Journal of Digital Convergence
Vol. 19. No. 10, pp. 287-293, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.10.287

무결성이 보장된 블록체인 기술을 활용한 PKI 기반 보안 게이트웨이의 인증 모델

김영수[1], 문형진[2*]
[1]한세대학교 IT융합전자공학과 조교수, [2]성결대학교 정보통신공학과 조교수

Authentication Model of PKI-based Security Gateway using Blockchain having Integrity

Young Soo Kim[1], Hyung-Jin Mun[2*]
[1]Assistant Professor, Department of IT Convergence, Hansei University
[2]Assistant Professor, Department of Information & Communication Engineering, Sungkyul University

요 약 최근 국가가 공인하는 인증기관에서 발행하는 공인인증서를 폐지하고 인터넷 기업이 자체적으로 공동인증서를 발급하면서 그 책임을 부여하는 방법으로 전자서명법이 개정되었다. 인터넷 기업이 인증기관으로서 발행하는 공동 인증서의 사용이 허용되면서 공개키 인증서 도용에 따른 사기 피해의 확대가 예상된다. 무결성과 보안성이 내재된 블록체인에 PKI를 결합한 보안 게이트웨이에서 사용할 수 있는 인증 모델을 제안하였다. 제안 모델의 실용성 평가를 위해서 전문가 집단을 활용한 델파이 기법으로 중요도를 도출하고 인간의 주관성을 배제하는 평가방법인 수게노의 계층퍼지적분을 이용한 인증 모델의 보안성을 평가했다. 블록체인 기반 공동인증서는 무분별한 공인인증서의 발행과 오남용을 방지하고 보안성과 편의성이 확보된 서비스의 기반기술로 활용이 기대된다.

주제어 : 블록체인, PKI, 인증, 보안 게이트웨이, 퍼지적분, 공동인증서

Abstract Recently, public certificates issued by nationally-recognized certification bodies have been abolished, and internet companies have issued their own common certificates as certification authority. The Electronic Signature Act was amended in a way to assign responsibility to Internet companies. As the use of a joint certificate issued by Internet companies as a certification authority is allowed, it is expected that the fraud damage caused by the theft of public key certificates will increase. We propose an authentication model that can be used in a security gateway that combines PKI with a blockchain with integrity and security. and to evaluate its practicality, we evaluated the security of the authentication model using Sugeno's hierarchical fuzzy integral, an evaluation method that excludes human subjectivity and importance degree using Delphi method by expert group. The blockchain-based joint certificate is expected to be used as a base technology for services that prevent reckless issuance and misuse of public certificates, and secure security and convenience.

Key Words : Blockchain, PKI, Authentication, Security Gateway, Fuzzy Integral, Joint Certificate

*This research was supported by the National Research Foundation of Korea(NRF) funded by the Ministry of Education and Ministry of Science and ICT (NRF-2019S1A5B5A07105353) in 2019.
*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received July 27, 2021 Revised August 12, 2021
Accepted October 20, 2021 Published October 28, 2021

1. 서론

웹브라우저에서 액티브X 문제로 인한 보안성과 안전성이 떨어지고 불편을 줬던 공인인증서가 폐지되었다. NPKI 디렉토리에 개인키와 공개키를 담고 있는 공인인증서를 저장하고 비밀번호를 통해 사용함으로써 비밀번호의 노출과 해킹 위험을 제공하는 암호학적 측면에서 처음부터 잘못 설계된 공인인증서였다. 또한 공인인증서를 구동을 위해 플러그인되는 액티브X 자체의 취약점 뿐만 아니라 새로운 사이트 접근시 매번 설치해야 하는 소프트웨어로 인해서 취약점은 늘어난다. 취약점으로 인해 다양한 공격으로 인한 공인인증서의 개인키가 노출될 위험이 커지는 문제점을 가지고 있었다. 인터넷을 통한 기업의 글로벌화 되면서 외국인이 국내 물품을 구매하기 위한 국내의 공인인증서 발급 등이 번거롭고 복잡함으로써 공인인증서가 글로벌화의 장애요인이 되었다[1]. 공인인증서를 폐지하고 인터넷 기업이 인증기관으로 자체적으로 공동인증서를 발급하고 책임을 부여하는 방법으로 전자서명법이 개정되었다. 인터넷 기업이 인증기관으로서 발행하는 공동인증서의 사용이 허용되면서 공개키 인증서 도용에 따른 사기 피해가 예상된다. 공개키 인증서는 거래 주체의 신분을 증명해주는 수단으로 사용되나 실체가 드러나지 않는 사이버 공간의 인증기관이 공개키 인증서를 발급으로써 신분도용이 가능하다. 또한 공동 인증서의 보관 방식에 따른 인증서 유출에 따른 보안 문제가 존재한다. 이를 위해서 PKI 기반 인증과 더불어 블록체인과 생체인증 등 다양한 인증 서비스가 요구된다. 본 논문은 PKI와 블록체인을 융합하여 블록체인 기반 보안 게이트웨이 인증 모델을 도출하고 직접 API 통신기반 인증모델과의 비교를 통해서 실용성과 보안성을 평가하였다.

본 논문의 구성은 다음과 같다. 2장에서는 PKI 인증서 확장 및 게이트웨이 모델을 조사 분석하고 3장에서는 블록체인 보안 모델을 분석하고 4장에서는 블록체인을 이용한 보안 게이트웨이의 인증 모델을 도출하고 검증 및 평가 결과를 보이고 마지막으로 시사점과 함께 결론을 맺는다.

2. PKI 인증서 확장 및 게이트웨이 모델

2.1 PKI 인증서 확장 보안 모델

PKI(Public Key Infrastructure)는 Fig. 1과 같이 비대칭키 알고리즘을 이용하여 개인키(Private Key)와 공개키(Public Key)의 한 쌍을 생성하고 개인키는 개인이 비밀로 소유하고 공개키는 공개해서 인증, 암호화, 전자서명을 제공하는 응용 환경 인프라이다[2,3].

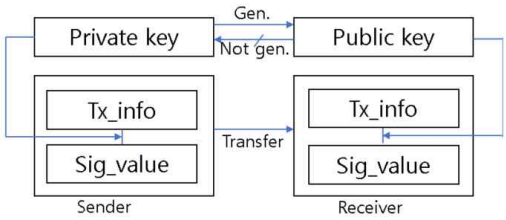


Fig. 1. Seurity Model of PKI

전자서명은 실제 이체와 같은 금융거래 사실에 대한 확인, 공공 사이트에서의 입찰 신청, 전자상거래 사실 확인을 위한 용도로 주로 사용된다[4,5]. 모든 IT 응용에서 신분증명과 전자서명은 가장 중요한 핵심요소이다. PKI 인증서 관리 모델은 Fig. 2와 같이 등록기관, 인증기관, 최상위 인증기관, 전자상거래업체의 4개의 하위 구성요소로 이루어져 있다.

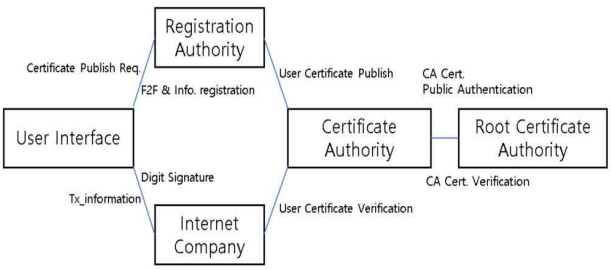


Fig. 2. Management Model of Certificate

PKI는 본인인증과 부인방지 기능을 제공하는 탁월한 기술로 다양한 인증기술과 결합되어 안전하고 편리한 인증서비스가 연구되고 있다. PKI 기반 바이오 정보 인증서비스는 Fig. 3와 같고 사용자의 얼굴과 홍채 그리고 지문과 같은 생체정보를 인식해서 사용자를 식별한 정보를 기반으로 PKI기반 인증 서비스를 제공한다.

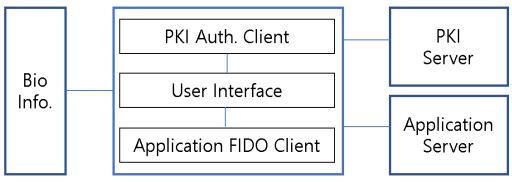


Fig. 3. The Extended Security Model of PKI Based Certificate

FIDO(Fast IDentity Online)는 생체인식을 활용해 간편하고 보안성 높은 인증체계에 대한 표준안을 만드는 국제표준단체이다[6,7]. FIDO기술은 비밀번호의 문제점을 해결하기 위한 목적으로 FIDO 얼라이언스에 의해 제안된 사용자 인증 프레임워크이다. FIDO에서 비밀번호와 같은 중요한 정보를 보내지 않는 대신 사용자의 공개키와 전자서명을 보낸다. 누구나 볼 수 있어도 문제가 없는 정보이다. FIDO 아키텍처는 Fig. 4와 같다.

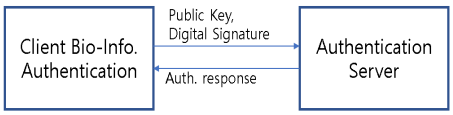


Fig. 4. FIDO Architecture

2.2 API 게이트웨이 모델

API 게이트웨이는 API 서버 앞단에서 모든 API 서버들의 엔드 포인트를 단일화 해주는 서버이다. API 게이트웨이는 요청 라우팅, 구성 및 프로토콜 변환을 담당한다. 클라이언트의 모든 요청은 먼저 API 게이트웨이를 통과한다. 그런 다음 요청의 핸들러인 라우팅 함수 내부에서 적절한 마이크로 서비스로 라우팅한다. 이는 API 게이트웨이에서 Flask 앱의 redirect나 url_for 메서드를 라우팅 함수 내부에 사용해서 API 서버의 적절한 라우팅 함수를 실행하는 방법과 같이 마이크로 서비스를 구현한다. API 게이트웨이는 종종 여러 마이크로 서비스를 호출하고 결과를 집계하여 요청을 처리한다. API 게이트웨이는 마이크로 서비스의 엔드포인트를 병합하거나 분할해서 최종 사용자가 이용하는 API 서버의 서비스에 대한 리팩토링을 용이하게 한다. 또한 애플리케이션의 서비스 구조를 캡슐화해서 특정 서비스를 직접 호출할 필요없이 클라이언트는 단순히 게이트웨이와 통신함으로써 접속 횟수가 줄고 클라이언트 코드를 단순화하는 장점을 제공한다[8-10]. API 게이트웨이의 보안 모델은 Fig. 5과 같이 마이크로 서비스 단위로 외부 호출자의 인증 및 권한 부여를 처리하는 API 보안 게이트웨이이다.

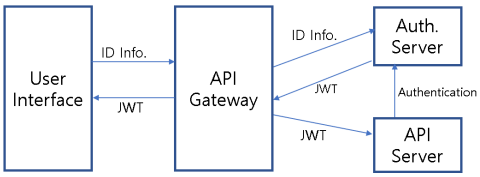


Fig. 5. Security Model of API Gateway

사용자는 로그인시에 API 게이트웨이를 통해서 신원정보를 인증서버로 전달한다. 인증서버는 JWT(Json Web Token)을 생성하여 사용자에게 반환한다. 사용자 클라이언트는 특정 리소스에 액세스할 때마다 API 게이트웨이에 요청과 함께 JWT를 보낸다. API 게이트웨이는 JWT와 함께 요청을 이 리소스를 소유한 마이크로 서비스로 전달한다. 그런 다음 마이크로 서비스는 인증 서버에게 JWT를 전달하여 사용자의 접근 권한을 검증해서 서비스를 제공한다[11,12].

3. 블록체인 보안 모델

3.1 스마트 컨트랙트 모델

스마트 컨트랙트를 이용한 블록체인 네트워크의 구축은 산업 전분야에 빠르게 확산되고 있다. 스마트 컨트랙트는 블록체인에 저장된 프로그램을 말한다. 블록체인에 탑재되는 스마트 컨트랙트는 비즈니스 로직과 인증 및 암호화 등의 보안 기능을 구현해서 사용한다. 스마트 컨트랙트 모델은 Fig. 6과 같이 사용자와 블록체인 사이에서 중개자 역할을 수행한다. 상태 트랜잭션은 모든 블록체인의 노드들이 공유하기 때문에 스마트 컨트랙트의 실행 결과를 조작하는 것은 불가능하다. 모든 블록체인 노드의 상태 트랜잭션은 무결성이 보장된다[13].

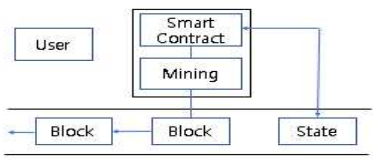


Fig. 6. Smart Contract Model

3.2 스마트 컨트랙트의 응용 모델

스마트 컨트랙트를 이용한 가상은행은 송신자가 송금액을 스마트 컨트랙트에 송금하면 스마트 컨트랙트는 수신자에게 이체하는 과정을 보여준다. CA계정을 사용한 스마트 컨트랙트의 메서드를 호출한 EOA계정은 컨트랙트 상태 정보로 저장되고 컨트랙트 호출 파라미터로 금액을 넘겨주면 잔액란에 금액을 저장한다. 송신자는 수신자의 EOA계정에 금액을 이체한다.

사용자 식별 관리를 위한 스마트 컨트랙트의 응용 모델은 Fig. 7과 같다. 전자지갑의 EOA 계정을 통한 사용자의 식별은 신분증과 같은 신원 증명 관리에 소요 되는

비용과 복잡성을 감소시킨다. 스마트 컨트랙트의 프로그램 코드로 사용자 식별 정보를 관리하는 기능을 구현하고 EOA 계정과 CA계정을 사용해서 사용자 식별 정보를 스마트 컨트랙트 상태 DB에 저장하고 검색해서 확인한다[13-16].

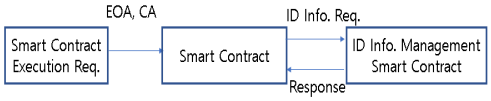


Fig. 7. Application Model of Smart Contract based ID Management

4. 인증 모델 및 검증

4.1 블록체인을 이용한 API 보안 게이트웨이 인증 모델

블록체인을 이용한 API 보안 게이트웨이의 인증 프로토콜 모델은 Fig. 8과 같이 블록체인과 API 보안게이트웨이를 사용해서 PKI 인증서를 확장한 인증 구조를 갖고 있다. 사용자는 공인 인증기관 없이 자신이 생성한 인증서를 사설 인증기관의 개인키로 인증받고 이를 블록체인에 저장한다. 사이드 체인 PKI과 생체인증의 결합을 통한 신분증명과 인증을 자동화함으로써 신분도용에 따른 사기 피해와 같은 오프체인 PKI인증서 모델의 한계점을 개선할 수 있도록 설계하였다.

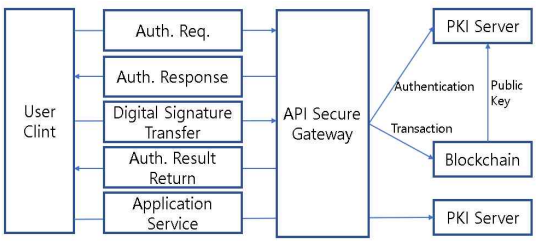


Fig. 8. PKI Authentication Model of API Security Gateway using Blockchain

4.2 보안 게이트웨이를 이용한 블록체인 기반 PKI 인증의 실용성 평가 모델

보안 게이트웨이를 이용한 블록체인 기반 PKI 인증의 실용성 평가 모델은 Fig. 9과 같고 게이트웨이 기반 보안 모델과 API 기반 보안 모델의 성능과 보안성을 비교 평가한다. 이의 성능을 확인하기 위한 모의실험은 Flask와 Flask Restful 모듈을 이용하여 보안 게이트웨이와 API를 구현하였고 pycrypto 모듈을 이용하여 PKI 시스템을 구축하였다. 또한 블록체인 노드는 이더리움 풀 노드를 사용하였다. 실용성 평가 실험은 공개키 인증서를 등록하고 보안 게이트웨이와 로컬 이더리움을 경유하는 보안게이트웨이 기반 인증과 직접 API 서비스를 경유해서 PKI시스템을 사용하는 직접 API 통신기반 인증에 소요되는 시간을 측정하여 실험하였다.

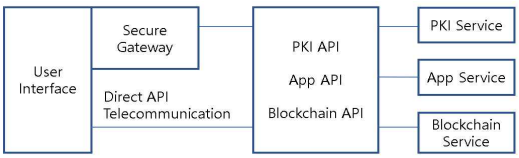


Fig. 9. Verification Model of Comparing Security Gateway and API Communication

Table 1에서 보는 것과 같이 초기 공개키 인증서 등록에 소요되는 시간은 블록체인과 PKI 모두를 사용하는 보안 게이트웨이 기반 인증보다 PKI를 이용하여 공개키 인증서를 등록하는 직접 API 통신기반 인증이 약간 우수하다는 것을 알 수 있다. 이는 보안 게이트웨이 기반 인증이 공개키 인증서 도용에 따른 사기 피해를 방지하기 위해서 PKI 기반 인증과 더불어 블록체인 인증 서비스를 사용하기 때문에 초기 공개키 인증서 등록에 소요되는 시간이 더 길게 나왔음을 알 수 있다.

Table 1. Registration Time of Public Certificate(second)

Auth. Count	Security Gateway	Direct API Telecommunication	Security Gateway − Direct API Telecommunication
100	2.8418	2.826	0.0158
200	5.6858	5.652	0.0338
300	8.5298	8.48	0.0498
400	11.3736	11.306	0.0676
500	14.2176	14.134	0.0836

보안 게이트웨이 모델과 직접 API통신 모델의 비교우위를 계층퍼지적분을 사용하여 평가하였다. 평가 대상이 다수 항목으로 구성되어 있고 각 항목의 중요 정도에 차이가 존재할 때 이들 항목 대한 평가를 통합하는데 계층퍼지적분이 사용된다[17,18]. OSI 보안 아키텍처에서 정의하고 있는 보안요구, 보안위협, 보안기능, 보안 기술을 평가항목으로 구성하여 게이트웨이 모델과 직접 API 통신 모델의 비교우위를 평가하였다. 계층 퍼지적분의 적

용을 위해서 공개인증서의 보안 요구 항목으로 무결성과 가용성으로 세분화하였고 보안 위험은 위조, 불법수정,방해로 세분화해서 검증 평가하였다. 보안 기능은 무결성 검사, 송신자 확인, 부인봉쇄로 세분화하였고 보안기술은 공증, 디지털 서명으로 구분하여 평가하였다. 계층퍼지 적분평가 알고리즘은 평가항목의 계층를 통해서 평가치를 구하고 각 계층을 종합해서 퍼지측도를 산출한다. 까모또의 퍼지측도는 통합평가에서 평가항목이 기여하는 정도를 나타내는 주관적 측도로 모호함에 대처해서 대상을 평가할 때 사용되는 분석 방법이다. 먼저 자료분석을 통한 평가항목의 중요도(μ)와 평가항목간의 상호작용계수(λ)를 구하고 이를 이용하여 퍼지측도(g(·))를 산출하고 항목별 평가치 h(·)를 구한다. 마지막으로 평가항목별 평가치 h(·)와 g(·)를 사용하여 단순가중법에 의해 종합평가를 수행한다. 퍼지측도(g(•))의 평가 결과는 Table 2와 같고 공개키 인증서 서비스 평가항목에 대한 전문가 집단이 평가한 중요도의 부분집합을 13개의 부분집합으로 구성하고 평균에 의한 측도값 g(·)를 산출하였다.

Table 2. Measure Value of Fuzzy integral

Number of Subset	Item Number	g(·)
1	1 2 3 4 5 6 7 8 9 10	0.0625
2	1 2 3 4 5 6 7 8	0.0599
3	1 2 3 4 5 9 10	0.0585
4	3 4 5 6 7 8 9 10	0.0635
5	1 2 3 4 5	0.0519
6	1 2 6 7 8	0.0665
7	1 2 9 10	0.0574
8	3 4 5 6 7 8	0.0604
9	3 4 5 9 10	0.0585
10	1 2	0.0583
11	3 4 5	0.047
12	6 7 8	0.0712
13	9 10	0.0703

Table 3. Evaluation Value of of Fuzzy integral

Number of Subset	Item Number	g(·)	
		Security Gateway Model	Direct API Telecommunication
1	1 2 3 4 5 6 7 8 9 10	0.063	0.063
2	1 2 3 4 5 6 7 8	0.062	0.062
3	1 2 3 4 5 9 10	0.060	0.061
4	3 4 5 6 7 8 9 10	0.063	0.063
5	1 2 3 4 5	0.059	0.059
6	1 2 6 7 8	0.065	0.065
7	1 2 9 10	0.063	0.063
8	3 4 5 6 7 8	0.0623	0.0622
9	3 4 5 9 10	0.0601	0.0603
10	1 2	0.0615	0.0612
11	3 4 5	0.0565	0.0565
12	6 7 8	0.0669	0.0668
13	9 10	0.0637	0.064

구현 항목에 대한 전문가 집단이 평가한 평가치를 입력치로 하여 평균에 의한 부분집합의 평가치 h(·)를 Table 3과 같이 구하였다.

구현 항목에 의한 인증 모델의 평가항목별 부분집합의 평점을 비교하면 보안 게이트웨이 인증모델과 직접 API 통신기반 인증 모델이 거의 유사함을 알 수 있다. 제안하는 보안게이트웨이의 인증 모델은 무결성과 공증 영역그리고 보안기술 영역에서 약간 우세하게 평가되고 있음을 확인할 수 있다. 이는 무결성 영역과 공증 부문에 상대적으로 높은 비중을 두어 평가하였기 때문에 보안 게이트웨이 인증모델에 대한 공증 영역의 평가치가 더 높게 나온 것으로 추정된다. 퍼지 평가치 h(·)와 퍼지 측도치 g(·)를 이용한 퍼지적분 종합 평가 알고리즘의 결과는 Table 4와 같다.

Table 4. Result of Fuzzy integral

Number of Subset	Measure Value g(·)	Direct API Telecommunication h(·)	Security Gateway Model h(·)	Direct API Telecommunication Model Total Evaluation Value	Security Gateway Model Total Evaluation Value
1	0.0625	0.063	0.063	0.0668	0.0669
2	0.0599	0.062	0.062		
3	0.0585	0.061	0.060		
4	0.0635	0.063	0.063		
5	0.0519	0.059	0.059		
6	0.0665	0.065	0.065		
7	0.0574	0.063	0.063		
8	0.0604	0.0622	0.0623		
9	0.0585	0.0603	0.0601		
10	0.0583	0.0612	0.0615		
11	0.047	0.0565	0.0565		
12	0.0712	0.0668	0.0669		
13	0.0703	0.064	0.0637		

직접 API 통신기반 인증 모델과 보안 게이트웨이 기반 인증모델에 대한 평가치 h와 퍼지척도 g의 평가치가 거의 차이가 나지 않음을 확인할 수 있다. 하지만 보안 게이트웨이 기반 인증모델은 공개키 인증서의 무결성과

공증에 있어서 좀 더 우월하므로 공개키 인증서의 보안성을 요구하는 전자상거래 업체의 메시지 보안 시스템으로 적합하다.

5. 결론

최근 국가기관이 공인하는 공인인증서와 공인인증기관이 폐지되고 인터넷 기업이 인증기관으로서 발행하는 공동인증서를 허용하였다. 실체가 드러나지 않는 사이버 공간의 인증기관이 인증서를 발급하고 이로 인한 신분도용을 통한 사기 피해의 확대로 전자상거래의 활성화와 기업의 글로벌화를 저해하게 된다. 본인인증과 부인방지 기능을 제공하는 탁월한 기술인 PKI 기술에 다양한 인증기술이 결합되어 안전하고 편리한 인증서비스가 요구된다. Gateway를 사용하는 보안 서비스는 클라이언트가 특정 API를 개별적으로 호출할 필요없이 게이트웨이에서 통합한 API의 단일 호출에 의해서 특정 서비스를 이용할 수 있게 한다. 클라이언트와 애플리케이션 간의 호출 횟수가 줄어들고 클라이언트 코드가 단순화되는 이점이 있다. 본 논문에서는 블록체인에 PKI를 결합한 보안 게이트웨이에서 사용할 수 있는 인증 모델을 제안하고 이의 실용성 평가를 위해서 인간의 주관성을 배제하는 평가방법인 수게노의 계층퍼지적분을 이용한 인증 모델의 보안성을 평가했다. 실용성 평가 및 검증을 위한 실험결과는 직접 API 통신기반 인증 모델과 보안 게이트웨이 기반 인증 모델에 대한 평가치 h(•)와 퍼지측도 g(•)의 평가치가 거의 차이가 나지 않음을 확인할 수 있다. 하지만 보안 게이트웨이 기반 인증모델은 공개키 인증서의 무결성과 공증에 있어서 좀 더 우월하므로 공개키 인증서의 보안성을 요구하는 전자상거래 업체의 메시지 보안 시스템으로 적합하다. 또한 보안 게이트웨이 기반 인증모델은 PKI 인증 모델과 더불어 블록체인 인증을 결합해서 인증 서비스를 제공하기 때문에 공개키 인증서 도용에 따른 사기 피해와 신분 도용을 방지하고 기존 인증서의 관리 비용의 절감을 통한 온라인 비즈니스 활성화와 인터넷 기업의 글로벌화에 기여한다.

REFERENCES

[1] E.S.Jeong.(2014). A Design of the Encrypted File System with PKI Authentication : User Authentication using PKI. *Soongsil University*, Master's Thesis.

[2] Liu Y, Tome W, Zhang L, Choffnes D, Levin D, Maggs B, Mislove A, Schulman A & Wilson C. (2015). An end-to-end measurement of certificate revocation in the web's PKI. I*n Proceedings of the 2015 internet measurement conference. ACM*, 183-196.

[3] J. Clark & P.C. Van Oorschot. (2013). SoK: SSL and HTTPS: revisiting past challenges and evaluating certificate trust model enhancements. In Proc. IEEE Symposium on Security and Privacy 2013, Berkeley, CA, USA, May 19-22, pp.511-525. IEEE Computer Society.

[4] J. A. Berkowsky & T. Hayajneh.(2017). Security issues with certificate authorities. *Proc. IEEE 8th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON).* 449-455.

[5] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, & C. Adams. (2013). X.509 Internet public key infrastructure online certificate status protocol—OCSP, RFC 6960. 1-41. https://www.hjp.at/(en,st_b)/doc/rfc/rfc6960.html

[6] S.C. Park.(2017). A Comparative Analysis of PKI Authentication and FIDO Authentication. *Journal of the Korea Institute of Information and Communication Engineering*. 21(7), 1411-1419.

[7] C. J. Chae, H. J. Cho & H.M. Jung. (2018). Authentication Method using Multiple Biometric Information in FIDO Environment. *Journal of Digital Convergence*, 16(1), 159-164. DOI : 10.14400/JDC.2018.16.1.159

[8] A. Balalaie, A. Heydarnoori & P. Jamshidi. (2016). Microservices architecture enables devops: Migration to a cloud-native architecture. *IEEE Software,* 33(3), 42-52.

[9] S.H. Lee.(2007). Implementation of Call Service Application Modeling and Performance Measurement in Open API based Gateway System. KWANGWOON UNIVERSITY. Master's Thesis. http://www.riss.kr/link?id=T11101637.

[10] J. W. Lee & H. S. Seo (2021). A Study on the API Gateway for human resources management modules extensions in ERP. *Journal of the Korea society of computer and information*, 26(2), 79-88. DOI : 10.9708/JKSCI.2021.26.02.079

[11] Y. M. Park, Y. I. Choi, B. S. Lee.(2004). Technology Trend on Open API for Converged Telecommunication Services. *Electronics and Telecommunications Trends*, 19(6), 105-117. DOI:10.22648/ETRI.2004.J.190611

[12] R. Xu, W. Jin & D. Kim. (2019). Microservice security agent based on API gateway in edge computing. *Sensors,* 19(22), 4905.

[13] D. Macrinici, C. Cartofeanu & S. Gao. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and*

Informatics, 35(8), 2337-2354.

[14] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and communication networks*, 9(18), 5943-5964.

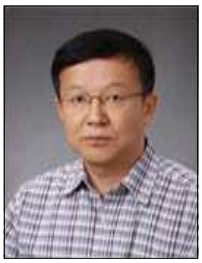
[15] M. Risius & K. Spohrer. (2017). A blockchain research framework, *Business & Information Systems Engineering*. 59(6). 385-409.

[16] C. Ebert, P. Louridas, T. M. Fernández-Caramés & P. Fraga-Lamas. (2020). Blockchain Technologies in Practice. *IEEE Software*, 37(4), 17-25.

[17] S. T. Lee. (1994). *A Study on the Development of Hierarchical Fuzzy Evaluation Algorithm and Its Application.* Korea Maritime & Ocean University. Master's Thesis.

[18] S. J. Shin & I.K. Park.(2000). A New Approach to the Verification of a Message Protocol : Fuzzy Integral. *Journal of Korea Information Processing Society.* 7(6), pp. 1903-1910.
DOI:10.3745/KIPSTE.2000.7.6.1903.

김 영 수(Young-Soo Kim) [정회원]



· 2003년 8월 : 국민대학교 정보관리학과 (시스템공학박사)
· 2020년 9월 ~ 현재 : 한세대학교 IT융합전자공학과 교수
· 관심분야 : 인공지능,스마트시티,공간정보
· E-Mail : experkim@gmail.com

문 형 진(Hyung-Jin Mun) [정회원]

· 2008년 2월 : 충북대학교 전자계산학과(이학박사)
· 2017년 3월 ~ 현재 : 성결대학교 정보통신공학과 조교수
· 관심분야 : 정보보안, 네트워크 보안, 빅데이터분석
· E-Mail : jinmun@gmail.com