Journal of Digital Convergence
Vol. 18. No. 11, pp. 227-232, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.11.227

블록체인과 Rotten Tomato 방식을 활용한 이메일 집단 인증 API 설계

김세민[1], 홍성혁[2*]
[1]전주교육대학교 컴퓨터교육과 외래교수, [2]백석대학교 정보통신학부 부교수

Design of E-Mail Group Authentication API using Blockchain and Rotten Tomato Method

Semin Kim[1], Sunghyuk Hong[2*]
[1]Adjuct Professor, Department of Computer Education, Jeonju National University of Education
[2]Associate Professor, Department of Information and Communication Engineering, Baekseok University

요 약 이메일을 사용하는데 있어서 가장 큰 애로사항으로 확인되지 않은 발신자를 걸러내기 힘들다는 것이다. 이에 본 연구에서는 최근 인증 수단으로 많이 활용되고 있는 블록체인 기술을 활용하여 이메일 집단 인증 API를 설계하였다. 제안한 모델로는 관계 연관성 네트워크를 통하여 노드-노드 가중치 지수를 구하였고, 이메일 신뢰도 모형을 설계한 후 Rotten Tomato 방식의 신뢰도 계산 모델을 구하였다. 이를 바탕으로 시스템 구조를 설계하고, 체인 코드 메소드를 정의한 후 API를 개발하였다. 본 연구를 통하여 이메일 사용자 인증 뿐만 아니라 인증이 필요한 다양한 분야에서 활용할 것으로 기대할 수 있으며, 향후 많은 수의 사용자를 대상으로 API를 사용하게 하여 집단 인증의 관계성을 증명할 수 있을 것으로 기대된다.

주제어 : 블록체인, 이메일 사용자 인증, 집단 인증, API, 로튼 토마토 방식

Abstract The one of the biggest challenges in using e-mail is that it is difficult to filter out unconfirmed senders. Therefore, in this study, an email group authentication API was designed using blockchain technology, which has been widely used as an authentication method. As the proposed model, the node-node weighting index was obtained through the relationship association network, and after designing the email reliability model, the reliability calculation model of the Rotten Tomato method was obtained. Based on this, the system structure was designed, chain code methods were defined, and API was developed. Through this study, it is expected that it will be used in various fields requiring authentication as well as email user authentication, and it is expected that the relationship of group authentication can be proved by allowing a large number of users to use the API in the future.

Key Words : Blockchain, E-Mail User Authentication, Group Authentication, API, Rotten Tomato Method. etc.

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (No. 2020R1F1A1048684).
*Corresponding Author : Sunghyuk Hong(shong@bu.ac.kr)
Received July 23, 2020 Revised August 3, 2020
Accepted November 20, 2020 Published November 28, 2020

1. 서론

최근 블록체인 기술이 발전함에 따라 여러 분야에서 블록체인을 적용하여 인증 기술을 발전시키는 사례가 많아지고 있다. 블록체인은 정보를 교환하는 모든 구성원이 인증된 제3자의 개입 없이, 공동으로 데이터를 보관하는 분산장부에 저장하고 기록하는 기술이다. 블록체인 기술을 활용하면 메시지의 전달과정과 데이터 발생에 따른 조작이 불가능 하므로 관련 상품에 대한 신뢰도를 높일 수 있으므로 인증 수단에 활용하기 적절하다[1-4].

이메일을 활용하면서 많은 사람들이 경험하는 문제는 수많은 스팸메일들을 마주한다는 것이다. 현재 시점에서 신뢰유무를 확실하게 구분할 수 있는 수단이 없으므로 신뢰할 수 있는 사람인지를 사용자가 직접 확인해야 하는 불편함이 있다.

이에 본 연구에서는 블록체인을 활용하여 신뢰할 수 있는 이메일을 검증하기 위한 시스템을 제안하였다. 이를 위하여 미국 할리우드 영화 평가 시스템인 로튼 토마토(Rotten Tomato) 영화 평가 시스템을 참고하였고, 사용자 중심의 집단 인증 네트워크로 인증한 내역과 확률을 기반으로 신뢰도를 체크할 수 있게 하였다. 해당 사용자와 이메일을 주고 받은 사람은 사용자와 친밀도가 높을 가능성이 있으므로 이를 집단 인증 네트워크로 구성하여 인증을 하면 의료 방역 분야에서 중요하게 여기는 집단 면역의 개념과 비슷한 집단 인증의 개념을 구현할 수 있을 것으로 연구목표를 설정하였다.

2. 관련 연구

2.1 이메일 사용자 인증

이메일의 주요 용도로는 인터넷을 통하여 메시지와 파일을 전달하거나 가입자를 대상으로 사용자 인증을 하는 수단으로 사용되고 있다[5]. 그러나 이메일을 통한 악의적인 의도로 인하여 사용자들이 피해를 당하는 경우가 많다[6]. 따라서 이를 방지하기 위하여 이메일 사용자 인증 방법 등이 연구되어 있다[7, 8]..

많은 사용자들은 이메일을 한 가지만 사용하는 것이 아니기 때문에 특정 플랫폼이나 브라우저에 제한을 두지 않는 Open API가 유용하다. 효율적인 사용자 인증을 위하여 상호 인증을 바탕으로 메시지의 기밀성과 안정성을 높이고 집단 인증 체제를 구축하는 것이 중요할 것이다.

2.2 블록체인 기술

블록체인은 비트코인 기반 기술로 사용되는 디지털 분산 원장이며, 이전 블록의 해시 값을 통하여 체인형태로 연결된다. 구성원들 간에 거래가 이루어질 때마다 해당 거래 정보에 대한 블록을 생성하여 모든 구성원들에게 브로드 캐스팅한다. 전송된 블록은 작업증명(PoW, Proof of Work) 단계를 통하여 유효성을 검증받고, 기존의 블록체인에 연결되어 공유된다[9-10] 또한 비트코인이 채택한 퍼블릭 블록체인 기술은 불특정 다수가 리소스 소모, 느린 처리 속도와 거래자의 익명성 등의 단점을 가지고 있기에 폐쇄적으로 네트워크를 운영하는 프라이빗 블록체인이 대안이 되고 있다[11-13].

2.3 관계 연관성 네트워크

관계 연관성 네트워크는 각종 SNS 매체들이 메시지를 전파하고 이식하는 구조를 설명하는 이론이다. 메시지를 네트워크에 전파하고 이식하려면 네트워크의 구조와 역학에 대한 이해가 필요하다. 매스미디어 네트워크는 Fig. 1과 같이 메시지를 보내는 노드에 대하여 나머지 노드들은 수신만 하고 있는 단방향 네트워크 형식이다. 이메일을 받은 메일함에서 열어서 메시지마다 각 편지함으로 이동시키거나 스팸 처리하는 절차를 통하여 개인적으로 분류하는 상황과 동일하다. 그러나 이러한 방식에서는 이메일에 대한 인증은 개인에 국한한다. 또한 시간이 지나도 관계 연관성이 강한 송신자와 약한 송신자의 메시지를 지속적으로 구분 없이 수신할 가능성이 높다[14, 15].

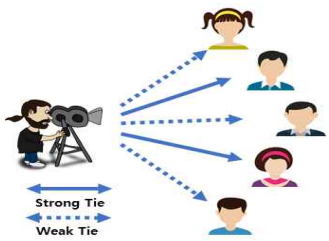

Fig. 1. Mass media network

이에 반하여 오가닉 미디어 네트워크는 Fig. 2와 같이 노드들이 자신과 군집계수가 높고 연관성 있는 노드끼리 무리를 지어 형성하여 있고, 약한 군집계수와 연관성을 통하여 다른 무리들이 서로 연결되어 있는 구조이다. 이러한 네트워크 구조의 특성 때문에 단순히 불특정 다수에 대한 공격으로는 전체 네트워크 구조에 전파하거나 이식을 시키기 어렵다[16].

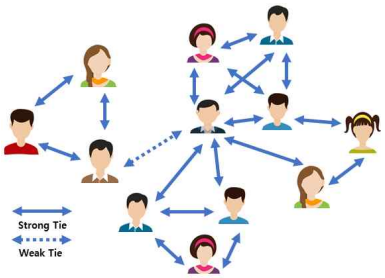

Fig. 2. Organic media network

본 연구에서 추구하고자 하는 집단 인증을 위해서는 전체 네트워크 안에서 각 노드들 간의 관계 연관성의 구조를 파악하여야 한다. 집단 인증을 위해서는 각 노드들을 연결하여줄 경로(path)가 존재하고, 임의의 노드끼리 연결할 때 얼마만큼의 경로의 길이가 필요한가를 파악하여야 한다. 예를 들어 페이스북(Facebook)에서는 평균 4.7의 경로를 가지고 노드와 노드의 연결을 파악하였다는 것을 Fig. 3을 통하여 알 수 있다.

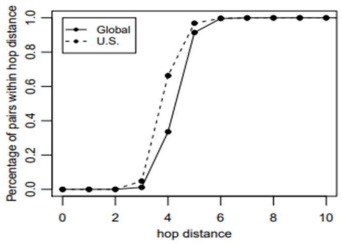

Fig. 3. Path's length of Facebook

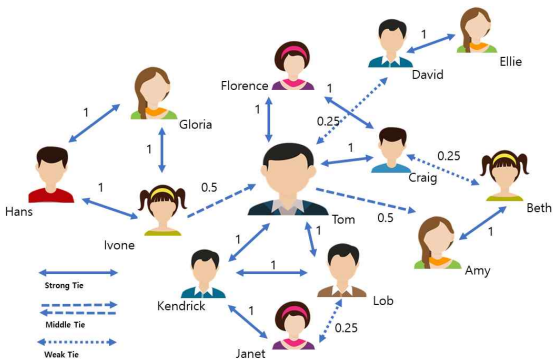

Fig. 4. Releative Model

3. 시스템 설계

3.1 관계연관성 모형 설계

이메일 계정의 신뢰도를 측정하기 위하여 본 절에서는 관계연관성 모형을 설계하였다. Fig. 4에서는 양쪽 사용자 모두 신뢰의 표시인 Fresh Tomato를 주고 받은 관계는 Strong Tie를 나타내는 양쪽 화살촉 실선화살표로 표현하고 1이라는 가중치를 부여하였고, 한 쪽의 사용자만 Fresh Tomato를 주고 다른 상대편 사용자는 그렇지 않은 경우는 Middle Tie를 나타내는 굵은 점선 화살표로 표현하고 0.5의 가중치를 부여하였으며, Fresh Tomato를 받은 사용자를 향하여 화살촉이 표시된다. 서로 Fresh Tomato를 주고 받지 못한 경우에는 Weak Tie를 의미하는 양쪽 점선 화살표로 표현하고 0.25의 가중치를 부여하였다. Fig. 4의 Tom과 Lob은 서로 Fresh Tomato를 주고 받았으므로 가중치가 1이 되었고, Tom과 David는 서로 Rotten Tomato를 주고 받았으므로 가중치가 0.25가 되었으며, Tom은 Amy에게 Fresh Tomato를 주었으나 Amy는 그렇지 않았으므로 0.5의 가중치가 주어진다. Table 1에서는 Fig. 4를 참고하여 일부 노드의 가중치를 구하였다. 관계노드마다 가중치의 평균을 구하였으며 Tom-Amy-Beth의 관계는 0.75, Tom-Craig-Beth의 관계는 0.625이므로 종합적인 Me와 Beth의 관계에서의 신뢰도 평균은 0.688이다. 관계의 평균은 0에서 1사이의 값으로 나타낼 수 있다.

Table 1. Node to Node Weight Index

Start User	1st	1st's Value	2nd	2nd's Value	Total
Tom	Amy	0.5	Beth	1	0.75
Tom	Craig	1	Beth	0.25	0.625
Beth's Avg.					0.688
Tom	Lob	1			1
Tom	Kendrick	1	Lob	1	1
Lob's Avg.					1
Tom	Kendrick	1	Janet	1	1
Tom	Lob	1	Janet	0.25	0.625
Tom	Kendrick 1	Lob	1	Janet 1	1
Tom	Lob 1	Kendrick	1	Janet 0.25	0.75
Janet's Avg.					0.844

3.2 이메일 신뢰도 모형 설계

본 절에서는 Fig. 4와 Table 1에서 나타낸 관계성 모형을 기반으로 Fig. 5와 같이 이메일 신뢰도 모형을 설계하였다. Hans의 친구 6명 중 5명에게 Fresh Tomato를 받았다. 따라서 Hans는 Tom을 87.5%의 확률로 신뢰할 수 있으며,Hans의 친구인 Ivone는 한스와 서로 Fresh Tomato 관계이다. 따라서 Ivone는 Tom을 87.5%의 확률로 신뢰할 수 있다. Hans의 친구인 Beth는 그의 친구

Amy, Kendrick도 Tom에게 Fresh Tomato를 주었다. 따라서 Tom을 100%의 확률로 신뢰할 수 있으며, Beth의 친구인 Amy는 Beth와 Kendrick을 통하여 Tom을 100%의 확률로 신뢰할 수 있다. 단 Tom이 Kendrick에게 Rotten Tomato를 준 것은 Amy와 Beth의 신뢰도에 영향을 미치지 않는다. 따라서 Kendrick의 친구인 Janet도 Tom을 100%의 확률로 신뢰할 수 있다. Tom은 Florence에게 Fresh Tomato를 주었으나 Rotten Tomato를 돌려받았다. 따라서 Florence의 친구인 Lob은 Tom을 신뢰할 수 없다(0%). 이와 같은 패턴이 계속하여 반복하면 사용자는 처음 여러 회 정도만 신뢰도 체크를 하면서 Fig. 4의 관계연관성 모델의 범위가 확장되어 집단인증 네트워크를 형성으로 이어질 수 있다.

그러나 Tom은 Fig. 4에서 나타난 인간 관계와는 상관없이 어느 순간에 이메일은 Fig. 5처럼 주고 받을 수 있다. 따라서 Tom이 불시에 이메일을 받았을 때 Fig. 4와 Fig. 5에 나타난 결과를 평균으로 계산하여 신뢰도를 최종적으로 계산하면, Table 2와 같이 0에서 1사이의 숫자로 나타낼 수 있다. 본 연구에서 평균으로 계속 계산하는 이유는 최종 신뢰도 지수를 0에서 1까지의 범위로 나타내기 위함이다.

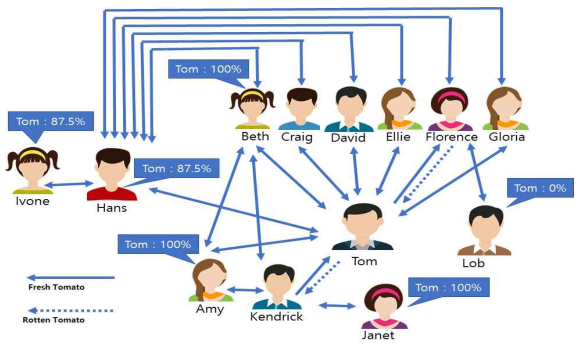

Fig. 5. Rotten Reliability Model for E-Mail Accout

Table 2. Reliability Result based on User

Name	Node-to-Node	Rotten Rate	Average Faith Rate
Amy	0.5	1.0	0.75
Beth	0.6875	1.0	0.84375
Craig	1.0	1.0	1.0
David	0.25	1.0	0.625
Ellie	0.625	1.0	0.8125
Florence	1.0	1.0	1.0
Gloria	0.79	1.0	0.895
Hans	0.79	0.875	0.8325
Ivone	0.5	0.875	0.6875
Janet	0.84375	1.0	0.921875
Kendrick	0.84375	1.0	0.921875
Lob	1.0	0.0	0.5

3.3 시스템 구조 설계

이메일을 선별할 수 있는 시스템을 구현하기 위하여 본 절에서는 시스템 구조를 설계하였다. Fig. 4와 Fig. 5에서 제안한 모델을 결합하여 로튼 토마토 이메일 API의 구조를 설계하였다. 로튼 토마토 이메일 API의 최초 받은 메일함(Gate INBOX)에서 처음 온 이메일이 수집된다. API에서 제공하는 셀렉트 메뉴에서는 Fresh Tomato와 Rotten Tomato 중 선별하여 해당 이메일 계정을 선택할 수 있다. Tomato의 등급에 따라 정크 메일을 선별한 AI에서는 통과된 메일 계정은 DB에 저장한 후 해당 메일 메시지는 사용자의 받은 편지함(User INBOX)에 저장하고, 그렇지 않은 메일 계정은 버리게 된다. Fig. 6의 E-Junk Jud. AI에 Rate Data들이 각 A, B, C의 User의 체인에 추가된다. 이메일 계정이 추천하는 메일은 DB에서 대조한 후 사용자의 받은 편지함에 저장될 수 있다. 본 연구에서 제안하는 시스템 구조도는 Fig. 6과 같다.

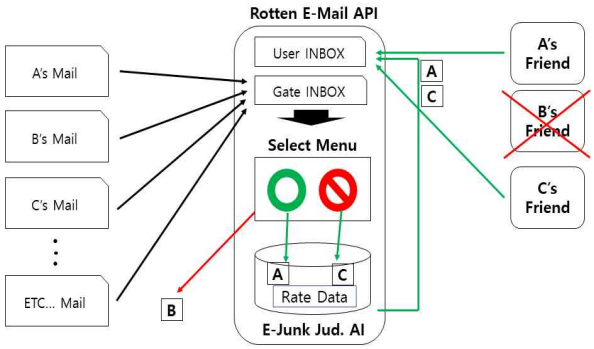

Fig. 6. System Architecture Model

Fig. 4~Fig 6에서 제안한 모델들과 시스템 구조가 사용자들끼리 집단 단위로 뭉칠수록 이메일 집단 인증 경우의 수가 많아지므로 더욱 정확도가 높아질 것이며 집단 인증 네트워크를 형성할 수 있다.

4. 시스템 구현

4.1 체인코드 메소드 정의

사용자가 이메일을 수신하였을 때 해당 이메일의 신뢰 여부를 선별할 수 있는 체인코드 메소드를 정의한 바는 Table 3과 같이 구성한다. 주요 체인코드 메소드는 시스템을 초기화 작업을 하기 위한 메소드로 init( )가 있고,

사용자가 선택한 이메일을 수집하고 신뢰 데이터를 기록하는 메소드로 collect()와 select( )가 있으며, 신뢰받은 이메일을 해당 사용자의 메일함(User INBOX)에 등록하고 집단 사용자에게 신뢰 내역을 기록하는 메소드로 newRegist( )가 있다. 아울러 showInfo( ) 메소드에서는 이메일 사용자가 해당 메일의 인증 정보를 조회할 수 있게 하였다.

Table 3. Definition of Chain Code Method

Method	Contents
init()	Method for system initialization
collect()	Among the emails that arrive, emails with no confidence level are separately sent to the select() method
select()	Method to record trust data and reliability by checking whether the mail received from collect() is fresh/rotten
newRegist()	Method that records authentication details to group users at the same time that trusted emails are registered in User Inbox in collectSelect() method.
showInfo()	Method for user to look up the authentication information of the mail

4.2 신뢰 데이터 기록 코드

아래의 의사코드는 새로운 메일이 도착하였을 때 신뢰도를 체크한 후 사용자의 User INBOX에 등록하거나 휴지통으로 보내는 코드를 나타낸 것이다.

```
select(){ string oldData[], newData[], temp[];
    char okData, noData;
    double faithRate, rottenMail, freshMail;

    if(noData == true){
        rottenMail ++;
        temp[] = newData[];
    } else {
        freshMail ++;
        oldData[] = oldData[] + newData[];
    }     faithRate = freshMail/(freshMail+rottenMail);
    newRegist(faithRate); }
```

4.3 Block 메시지 열람 결과

아래의 메시지는 Fig. 6에서 제시한 시스템의 흐름에 기반하고 Fig 5에서 제시한 신뢰도 체크 모델을 적용한 결과를 구현한 결과를 나타내기 위하여, 사용자의 User INBOX에서 열람할 수 있는 메시지의 형태이다.

```
{  "ChainID" : "1"
   "UserName" : "Alice"
   "Title" : "No Title"
   "Contents" : "Blah blah..."
   "UserSelect" : "Fresh"
   "RottenRate" : "X.X %"
   "NodeToNodeRate" : "X.X %"
   "AverageFaithRate" : "X.X %"
   "FreshCnt" : "X EA Vs."
   "RottenCnt" : "X EA"
   "FaithResult" : "Yes"
   "NodeValue" : "X.X" }
```

5. 결론 및 제언

최근 블록체인 기술 분야의 성장으로 인하여 다양한 분야에서 사용자 인증 부문에서 활용하고 있다. 본 연구는 신뢰할 수 있는 이메일인지의 여부를 집단 인증 개념을 도입하여 API를 설계하였다

본 연구에서 제안한 API를 개발하기 위하여 노드 간 가중치를 측정하는 모델을 구현하였다. 또한 미국 할리우드의 영화 평가 사이트인 Rotten Tomato에서 활용하는 모델을 활용하여 이메일 신뢰도 모형을 구현하였고, 이 모형들을 바탕으로 Rotten E-Mail API의 구조를 개발하고 체인코드 메소드를 정의하였다. 설계하였다. 기존의 모델에서는 네트워크 구성원이 극도로 많아졌을 때의 성능이 확실하게 입증된 바 없지만 본 연구에서 제안한 모델을 통하여 Fig. 3과 같이 SNS 경로 길이 모델과 같이 집단인증 네트워크의 가능성이 높다고 할 수 있다.

본 연구의 한계점으로는 API의 설계 단계이기 때문에 많은 수의 집단을 바탕으로 검증하지는 못하였다. 그러나 페이스북에서 조사한 관계연관성 모델의 데이터를 참고하였을 때 많은 수의 집단으로 검증하면 오히려 더 촘촘한 집단인증 네트워크가 될 것으로 기대할 수 있다. 또한 이메일 뿐만 아니라 이력확인이나 인증이 필요한 다양한 분야에서 활용할 수 있을 것이라고 기대할 수 있다.

향후 연구과제로는 많은 수의 사용자를 대상으로 이메일 집단 인증 API의 효과성을 최종 확인하고, 다양한 분야에서 본 연구에서 제안한 API 모델을 적용하는 것이다.

REFERENCES

[1] S. H. Hong. (2019). Research on a new approach to enhance IoT security using blockchain technology.

Journal of Digital Convergence, 17(12), 235-241.

[2] J. C. Park. (2017), "A Secure Single Sign-On Scheme across Multiple Allied Websites using Smartphones". *Journal of Security Engineering*, 14(3), 189-204. DOI: dx.doi.org/10.14257/jse.2017.06.01

[3] Y. Choi & H. Kwon. (2018), "A Study on Legal Issues between the Application of Blockchain Technology and Deletion and the Third Party Supply of Personal Information", *Journal of the Korea Institute of Information Security & Cryptology*, 28(6), 1607-1621. DOI: doi.org/10.13089/JKIISC.2018.28.6.1607

[4] S. J. Han, S. T. Kim and S. Y. Park. (2019), "A GDPR based Approach to Enhancing Blockchain Privacy", *The Journal of The Institute of Internet, Broadcasting and Communication*, 19(5), 33-38, DOI: doi.org/10.7236/JIIBC.2019.19.5.33

[5] M. S. Yim. (2013), Moral Disengagement in Information Security Context, *A Study of Antecedents and Outcomes*, 11(11), 1-13.

[6] Kitterman, S. (2017), "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208,

[7] D. H. Lim(2013), *A Study on International Standardization of Certified Email Address(#mail)*, Master's Thesis, Graduate School of Soongsil University, Seoul.

[8] H. B. Ahn and S. Y. Lee. (2016), The Study on Secure Mail Platform and Mutual Authentication Using Mail Proxy, *Journal of Digital Convergence*, 14(12), 201-208.

[9] Satoshi Nakamoto. (2009), *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin.org.

[10] S. Y. Son and Y. T. Shin. (2018), "A Study on the Agreement Algorithm for Securing IoT Data Integrity Using Blockchain," *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences*, 1136-1137.

[11] A. Dorri, S. S. Kanhere, and R. Jurdak. (2016), "Blockchain in Internet of Things: Challenges and Solutions," arXiv Preprint arXiv: 1608.05187,

[12] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram(2017), *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*, In IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing.

[13] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman. (2017), FairAccess: a New Blockchain-based Access Control Framework for the Internet of Things, *Security and Communication Networks*, 5943-5964.

[14] J. Y. Yoon. (2014), *Organic Media*, Pressbooks, Seoul, Korea.

[15] S. G. Noh. (2016), *Organic business : Network is eating the world*, Pressbooks, Seoul, Korea.

[16] Johan Ugander, Brian Karrer, Lars Backstrom & Cameron Marlow. (2011), *The Anatomy of the Facebook Social Graph*, arXiv Preprint arXiv.org:1111.4503.

김 세 민(Semin Kim) [정회원]

- 2018년 8월 : 한밭대학교 정보통신공학과(공학박사)
- 2008년 2월 ~ 현재 : 전주교육대학교 컴퓨터교육과 외래교수
- 관심분야 : 블록체인, 소프트웨어교육, 메이커 및 로봇활용교육
- E-Mail : imsil303@hotmail.co.kr

홍 성 혁(Sunghyuck Hong) [종신회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 블록체인, 사물인터넷 보안, 경량보안프로토콜
- E-Mail : shong@bu.ac.kr