블록체인을 활용한 USB 보안관리 강화 방안

심기천, 오한수, 김희연, 임준혁, 김기형*, 김선영**

아주대학교

lemon7504@ajou.ac.kr, ogemini@ajou.ac.kr, heey08@ajou.ac.kr, amigojun@ajou.ac.kr,
*kkim86@ajou.ac.kr, **syk2009@ajou.ac.kr

USB Security Management Enhancement Method Using Blockchain

Ki-Chun Sim, Han-Su Oh, Hee-Yeon Kim, Jun-Hyeok Im,

Ki-Hyung Kim*, Sun-young Kim**

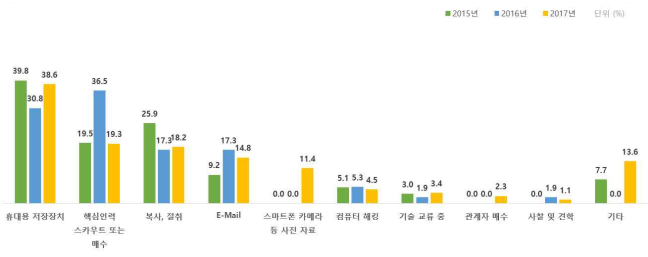
Ajou Univ.

요 약

4차 산업혁명 시대에 들어섬에 따라 기술 및 기술유출 방지의 중요성이 점점 증가하고 있다. 특히 기술유출 수단으로 USB가 주로 이용되고 있는 만큼 USB 보안성 강화가 필요한 상황이다. 이에 본 논문에서는 블록체인을 활용한 USB 보안관리 강화 방안을 제안한다. 이 방안에서는 DID 인증 방식이 사용되기 때문에 아이디, 패스워드 입력 방식이나 지문 인식 방식보다 더 높은 수준의 보안이 제공되고, 블록체인이 활용되기 때문에 파일 열람 기록의 무결성이 보장된다.

Ⅰ. 서 론

4차 산업혁명 시대에 들어섬에 따라 기술 및 기술유출 방지의 중요성이 점점 증가하고 있다. 이에 국가에서 산업기술유출 방지 및 보호에 관한 법률, 부정경쟁방지 및 영업비밀보호에 관한 법률 등을 제정하며 기술유출 방지에 힘쓰고 있지만, 기술유출 사건은 끊임없이 발생하고 있다. 과거에는 직접적인 문서의 이동이나 지식을 가진 핵심인력의 이직으로 인한 기술유출이 주를 이루다가, 2011년을 기점으로 이메일, USB, 외장 하드 등의 휴대용 저장장치를 이용한 기술유출이 많이 발생하기 시작하였다[1].



〔표 1〕 기술정보 유출 수단

특히 중소벤처기업부에 따르면 2015년부터 2017년까지 이용된 기술정보 유출수단 중 '휴대용 저장장치(USB, 외장하드 등)'가 38.6%로 가장 높았고, '핵심인력 스카우트 또는 매수'가 19.3%, '복사, 절취'가 18.2%, 'E-Mail'이 14.8% 등의 순이었다[2]. 이처럼 USB를 비롯한 휴대용 저장장치 보안성 강화 필요성이 증대됨에 따라 본 논문에서는 블록체인을 활용한 USB 보안관리 강화 방안을 제안한다. 먼저 2장에서 관련 기술인 블록체인, DID를 소개하고, 3장에서 블록체인을 활용한 USB 보안관리 강화 방안을 제안하며, 4장에서 결론을 맺는다.

Ⅱ. 본론

1. 배경지식

1.1. 블록체인

블록체인은 데이터가 담긴 블록들을 체인 형태로 연결하는 분산 데이터 저장 기술이다[3]. 데이터가 네트워크에 분산 저장되는 특성을 가져 위·변조가 불가능한 블록체인은 크게 퍼블릭 블록체인(Public Blockchain)과 프라이빗 블록체인(Private Blockchain)으로 나뉜다. 퍼블릭 블록체인에서는 누구나 열람 및 트랜잭션 생성 등을 할 수 있지만, 프라이빗 블록체인에서는 허가된 사용자만 열람 및 트랜잭션 생성 등을 할 수 있다.

1.2. DID

DID는 중앙 집중형 등록 기관이 필요 없는 탈중앙화된 식별자로 DID scheme, DID method, DID method-specific identifier로 나뉜다. DID scheme은 URI가 자원에 접근할 때 사용하는 프로토콜을 나타내고, DID method는 DID와 DID document가 생성, 갱신, 비활성화되는 일련의 과정을 나타내며, DID method-specific identifier는 DID document의 정확한 위치를 나타낸다. 또한 DID subject는 DID에 의해 식별되는 개체로 사람, 조직, 추상적인 개념 등 무엇이든 될 수 있으며, DID controller는 DID를 다룰 수 있는 개체로 하나 이상 존재할 수 있다[4]. DID의 소유권을 증명할 수 있는 인증 수단이 포함된 DID document는 DID controller가 DID를 다룰 수 있다는 것을 증명할 수 있게 하며, 분산원장인 블록체인에 저장된다[5].

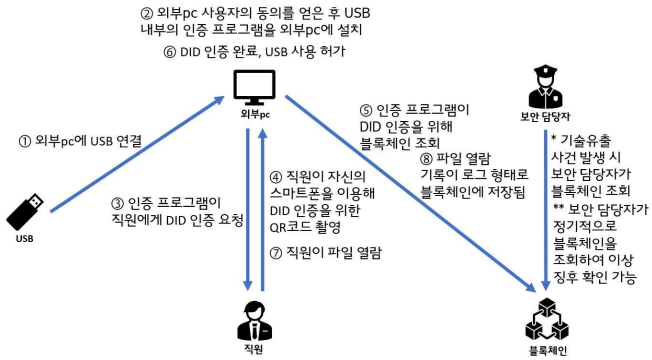
1.3. 기존 USB 작동 방식

보안 USB는 저장된 데이터를 보호하기 위해 간단한 패스워드 인증방식에서 파티션 암호화, 데이터 암호화 방식을 사용해 보안성을 강화하고 있

다[6]. 또 하드웨어 암호화를 통해 외부로부터의 위협을 막고, 파일 복사, 화면 캡처, 인쇄 등과 같은 특정 기능을 제한할 수 있는 DRM 기능을 통해 내부로부터의 위협을 막기도 한다[7].

2. 블록체인을 활용한 USB 보안관리 강화 방안과 보안성 분석

본 논문에서는 블록체인을 활용한 USB 보안관리 강화 방안을 제안하며, 이 방안이 실행되기 위해서는 직원에게 부여된 DID가 존재해야 하고, 직원이 자신의 스마트폰에 DID 인증 소프트웨어를 설치해야 하고, 직원이 USB 내부의 파일을 열람하는 것만 가능하고, 직원이 자신의 파일 열람기록을 로그 형태로 블록체인에 저장하는 것에 동의해야 한다. 블록체인을 활용한 USB 보안관리 강화 방안은 다음과 같다.



〔그림 1〕 블록체인을 활용한 USB 보안관리 강화 방안

먼저 직원이 회사 외부pc에 USB를 연결하고, 외부pc 사용자의 동의를 얻은 후 USB 내부의 인증 프로그램을 외부pc에 설치해야 한다. 외부pc 소유자의 동의하에 설치된 인증 프로그램이 pc 화면에 DID 인증 창을 생성하여 직원에게 DID 인증을 요청하면, 직원이 자신의 스마트폰에 설치된 DID 인증 소프트웨어를 통해 QR코드를 촬영한다. 이후 인증 프로그램은 DID 인증을 위해 블록체인을 조회하고, DID가 식별되면 직원의 USB 사용을 허가한다. 파일을 열람하는 직원의 행위는 로그 형태로 블록체인에 저장되며, 이는 추후 기술유출 사건 발생 시 보안 담당자가 사건의 용의자를 특정하는 데 도움을 준다. 보안 담당자가 데이터의 무결성을 보장하는 블록체인을 조회하기 때문이다. 또 보안 담당자가 정기적으로 블록체인을 조회하여 수상한 IP, 비정상적인 열람 횟수 등 이상 징후를 발견하면 기술유출을 의심해볼 수 있다.

블록체인을 활용한 USB 보안관리 강화 방안에서는 사용자 인증 방식으로 아이디, 패스워드 입력 방식이나 지문 인식 방식이 아닌 DID 인증 방식을 사용한다. 아이디, 패스워드 입력 방식에는 보안을 위해 패스워드를 주기적으로 변경해야 하고, 패스워드 유출 위협을 경계해야 하는 단점이 존재한다. 또 지문 인식 방식에는 지문 복제를 통한 허가받지 않은 제3자의 잠금 해제 위협이 존재한다는 단점이 있다. 2000년 들어 휴대전화나 출입문 등 보안이 요구되는 곳에 지문을 이용한 생체인증 시스템이 도입됐지만 이러한 지문 인식을 뚫는 기술도 같이 발전했다. 심지어 인터넷에서 실리콘·점토 등을 이용한 지문 복사 방법을 쉽게 찾을 수 있고, 지문 복사용 실리콘을 판매하는 사이트도 존재한다[8]. 반면 DID 인증 방식은 아이디, 패스워드 입력 방식이나 지문 인식 방식보다 더 높은 수준의 보안을 제공한다. 인증 프로그램으로 전송되는 DID가 유출되더라도 스마트폰에 저장된 개인키가 해킹당하지 않는 이상 안전하기 때문이다.

블록체인을 활용하여 얻을 수 있는 또 하나의 장점이 있다. 현재 사용되고 있는 보안 USB도 로그 저장 서비스를 제공하나 데이터 위변조 가능성이 존재하는데, 블록체인에 로그가 저장되면 위변조가 불가능에 가깝다. 따라서 데이터의 정확성, 일관성, 유효성이 유지되는 무결성이라는 특성을 갖는 블록체인에 파일 열람기록을 저장하면, 기술유출 사건의 책임소재를 명확히 하는 데 도움이 될 수 있다. 실제로 법정에 제출된 디지털 증거가 증거능력을 인정받기 위해서는 수집, 분석 및 제출과정에서 변경·훼손되지 않았다는 무결성이 보장되어야 한다[9].

Ⅲ. 결론

본 논문에서는 기술유출 수단으로 많이 이용되고 있는 USB의 보안성 강화를 위해 블록체인을 활용한 USB 보안관리 강화 방안을 제안하였다. 이 USB 보안관리 강화 방안에서는 데이터의 무결성을 보장하는 블록체인을 활용하기 때문에 기술유출 사건이 발생했을 때, 보안 담당자나 수사기관이 직원의 파일 열람기록을 신뢰하고 수사에 활용할 수 있다. 또 사용자 인증 방식으로 DID 인증 방식을 사용하기 때문에 아이디, 패스워드 입력 방식이나 지문 인식 방식을 사용할 때보다 더 높은 수준의 보안이 제공된다. 추후 파일을 추적하는 방안을 모색하여 파일 열람뿐만 아니라 이동, 복사 등을 가능하게 하는 연구가 진행된다면 본 논문에서 제안하는 USB 보안관리 강화 방안이 더욱 정교해질 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업과 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업과 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원과 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원의 연구결과로 수행되었음.
(IITP-2021-0-01835, IITP-2022-2018-0-01396, P0008703, 2022년 산업혁신인재성장지원사업, 2021R1F1A1045861, 2021-0-00590, 대규모 노드에서 블록단위의 효율적인 거래 확정을 위한 최종성 보장 기술개발)

참 고 문 헌

[1] 장항배, "산업기밀 유출사고 사례분석을 통한 유형별 대응방안 연구", pp. 44, 2015

[2] 김진석, "산업 기술유출 방지를 위한 기술·규모별 보안관리 및 기술유출 대응방안 연구", pp. 21, 2019

[3] Satoshi Nakamoto, "Bitcoin : A Peer-to-Peer electronic Cash System", pp. 1-8, 2008

[4] W3C, "Decentralized Identifiers (DIDs) v1.0.", 2022

[5] ETRI 블록체인기술연구센터·윤대근, "자기주권 신원증명 구조 분석서", pp. 40-41, 2020

[6] 김민호, "소프트웨어 기반 보안 USB에 대한 취약성 분석 방법론", pp. 1345-1347, 2012

[7] https://www.secudrive.co.kr/category/usb-security/page/2/

[8] https://www.joongang.co.kr/article/25025362#home

[9] 최복용, "블록체인을 활용한 디지털 증거의 무결성 강화 방안 연구", pp. 297, 2016