 파기 등)할 수 있는 수단을 제공할 필요가 있다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(프라이버시 클래스)를 활용한다[10].

※ 개인 정보를 분산원장에 저장하는 경우, 분산원장기술의 특성 상 분산원장에 한 번 저장된 정보는 변경 또는 삭제가 어려우므로 “개인정보 보호” 보안 기능은 관련 법규의 기술적 보안 요구사항인 “개인정보의 파기”를 만족하기 위해 별도의 개인 정보 분리 및 완전 삭제 기능을 구현할 필요가 있다[9],[13],[14].

사. 데이터 보호

분산원장기술 시스템은 이용자의 거래 데이터, 분산원장 데이터(개인정보 포함) 등 중요 정보가 유출 또는 위·변조 되지 않도록 안전하게 전송 또는 저장하는 수단을 제공할 필요가 있다[6]-[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(사용자 데이터 보호 클래스)를 활용한다[10].

아. 자원 가용성

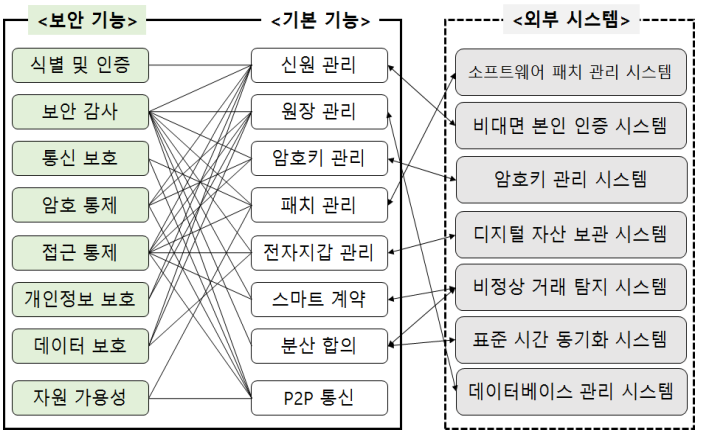
분산원장기술 시스템은 분산원장 네트워크에 참여하는 노드의 시스템 자원(CPU, 메모리, 네트워크, 스토리지 등) 부족, 분산원장기술 시스템을 운영하는 소프트웨어 오류 등에 대응하여 시스템 가용성을 극대화할 수 있는 수단을 제공할 필요가 있다[8],[9]. 본 보안기능을 구현 시 공통평가기준 보안기능 컴포넌트(자원 활용 클래스)를 활용한다[10].

2. 보안이 강화된 분산원장기술 시스템

본 절에서는 보안 기능이 반영된 분산원장기술 시스템의 모델을 제안한다.

[그림 2]의 보안이 강화된 분산원장기술 시스템 모델은 [그림 1]에서 이미 설명한 기본 기능과 외부 시스템을 포함하여 식별 및 인증, 보안 감사, 통신 보호, 암호 통제, 접근 통제, 개인정보 보호, 데이터 보호, 자원 가용성 등의 보안 기능으로 구성된다. 각 보안 기능에 대한 설명은 전술한 보안기능 요구사항을 참조한다.

[그림 2] 및 [표 3]에서 보안 기능과 기본 기능 및 보안 위협간의 연관성은 다음과 같다. 보안 기능 “식별 및 인증”은 기본 기능 “신원 관리”의 보안성을 강화하고, 보안 위협 “이용자 익명성”에 대응할 수 있다. 보안 기능 “보안 감사”는 기본 기능 “신원 관리”, “원장 관리”, “암호키 관리”, “패치 관리”, “전자지갑 관리”, “스마트 계약”, “분산 합의”, “P2P 통신”의 보안성을 강화하고, 보안 위협 “감사 기록 손실”에 대응할 수 있다. 보안 기능 “통신 보호”는 기본 기능 “패치 관리”, “P2P 통신”의 보안성을 강화하고, 보안 위협 “데이터 유출 및 위변조”에 대응할 수 있다. 보안 기능 “암호 통제”는 기본 기능 “신원 관리”, “원장 관리”, “암호키 관리”, “P2P 통신”의 보안성을 강화하고, 보안 위협 “암호키 유출”에 대응할 수 있다. 보안 기능 “접근 통제”는 기본 기능 “신원 관리”, “원장 관리”, “암호키 관리”, “패치 관리”, “전자지갑 관리”, “스마트 계약”, “P2P 통신”의 보안성을 강화하고,



〈자료〉 서울외국어대학원대학교 자체 작성

[그림 2] 보안이 강화된 분산원장기술 시스템 모델

보안 위협 “비인가된 접근”에 대응할 수 있다. 보안 기능 “개인정보 보호”는 기본 기능 “신원 관리”, “원장 관리”의 보안성을 강화하고, 보안 위협 “데이터 유출 및 위변조”에 대응할 수 있다. 보안 기능 “데이터 보호”는 기본 기능 “신원 관리”, “원장 관리”, “전자지갑 관리”의 보안성을 강화하고, 보안 위협 “데이터 유출 및 위변조”에 대응할 수 있다. 보안 기능 “자원 가용성”은 기본 기능 “패치 관리”, “P2P 통신”의 보안성을 강화하고, 보안 위협 “소프트웨어 위변조” 및 “시스템 장애”에 대응할 수 있다.

[표 3] 보안 기능과 기본 기능 및 보안 위협 간의 연관성

보안 기능	기본 기능	보안 위협
식별 및 인증	- 신원 관리	- 이용자 익명성
보안 감사	- 신원 관리 - 원장 관리 - 암호키 관리 - 패치 관리 - 전자지갑 관리 - 스마트 계약 - 분산 합의 - P2P 통신	- 감사 기록 손실
통신 보호	- 패치 관리 - P2P 통신	- 데이터 유출 및 위변조
암호 통제	- 신원 관리 - 원장 관리	- 암호키 유출

보안 기능	기본 기능	보안 위협
	- 암호키 관리 - P2P 통신	
접근 통제	- 신원 관리 - 원장 관리 - 암호키 관리 - 패치 관리 - 전자지갑 관리 - 스마트 계약 - P2P 통신	- 비인가된 접근
개인정보 보호	- 신원 관리 - 원장 관리	- 데이터 유출 및 위변조
데이터 보호	- 신원 관리 - 원장 관리 - 전자지갑 관리	- 데이터 유출 및 위변조
자원 가용성	- 패치 관리 - P2P 통신	- 소프트웨어 위변조 - 시스템 장애

〈자료〉 서울외국어대학원대학교 자체 작성

3. 보안 기능과 보안 위협 간의 대응 관계

본 절에서는 보안 기능과 보안 위협 간의 대응 관계를 설명한다.

[표 4] 보안 기능과 보안 위협 간의 대응 관계

보안 기능	보안 위협						
	위협1	위협2	위협3	위협4	위협5	위협6	위협7
식별 및 인증	O						
보안 감사							O
통신 보호					O		
암호 통제			O				
접근 통제				O			
개인정보 보호					O		
데이터 보호					O		
자원 가용성		O				O	

주 1) 위협1=이용자 익명성, 위협2=소프트웨어 위변조, 위협3=암호키 유출, 위협4=비인가된 접근, 위협5=데이터 유출 및 위변조, 위협6=시스템 장애, 위협7=감사 기록 손실
주 2) O = 대응

[표 4]는 보안이 강화된 분산원장기술 시스템 모델의 보안 기능과 3장에서 식별한 보안 위협 간의 대응 관계를 보여주고 있다. 보안 기능 “식별 및 인증”은 보안 위협 “이용자 익명성”에 대응한다. 보안 기능 “보안 감사”는 보안 위협 “감사 기록 손실”에 대응한다. 보안 기능 “통신 보호”는 보안 위협 “데이터 유출 및 위변조”에 대응한다. 보안 기능 “암호 통제”는 보안 위협 “암호키 유출”에 대응한다. 보안 기능 “접근 통제”는 보안 위협 “비인가된 접근”에 대응한다. 보안 기능 “개인정보 보호”는 보안 위협 “데이터 유출 및 위변조”에 대응한다. 보안 기능 “데이터 보호”는 보안 위협 “데이터 유출 및 위변조”에 대응한다. 보안 기능 “자원 가용성”은 보안 위협 “소프트웨어 위변조” 및 “시스템 장애”에 대응한다.

V. 결론

최근 공공 및 민간 분야에서 널리 활용되고 있는 오픈소스 기반 분산원장기술 시스템(하이퍼레저 패브릭, 이더리움 등)에서 일부 보안 기능을 제공하고 있으나 분산원장기술 시스템에서 발생할 수 있는 이용자 익명성, 소프트웨어 위·변조, 암호키 유출, 비인가된 접근, 데이터 유출 및 위·변조, 시스템 장애, 감사 기록 손실 등 보안 위협에 적절히 대응하기에는 매우 미흡하다.

본 고에서는 상기와 같은 오픈소스 기반 분산원장기술 시스템에 대한 보안 위협에 대응할 수 있는 식별 및 인증, 보안 감사, 통신 보호, 암호 통제, 접근 통제, 개인정보 보호, 데이터 보호, 자원 가용성 등 보안기능 요구사항을 도출하였다.

결론적으로 IT 제품의 보안성 평가를 위한 국제 표준인 공통평가기준(CC)의 보안기능 컴포넌트 분석을 통해 이용자 애플리케이션을 운영하는 분산원장기술 시스템에 필요한 보안 기능을 구현할 수 있는 방안을 제안함으로써 오픈소스 기반 분산원장기술 시스템의 보안을 강화하고자 한다. 마지막으로 본 고에서 제시한 분산원장기술 시스템을 위한 보안 기능 요구사항은 과학기술정보통신부와 한국정보통신기술협회(TTA)에서 추진하는 ICT 표준화전략맵 Ver.2020에 중점항목으로 선정되었고, 국내외 표준화 기구인 TTA PG502(블록체인보안) 및 ITU-T SG17(정보보호) 등에서 표준으로 개발될 예정이다.

[참고문헌]

[1] Tracy Kuhrt, Christopher Ferris, “하이퍼레저 패브릭(Hyperledger Fabric)”, 리눅스 재단, 2019. 3.
[2] 하이퍼레저 아키텍쳐 워킹그룹, “Hyperledger Architecture Volume 1,” 리눅스 재단, 2017. 8, pp.2-14.
[3] 하이퍼레저 패브릭 커뮤니티, “엔터프라이즈를 위한 블록체인 플랫폼(A Blockchain Platform for the Enterprise)”, 리눅스 재단, 2019. 3.
[4] 이더리움 커뮤니티, 이더리움, “https://www.ethereum.org/,” 이더리움 재단, 2019. 3.
[5] 이더리움 커뮤니티, 이더리움 홈스테드 문서(Ethereum Homestead Documentation), https://ethereum-homestead.readthedocs.io/en/latest/index.html,” 이더리움 재단, 2019. 8.
[6] 개인정보보호윤리과, “「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회고시 제2015-3호),” 방송통신위원회, 2015. 5.
[7] 개인정보보호정책과, “「개인정보의 안전성 확보조치 기준」(행정안전부고시 제2019-47호),” 행정안전부, 2019. 6.
[8] 전자금융과, “「전자금융감독규정」(금융위원회고시 제2018-36호),” 금융위원회, 2018. 12.
[9] 보안수준인증팀, “「정보보호 및 개인정보보호 관리체계 인증 기준」,” 한국인터넷진흥원, 2019. 1.
[10] 국가보안기술연구소, “공통평가기준 제2부: 보안기능 컴포넌트, 2017년 4월, 버전 3.1 리비전 5, CCMB-2017-04-002,” 2017. 4, pp.21-180.
[11] 전자정부정책과, “「전자정부법」,” 행정안전부, 2017. 10.
[12] 전자정부정책과, “「전자정부법 시행령」,” 행정안전부, 2018. 12.
[13] 개인정보보호윤리과, 통신정책기획과, 사이버침해대응과, 이용자정책총괄과, 인터넷윤리팀, “「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,” 과학기술정보통신부, 방송통신위원회, 2018. 12.
[14] 개인정보보호정책과, “「개인정보 보호법」,” 행정안전부, 2017. 7.