https://doi.org/10.5392/JKCA.2018.18.06.434

클라우드 환경에서 블록체인관리서버를 이용한 인증기반 내부망 분리 보안 모델

Internal Network Partition Security Model Based Authentication using BlockChain Management Server in Cloud Environment

김영수, 이병엽
배재대학교 사이버보안학과

Young Soo Kim(experkim@gmail.com), Byoung Yup Lee(bylee@pcu.ac.kr)

요약

오늘날 보안 위협이 점차 증가하고, 인터넷을 통한 외부악성 코드에 감염된 디바이스에 의해서 중요 데이터가 유출되는 피해가 증가하고 있다. 따라서 내부망에 연결된 디바이스에 대한 인증을 통해서 업무용 서버로의 접근을 차단하는 내부망 분리 모델이 필요하다. 이를 위한 VDI (Virtual Desktop Infrastructure)방식을 사용한 논리적 망 분리는 내부망에 연결된 물리 디바이스와 가상 디바이스 간에는 정보 교환이 차단되는 방식으로 중요 데이터의 유출을 방지하고 있으나 미등록 디바이스를 사용하여 내부망의 업무용 서버에 접근하여 중요 자료를 유출하는 공격에는 취약하다. 따라서 이의 해결책으로 VDI(Virtual Desktop Infrastructure) 기술에 블록체인 기술을 수용하여 블록체인 기반 망 분리 모델을 제안한다. 이는 VDIVirtual Desktop Infrastructure) 방식의 논리적 망 분리의 보안 취약점인 디바이스의 위변조에 대한 식별 능력과 디바이스의 무결성 강화를 통한 내부의 중요 데이터의 유출 위협을 감소시키는데 기여한다.

■ 중심어 : | 클라우드 | 블록체인 | 인증 | MAC주소 | 내부망분리 | 보안 |

Abstract

Recently, the threat to the security and damage of important data leaked by devices of intranet infected by malicious code through the Internet have been increasing. Therefore, the partitioned intranet model that blocks access to the server for business use by implementing authentication of devices connected to the intranet is required. For this, logical net partition with the VDI(Virtual Desktop Infrastructure) method is no information exchange between physical devices connected to the intranet and the virtual device so that it could prevent data leakage and improve security but it is vulnerable to the attack to expose internal data, which has access to the server for business connecting a nonregistered device into the intranet. In order to protect the server for business, we suggest a blockchain based network partition model applying blockchain technology to VDI. It contributes to decrease in threat to expose internal data by improving not only capability to verify forgery of devices, which is the vulnerability of the VDI based logical net partition, but also the integrity of the devices.

■ keyword : | Cloud | BlockChain | Authentication | MAC Address | Internal Network Partition | Security |

* 이 논문은 2018학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임.
접수일자 : 2018년 04월 16일
심사완료일 : 2018년 05월 14일
수정일자 : 2018년 05월 14일
교신저자 : 이병엽, e-mail : bylee@pcu.ac.kr

Ⅰ. 서론

인터넷망과 내부 을 분리하는 망 분리 방식은 크게 물리적 망 분리와 논리적 망 분리로 나눌 수 있다. 물리적 망 분리는 물리적으로 두 대의 PC를 사용하여 한 대는 내부망에 연결하고 다른 한 대는 인터넷 망에 연결하면서 두 대의 PC 간의 연결을 완전히 차단하는 방식이다. 물리적인 망 분리는 보안 관점에서 보면 외부의 공격으로부터는 완전히 안전하다고 생각할 수 있다. 그러나 물리적으로 2대의 터미널 단말을 분리하더라도 각 터미널 단말의 악의적인 사용자의 중요 데이터의 복제를 통한 정보 이동 및 유출에 있어서는 상당히 취약하다[1-5]. 이를 방지하기 위한 보안 솔루션으로 VDI (Virtual Desktop Infrastructure)를 이용한 논리적 망 분리 기술이 등장하였다. VDIVirtual Desktop Infrastructure) 방식은 클라우드 시스템에서 제공되는 서비스로 사용자의 터미널 단말이 바이러스에 감염되어 저장된 데이터가 손실될 경우 정보 자산에 대한 안전성을 제공할 수 없다는 단점이 있고 터미널 단말의 MAC(Media Access Control) 주소의 위변조를 통한 불법적인 업무서버에 접속하여 중요 데이터를 유출할 수 있는 취약점이 존재한다[6-8]. 이의 해결을 위하여 무결성을 보장하는 블록체인 플랫폼을 사용하는 블록체인 관리서버를 구축할 필요가 있다. 블록체인관리서버에 탑재되는 터미널의 단말 정보 DB와 트랜잭션 검색 키워드 DB는 클라우드 시스템을 이용하여 구축할 수 있다. 클라우드와 블록체인을 결합하여 블록체인기반 응용시스템을 구축하는 경우에 허가된 기관의 블록체인 노드만이 트랜잭션의 생성에 참여하고 트랜잭션 검색은 모든 참여자가 수행하는 구조를 갖는다. 물론 블록체인이 클라우드에 종속되는 것은 아니고 서로 대치되는 네트워크 구조로, 혼합하면 부족한 부분을 서로 보완해줄 수 있는 클라우드 보완 기술로 블록체인기술을 활용할 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 내부망 분리 모델을 분석하고 3장에서는 블록체인 모델을 분석하였다. 4장에서는 내부망 분리 모델에 블록체인 모델을 접목한 블록체인관리서 기반 내부망 분리 보안 모델을 제안한다. 5장에서는 결론과 시사점을 기술한다.

Ⅱ. 내부망 분리 모델

2.1 MAC 어드레스 기반 인증 모델

MAC(Media Access Control) 어드레스는 네트워크 인터페이스에 할당된 고유의 식별 주소로 OSI 모델의 MAC Protocol에서 사용한다. 따라서 MAC 어드레스는 고유의 식별 주소를 부여 받음에 따라, MAC 어드레스를 통한 인증이 가능하다. MAC 어드레스 기반 인증 방식은 인트라넷 환경에서 네트워크 접근제어를 위하여 주로 사용한다. MAC 어드레스 인증 방식은 네트워크에 연결된 적합한 단말의 MAC 주소를 인증서버에 등록하여, 단말의 네트워크 접속 요청 시 단말의 MAC 어드레스가 서버에 등록되어 있을 경우 연결을 승인하는 방식이다[9][10]. 따라서 기기의 MAC 어드레스를 사전에 서버에 등록해야 하며, 서버는 기기들의 MAC 어드레스 테이블을 관리한다.

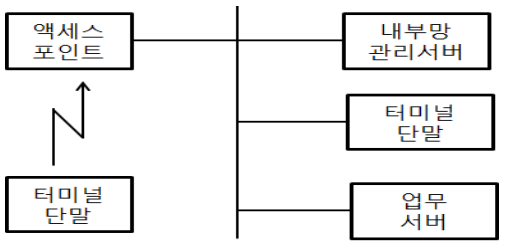

그림 1. MAC Address 기반 인증 모델

[그림 1]과 같은 일련의 과정을 통하여 인증이 수행된다. 내부망 관리서버의 인증자는 터미널의 단말 정보로부터 ID, 패스워드, MAC 어드레스를 추출하고 등록 유무를 확인하거나 MAC 어드레스에 연결된 IP 어드레스가 유효한지를 검사하여 1차 인증을 수행한다. 1차 인증이 성공하면 내부망 관리서버의 인증자는 클라이언트 단말에 인증서를 요청하여 그 요청한 인증서를 이용하여 2차 인증을 수행한다. 내부망 관리서버의 인증자는 인증 수행 이전에 클라이언트 단말로부터 단말 정보를 제공 받아 제공 받은 단말 정보를 저장하고, 내부

망 관리서버의 인증자로부터 인증서를 발급 받아 발급 받은 인증서를 클라이언트 단말에 미리 제공한다. 2차 인증이 성공하면 터미널 단말은 내부망을 사용하여 업무서버에 접속한다.

MAC 어드레스 기반 인증기술은 비교적 간단하고 속도도 빠르다는 장점이 있다. 하지만 최근 MAC 어드레스 위조가 가능함에 따라 사실상 MAC 어드레스 기반 인증은 상당히 취약하며, MAC 어드레스 테이블을 관리해야 하여 새로운 기기의 추가나 수정시 관리상에 어려움이 있다.

2.2 VDI(Virtual Desktop Infrastructure) 기반 망 분리 모델

인터넷 망과 내부망을 분리하는 망분리 방식은 크게 물리적 망분리와 논리적 망분리로 나눌 수 있다. 물리적 망 분리는 물리적으로 두 대의 PC를 사용하여 한 대는 내부망에 연결하고 다른 한 대는 인터넷 망에 연결하면서 두 대의 PC 간의 연결을 완전히 차단하는 방식이다. 물리적인 망분리는 보안 관점에서 보면 외부의 공격으로부터는 완전히 안전하다고 생각할 수 있다. 그러나 물리적으로 2대의 터미널 단말을 분리하더라도 각 터미널 단말간의 의도된 사용자의 중요데이터의 복제를 통한 정보 이동 및 유출에 있어서는 상당히 취약하다[11-16]. 이를 방지하기 위한 보안 솔루션으로 VDI(Virtual Desktop Infrastructure) 기반 망 분리 방식과 서버기반 컴퓨팅(SBC; Server Based Computing)) 방식의 논리적 망 분리 모델이 활용된다. 본 논문의 제안 모델에서 사용하는 VDI(Virtual Desktop Infrastructure) 방식은 [그림 2]와 같은 일련의 과정을 통하여 망 분리를 수행한다. 사용자의 단말은 기본적으로 호스트 OS가 활성화된 상태로 시작하고 내부망에 연결되어 있는 내부 사이트에 접속 가능한 반면, 외부 인터넷망에 연결되어 있는 웹사이트에는 접속이 불가능한 상태이다. 하지만 호스트 OS가 활성화된 상태의 사용자 단말에서 외부 인터넷망의 접속 인터페이스를 통한 웹사이트 접속 요청을 망 분리 관리서버에 전송하여 인터넷을 이용한다. 망 분리 관리서버는 웹사이트 접속 요청에 포함된 웹사이트의 도메인 네임을 IP 주소로 변환하고, 변환된 IP 주소가 내부 사이트의 IP 리스트에 속하는지 IP 리스트를 검색하여 웹사이트 접속 요청이 외부 인터넷에 대한 접속 요청임을 식별한다. 이때 망 분리 관리 서버는 웹사이트 접속 요청에 포함된 OS 지시자를 검출하여 사용자 단말이 호스트 OS로 운용되고 있음을 확인할 수 있다. 호스트 OS로 운용되고 있는 사용자 단말이 외부망에 연결되어 있는 웹사이트에의 접속을 요청하고 있으므로, 망 분리 관리 서버는 자신에게 접속을 시도하는 사용자 단말에게 OS 전환 지시를 전송하면 사용자 단말이 호스트 OS를 비활성화하고 게스트 OS를 활성화한다. 게스트 OS가 활성화된 사용자 단말은 VDI(Virtual Desktop Infrastructure) 기반 프라이빗 클라우드 서버에 웹사이트 접속 요청을 전송하고 웹서비스를 이용한다. VDI(Virtual Desktop Infrastructure) 방식을 사용한 논리적 망 분리는 인터넷 접속을 위한 가상 디바이스를 VDI(Virtual Desktop Infrastructure) 기반 프라이빗 클라우드 서버에서 구동하고 그 디바이스의 화면만 물리 디바이스로 전송하여 내부망에 연결된 물리 디바이스와 가상 디바이스 간에는 정보 교환이 차단되는 방식으로 중요 데이터의 유출을 방지하고 있다.

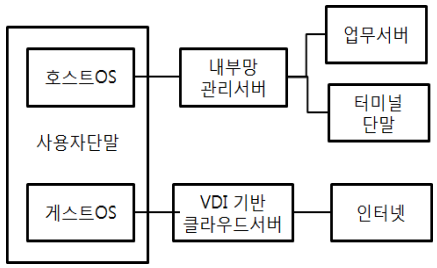

그림 2. VDI(Virtual Desktop Infrastructure) 기반 망 분리 모델

VDI(Virtual Desktop Infrastructure) 방식은 별도의 비용 없이 구축이 가능한 반만 사용자의 PC가 바이러스에 감염되어 저장된 데이터가 손실될 경우 정보 자산에 대한 안전성을 제공할 수 없다는 단점이 있다. 또한 터미널 단말의 MAC 주소의 위변조를 통한 불법적인 업무서버에 접속하여 중요 데이터를 유출할 수 있는 취약점이 존재한다.

Ⅲ. 블록체인 모델

3.1 프라이빗 블록체인 모델

블록체인은, 컴퓨터 네트워크 상에서 사용자 각자가 생성한 디지털 데이터의 집합인 블록을 생성하고, 이전 블록을 포함하는 위·변조 검증 메커니즘이 적용되어 다수의 블록들이 연결 관계를 갖게 되는 일종의 분산형 데이터베이스를 의미한다. 블록체인은 또한 웹처럼 인터넷을 기반으로 한다. 인터넷은 하나의 공개망과 변형된 여러 개의 사설망으로 이루어진다. 블록체인도 비슷한 흐름을 타고 공개 블록체인과 비공개 블록체인으로 분류된다. 프라이빗 블록체인은 모든 사용자가 참여할 수 있는 퍼블릭 블록체인과 달리 미리 기관으로부터 인증된 사용자만 참여할 수 있다는 특징이 있다[17-19]. 모든 노드가 트랜잭션을 검증할 수 없고, 노드별로 권한을 다르게 설정이 가능하다. 커스텀하게 블록체인 엔진을 수정할 수 있고, 엔진에서 제공해야만 가능한 기능들을 추가 할 수 있다. 또한 클라우드와 블록체인 결합형인 프라이빗 블록체인을 사용하여 분산형 애플리케이션을 구축하는 경우에 블록체인이 클라우드에 종속되는 구조가 아닌 서로 대치되는 네트워크 구조로서 서로 부족한 부분을 보완해줄 수 있도록 구축하여 블록체인기술을 클라우드 보완기술로 활용할 수 있다. 블록체인의 애플리케이션 모델은 [그림 3]과 같이 웹서버를 통한 블록체인 API를 이용하는 방식과 직접 블록체인 API를 이용하는 2가지로 방식으로 분류된다.

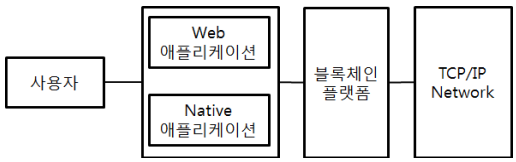

그림 3. 블록체인의 애플리케이션 모델

웹기반으로 블록체인에 접속할 수 있는 웹서버를 통한 웹 애플리케이션을 개발하여 웹을 통한 블록체인을 사용한다. 또는 블록체인 네트워크를 구성하는 노드에서 블록체인 API를 통해서 직접 접속하는 형태의 애플리케이션을 활용하는 방식으로 블록체인 애플리케이션은 인터넷을 필요로 하지만 웹은 거치지 않아도 되기 때문에 웹보다 더욱 공정하고 탈중앙화된 환경을 제공한다.

3.2 이더리움 기반 DApp 모델

이더리움은 비트코인과 같이 블특정 다수가 네트워크에 참여하는 퍼블릭 블록체인이다. 퍼블릭 블록체인은 네트워크를 유지 관리하는데 많은 자원이 투입되고 처리속도가 느리다는 단점이 있고 모든 사용자들이 트랜잭션을 생성하거나 모든 트랜잭션의 데이터를 확인할 수 있다. 그러나 애플리케이션에 따라 법적으로 책임질 수 있는 기관 그룹 간에만 트랜잭션 데이터가 공개되고 개별 사용자에게는 공개해서는 안 되고 경우에는 기관만이 트랜잭션을 생성하고 확인할 수 있는 기능이 요구되는데 이는 인증된 참여자만을 대상으로 분산 네트워크를 구성하는 프라이빗 블록체인의 구축이 필요하다. 이더리움 프로토콜 위에 분산화된 애플리케이션(Decentralized application, Dapp)을 구축해 이더리움의 스마트 계약 기능을 실행하고 그들 고유의 토큰을 생성할 수 있는 프라이빗 블록체인은 기업의 목적에 부합하는 특화형 설계가 보다 용이하며, 금융, 의료, 무역 등 다양한 분야에 폭넓게 응용되어 사용한다[20][21]. 이더리움 기반 Dapp 모델은 [그림 4]와 같이 이더리움 플랫폼을 이용하여 응용 로직을 담고 있는 스마트 컨트랙트를 작성하고 이를 실행하는 dapp을 통하여 스마트 컨트랙트의 결과를 블록체인에 기록하고 검색하는 등의 처리를 할 수 있다. Ethereum에서의 P2P 네트워크를 사용한 파일 송수신 프로토콜인 Swarm은 콘텐츠를 다운받거나 업로드 할 수 있는 기능에 고유한 시드값의 암복호화를 통한 인증을 제공한다. Whisper는 Ethereum에서의 P2P 네트워크를 사용한 메시지 전송 프로토콜로 해시된 토픽을 기반으로 노드 간에 P2P 통신을 하고, 메시지 암호화와 디지털 서명을 통해 데이터의 무결성 및 기밀성을 제공한다.

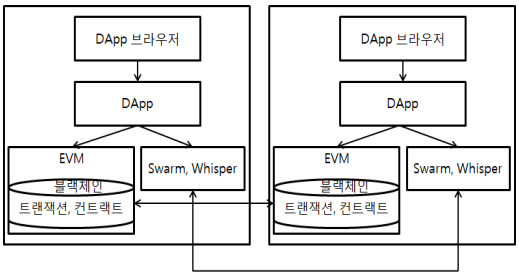

그림 4. 이더리움 기반 DApp 모델

Ⅳ. 블록체인관리서버를 이용한 인증기반 내부망 분리 보안 모델

4.1 블록체인관리서버를 이용한 내부망 분리 모델

블록체인 관리서버는 단말정보 DB와 트랜잭션 검색 키워드 DB를 탑재하고 트랜잭션을 관리하고 스마트 컨트랙트를 사용하여 MAC 어드레스 기반 인증 모델에서 사용하는 단말정보와 동일한 정보를 사용하여 터미널 단말을 등록하고 단말 검증을 통한 인증을 하는 모델을 사용한다. [그림 5]와 같이 내부망 분리 모델과 블록체인 모델을 수용한 블록체인 관리서버를 이용한 내부망 분리 모델을 제안한다. 기존의 내부망 관리서버를 블록체인 관리서버로 교체하고 있다. 사용자의 터미널 단말은 DApp브라우저에서 실행되는 DApp을 통하여 내부망에 접속하는 경우에 DApp은 단말로부터 MAC주소와 IP주소를 추출하여 단말정보를 구성하고 이를 블록체인관리서버에 전송한다. 블록체인관리서버는 사전에 등록한 단말정보 DB와 매칭을 수행하고 매칭이 되는 정보가 존재하면, 트랜잭션으로 가공하고 스마트 컨트랙트로 전송한다. 스마트 컨트랙트는 트랜잭션을 생성 배포하고 트랜잭션정보를 검색하는데 키 값으로 이용되는 트랜잭션 ID정보를 생성하여 블록체인관리서버의 검색키워드 DB에 저장 관리하고 이를 터미널 단말의 검증에 활용한다. 트랜잭션은 블록체인 보유서버로 동작하는 블록체인 네트워크를 구성하는 노드의 블록체인에 저장된다.

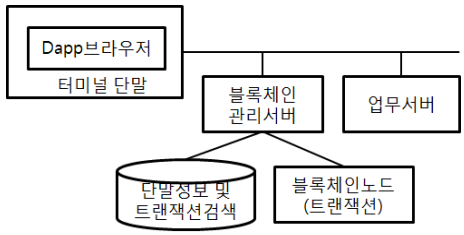

그림 5. 블록체인 관리서버를 이용한 터미널 단말 인증 모델

블록체인 관리서버에 의한 터미널 단말의 인증이 성공하면 웹사이트 접속 요청에 포함된 웹사이트의 도메인 네임을 IP 주소로 변환하고, 변환된 IP 주소가 내부 사이트의 IP 리스트에 속하는지 IP 리스트를 검색하여 외부 인터넷에 대한 접속 요청임을 식별한다. [그림 6]과 같은 일련의 과정을 통하여 내부망과 외부망의 분리를 수행한다. 블록체인 관리서버의 IP주소 변환 모듈은 도메인 서비스를 이용하여 내부 사이트의 도메인 네임 및 외부의 웹사이트의 도메인 네임을 IP 주소를 변환한다. 사이트 식별 모듈은 IP 주소 변환 모듈에서 변환된 IP 주소를 이용하여 IP 주소가 내부망에 연결되어 있는 내부 사이트의 IP 주소인지 또는 외부망에 연결되어 있는 웹사이트의 IP 주소인지 여부를 판단한다.

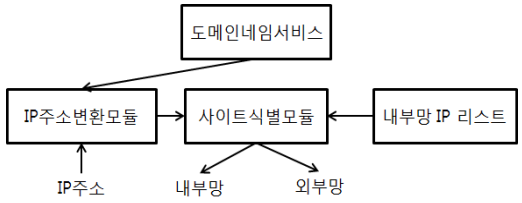

그림 6. 블록체인 관리서버의 사이트 식별 모델

블록체인 관리서버에는 DB가 탑재되고, 그 탑재된 DB에는 사용자의 식별정보로 이루어진 단말정보와 트랜잭션정보를 검색하는데 키 값으로 이용되는 사용자별 트랜잭션 검색 키워드정보 DB를 갖는다. 트랜잭션은 터미널 단말 정보의 인증 요청 그리고 트랜잭션 검색 요청시에 생성되어 블록체인에 기록된다. 블록체인 관리서버의 트랜잭션 검색 모델은 [그림 7]과 같다. 블록체인관리서버는 트랜잭션처리엔진을 운영하여 터미널 단말 인증과 사용자 별 트랜잭션 검색을 수행한다.

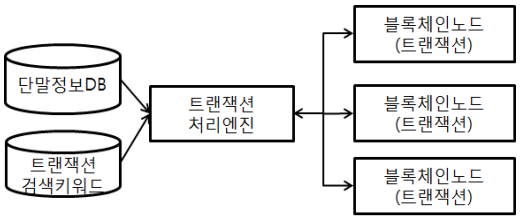

그림 7. 블록체인 관리서버의 트랜잭션 검색 모델

4.2 응용모델 및 실용성 확인

블록체인 관리서버를 이용한 내부망 분리 모델의 실용성 확인을 위한 응용 구조는 [그림 8]과 같다. 응용모델의 구현을 위하여 애저(Azure) 클라우드에서 제공하는 블록체인 서비스의 개발 환경 및 기능을 활용하여 제안 모델을 구현하였다. 블록체인 관리서버는 웹사이트 접속 요청에 포함된 IP주소와 MAC주소를 검출하여 터미널 단말의 인증과 사이트 식별을 수행한다. 터미널 단말의 인증이 성공하고 외부 웹사이트로 식별이 되면 VDI(Virtual Desktop Infrastructure) 기반 클라우드 서버에 웹사이트 접속 요청을 전송하고 웹서비스를 제공받는다.

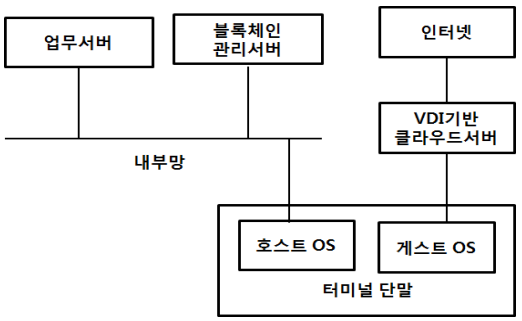

그림 8. 블록체인 관리서버의 응용 모델

VDI(Virtual Desktop Infrastructure) 기반 클라우드 서버는 인터넷 접속을 위한 가상 디바이스를 구동하고 그 디바이스의 화면만 터미널 단말로 전송함으로써 사용자의 터미널 단말이 바이러스에 감염되어도 사용자의 데이터가 서버에 남아 있기 때문에 정보 자산에 대한 보호를 제공하고 내부망에 연결된 물리 디바이스와 가상 디바이스 간에는 정보 교환이 차단되는 방식으로 중요 데이터의 유출을 방지한다.

우리의 제안 모델은 VDI(Virtual Desktop Infrastructure) 기반 클라우드 서버의 취약점인 업무망 네트워크에 연결되는 터미널 단말의 도용을 방지하기 위하여 터미널 단말의 등록 정보를 변경하지 못하도록 블록체인의 불역성 특성을 활용한 블록체인관 리서버를 이용하고 있다. 또한 애저(Azure) 클라우드 서비스를 이용하여 업무서버, VDI 구현 서버, 블록체인관리서버, 이더리움 노드 3개로 구성된 내부망을 구축하고 터미널 단말의 등록 및 인증에 대한 내용에 한해서 블록체인에 저장하였고 터미널 단말의 추가적인 식별정보와 트랜잭션 검색 정보는 블록체인관리서버의 데이터베이스에 저장하였다. 기존의 VDI기반 클라우드 서버의 보안취약점을 제거하기 위하여 무결성 특성을 갖는 블록체인 관리서버를 이용함으로써 구축 비용은 조금 증가하였으나 터미널 단말의 등록 요청 및 인증 요청을 블록체인 저장함으로써 악의적인 수정 및 변경에 따른 보안위협을 차단하고 업무서버를 이용하는 터미널 단말의 분석 정보에 신뢰성을 제공한다.

블록체인관리서버의 데이터베이스에 터미널 단말의 MAC주소와 이의 블록 해쉬값을 매핑한 테이블을 구성하여 터미널 단말의 인증 트랜잭션에 대한 검증을 실험하였다. [표 1]과 같이 터미널 단말의 유형에 따라서 인증 트랜잭션의 성공 유무를 확인하였다.

표 1. 인증 트랜잭션의 성공 유무

터미널단말유형	트랜잭션개수	인증성공개수	인증실패개수
등록단말	100	100	0
미등록단말	100	0	100
위조공격단말	100	0	1000

우리의 제안 모델은 블록체인관리서버의 동작에 오류가 없고 내부망 분리에 적용하여 터미널 단말에 대한 인증 및 무결성을 담보함으로 내부망을 통한 중요자산 유출 공격을 사전 예방하는 효과를 얻고 미인가 된 공격자에 의한 업무서버공격에 감내할 수 있는 해결 방안으로 사용될 수 있음을 확인하였다.

V. 결론

물리적인 망분리는 보안 관점에서 보면 외부의 공격으로부터는 완전히 안전하다고 생각할 수 있다. 그러나 물리적으로 2대의 터미널 단말을 분리하더라도 각 터미널 단말의 악의적 사용자가 중요 데이터의 복제를 통한 정보 이동 및 유출에 있어서는 상당히 취약하다. 또한 VDI 방식의 데스크탑 가상화 방식은 사용자의 터미널 단말이 바이러스에 감염되어 저장된 데이터가 손실될 경우 정보 자산에 대한 안전성을 제공할 수 없다는 단점이 있고 터미널 단말의 MAC 주소의 위변조를 통한 불법적인 업무서버에 접속하여 중요 데이터를 유출할 수 있는 취약점이 존재한다. 이의 해결을 위해서 블록체인 관리서버를 이용한 인증기반 망분리 보안 모델을 제안하고 이의 실용성 확인을 위해서 응용시스템을 설계 및 구현하였다. 블록체인 관리서버를 이용한 인증기반 내부망 분리 보안 모델은 내부망에 연결된 디바이스에 대한 인증을 통해서 업무용 서버로의 접근을 제어하는 블록체인관리서버와 실행 결과 화면을 전송하는 VDI(Virtual Desktop Infrastructure) 방식을 사용하고 있다. 블록체인관리서버에 탑재되는 터미널 단말 정보 DB와 트랜잭션 검색 키워드 DB는 클라우드 시스템을 이용하여 구축할 수 있다. 클라우드와 블록체인을 결합하여 프라이빗 블록체인을 구축하는 경우에 허가된 기관의 노드만이 트랜잭션의 생성에 참여하고 트랜잭션 검색은 모든 참여자가 수행한다. 물론 블록체인이 클라우드에 종속되는 것은 아니고 서로 대치되는 네트워크 구조로 혼합하여 사용하면 부족한 부분을 서로 보완해 줄 수 있으므로 클라우드 보완 기술로 블록체인기술을 활용할 수 있다. 기존의 VDI(Virtual Desktop Infrastructure) 방식을 사용한 논리적 망 분리는 인터넷 접속을 위한 가상 디바이스를 VDI(Virtual Desktop Infrastructure) 기반 클라우드 서버에서 구동하고 그 디바이스의 화면만 물리 디바이스로 전송하여 내부망에 연결된 물리 디바이스와 가상 디바이스 간에는 정보 교환이 차단되는 방식으로 중요 데이터의 유출을 방지하고 있으나 미등록 디바이스를 사용하여 내부망의 업무용 서버에 접근하여 중요 자료를 유출하는 공격에는 취약하다. 또한 클라우드 서버의 관리자에 의해서 이루어지는 터미널 단말의 악의적 등록 요청에 대한 트랜잭션으로 인한 보안 위협은 완전히 차단하기 어렵다. 따라서 업무서버를 이용하는 트랜잭션의 분석 기술과 악의적 행동의 추적 기술에 대해서 스마트 컨트랙트의 활용 방안에 대한 추가 연구가 필요하다. 제안모델은 블록체인 관리서버를 사용하여 내부망에 접속하는 디바이스의 MAC(Media Access Control) 주소를 블록체인화하여 이를 관리하는 블록체인 관리서버를 구축하여 디바이스 인증을 수행하고 업무용 서버를 보호한다. 이는 기존의 VDI기반 클라우드 서버의 보안취약점을 제거하기 위하여 무결성 특성을 갖는 블록체인 관리서버를 이용함으로써 구축 비용은 조금 증가하였으나 터미널 단말의 등록 요청 및 인증 요청을 블록체인 저장함으로써 악의적인 수정 및 변경에 따른 보안위협을 차단하고 업무서버를 이용하는 터미널 단말의 분석 정보에 신뢰성을 제공한다. VDI 방식의 논리적 망 분리의 보안 취약점인 디바이스의 위변조에 대한 식별 능력과 디바이스의 무결성 강화를 통한 내부의 중요 데이터의 유출 위협을 감소시키는데 기여한다.

참 고 문 헌

[1] 김영수, 문형진, 조혜선, 김병익, 이진해, 이진우, 이병엽, “계층적침해자원기반의 침해사고 구성 및 유형 분석,” 한국콘텐츠학회논문지, 제16권, 제11호, pp.139-153, 2016.

[2] 김영수, 이병엽, “클라우드 환경에서 문서의 유형 분류를 위한 시맨틱 클러스터링 모델,” 한국콘텐츠학회논문지, 제17권, 제11호, pp.389-397, 2017.

[3] E. B. Lee, A Study on Information Security of Network Partition Based, Proc. of the KIISC Conference 20, Vol.1, pp.39-46, 2010.

[4] M. E. Kuhl, Cyber Attack Modeling and Simulation for Network Security Analysis, Simulation Conference 2007 (Winter), pp.1180-1188, 2007.

[5] J. S. Moon, Cyber Terrorism Trends and Countermeasures, Proc. of the KIISC Conference 20, Vol.4, pp.21-27, 2010.

[6] B. Lee and J. H. Lee, “Blockchain based secure firmware update for embedded devices in an Internet of Things environment,” Journal of Supercomputing, Vol.73, No.3, pp.1152-1167, 2017.

[7] Satoshi Nakamoto, "Bitcoin:A peer-topeer electronic cash system," 2008.

[8] B. Lee, Y. J. Lim, and J. H. Lee, “Consensus algorithms in block-chain platforms,” Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.386-387, 2017.

[9] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, “A timing-based scheme for rogue AP detection,” IEEE Trans. Parallel Distrib. Syst., Vol.22, No.11, pp.1912-1925, Nov. 2011.

[10] D. Inoue, R. Nomura, and M. Kuroda, Transient MAC address scheme for untraceability and DOS attack resiliency on wireless network,” in Proc. Wireless Telecommun. Symp., pp.15-23, Pomona, U.S.A., Apr. 2005.

[11] S. Banerjee, Order-P, An Algorithm To Order Network Partitionings, ICC '92, Conference record, SUPERCOMM, ICC '92, Discovering a New World of Communications, IEEE International Conference on 1, pp.432-436, 1992.

[12] Samuel T. King, SubVirt:Implementing Malware with Virtual Machines, Proceedings of the 2006 IEEE Symposium on Security and Privacy, 2006.

[13] C. Y. An and C. Yoo, Comparison of Vitualization Method, Proc. of the KIISE Korea Computer Congress 2008, Vol.35, No.1, pp.446-450, 2008.

[14] Guangda Lai, A Service Based Lightweight Desktop Virtualization System, Service Sciences (ICSS), 2010 International Conference on, pp.277-282, 2010,

[15] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," Proc. of the 9th SOSP, pp.164-177, Oct. 2003.

[16] B. Liu, L. Lishen, and X. Qin, "Research on Hardware I/O Passthrough in Computer Virtualization," Proc. of ISCSCT 2010, pp.353-356, Aug. 2010.

[17] S. H. Kim, J. Y. Yang, and Y. J. Kim, “A Study on the Selfish Mining of Block Chain,” Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.422-423, 2015.

[18] I. Eyal and Emin G. Sirer, “Majority is not Enough: Bitcoin Mining is Vulnerable,” In Financial Cryptography, pp.436-454, 2014.

[19] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp.3-16, Oct. 2016.

[20] Muneeb Ali and Jude Nelson, Blockstack: A Global Naming and Storage System Secured by Blockchains, USENIX ATC, 2016.

[21] Vitalik Buterin, “A Next Generation Smart Contract & Decentralized Application Platform,” Ethereum White Paper, 2014.

저 자 소 개

김 영 수(Young Soo Kim) 정회원

- 2003년 8월 : 국민대학교정보관리학(정보관리학박사)
- 현재 : 충남 재활IT 융합 기술원 대표 컨설턴트
- 현재 : 배재대학교 사이버보안학과

<관심분야> : 빅데이터서비스보안, 정보 보안

이 병 엽(Byoung Yup Lee) 종신회원

- 1991년 2월 : 한국과학기술원 전산학과(공학사)
- 1993년 2월 : 한국과학기술원 전산학과(공학석사)
- 1997년 2월 : 한국과학기술원 경영정보공학(공학박사)
- 1993년 1월 ~ 2003년 2월 : 대우정보시스템 차장
- 2003년 3월 ~ 2016년 2월 : 배재대학교 전자상거래학과 부교수
- 2016년 3월 ~ 현재 : 배재대학교 사이버보안학과 교수

<관심분야> : XML, 지능정보시스템, 데이터베이스시스템, 전자상거래학