하이브리드 블록체인을 이용한 데이터베이스 보안

배근우[1], 이근호[2*]
[1]백석대학교 정보통신학부 학생, [2*]백석대학교 정보통신학부 교수

Security of Database Based On Hybrid Blockchain

Keun-Woo Bae[1], Keun-Ho Lee[2*]
[1]Student, Dept. of ICT, BaekSeok University
[2*]Professor, Dept. of ICT, BaekSeok University

요 약 최근에 블록체인 기술에 대한 관심이 높아지고 있다. 본 연구에서는 하이브리드 블록체인을 이용하여 데이터를 안전하게 보관하는 솔루션을 제시하였다. 세계적으로 데이터를 이용한 산업이 점차 늘어나고 있으며 이를 대상으로 삼아 공격하는 일이 빈번히 발생하고 있다. 2017년도 OWASP는 웹 애플리케이션 보안 취약점 1위를 SQL 인젝션 공격으로 선정하였다. 그에 비해 데이터 산업에서 보안이 차지하고 있는 비중은 제일 적다. 데이터를 안전하게 보관하고 공격을 막기 위해 단순히 데이터베이스에 데이터를 저장하는 방식이 아닌 블록체인과 데이터베이스를 결합한 데이터 저장방식을 소개하였다.

주제어 : 블록체인, 데이터베이스, 하이브리드 블록체인, 웹 서버, 보안

Abstract Recently, interest in blockchain technology has increased. The data industry is increasingly growing around the world. In addition, databases which obtain important information such as personal data are targeted by hackers. Data exposed by attackers happen frequently. In 2017, OWASP announced SQL injection is a top 1 threat to web applications. However, the proportion of data security is the smallest in the data industry. To prevent data exposure, this paper proposes a method that can protect databases by using hybrid blockchain.

Key Words : Blockchain, Database, Hybrid Blockchain, Web Server, Security

1. 서론

4차 혁명이 진행되고 있는 2020년, 현재 가장 대두되고 있는 분야는 바로 데이터이다. 이러한 데이터 산업이 현재 국내/외로 점차 진화하고 있다. 한국 데이터 산업진흥원에 따르면, 2018년 국내 전체 데이터 산업 시장규모는 2017년도 기준 5.6% 성장한 약 15조 1500억원 이라고 발표하였다. 동시에 국내 데이터 산업 인력 또한 꾸준히 늘고 있다고 전하였다[1]. 하지만 동시에 OWASP (Open Web Application Security Project)는 2017년도 가장 위험한 웹 애플리케이션 보안 1위를 인젝션(Injection) 공격으로 뽑았다. 이러한 인젝션 공격은 개인정보의 노출과 정보 공개, 서비스 거부 결과를 불러올 수 있다[2]. 이는 데이터 산업이 긍정적인 방향으로 확장되고 있으나, 정작 데이터 보안은 그렇지 않다는 것을 방증해준다. 데이터 보안을 향상시키기 위하여 민감한 개인정보를 저장하고 관리하는 데이터베이스(Database)의 보안을 퍼블릭 블록체인(Public Blockchain)과 프라이

본 논문은 2020년 백석대학교 학술연구에 의하여 지원되었음
*교신저자 : 이근호(leekeunho1004@gmail.com)
접수일 2020년 1월 21일 수정일 2020년 2월 19일 심사완료일 2020년 2월 21일

빗 블록체인(Private Blockchain)을 혼합한 하이브리드 블록체인(Hybrid Blockchain)을 이용한 데이터베이스 보안솔루션을 제안하고자 한다.

2. 국내/외 데이터 산업 동향

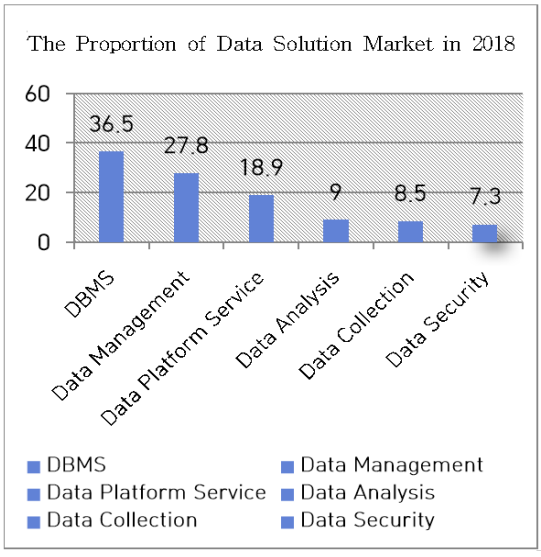
2.1 데이터 산업의 국내 동향

현재 국내 데이터 산업 시장 규모는 2010년도부터 2018년도까지 꾸준히 증가하고 있다. 아래의 Table 1은 데이터 산업 부문별 시장 규모를 나타내었다[1].

〈Table 1〉 The Amount of National Data Industry Market. (100 Million ₩)

	2016	2017	2018
Data Solution	15,720	16,457	17,561
Data Construction and Consulting	55,850	58,894	61,934
Data Services	65,977	68,179	72,050
Overall	137,547	143,530	151,545

데이터 보안 시장은 데이터 솔루션 시장에 속해 있는데, 약 총 1,281억 원의 시장 규모를 갖고 있다. 이는 솔루션 시장 중 가장 작은 규모의 크기이며 자세한 규모는 아래의 Figure 1과 같다.



[Fig. 1] The proportion of Data Solution Market in 2018

DBMS의 시장이 36.5%로 솔루션 시장 중 가장 시장 규모 비율이 높았으며, 데이터 보안 시장은 데이터 솔루션 시장에 속해 있는 제일 적은 수치인 7.3%를 차지하고 있다[1]. 이는 단편적으로나마 데이터 보안의 중요도를 나타낸다. 아래의 Table 2에서는 데이터 보안 시장규모를 라이선스, 개발, 유지보수로 나누었다.

〈Table 2〉 The Amount of National Security Data Industry Market. (100 Million ₩)

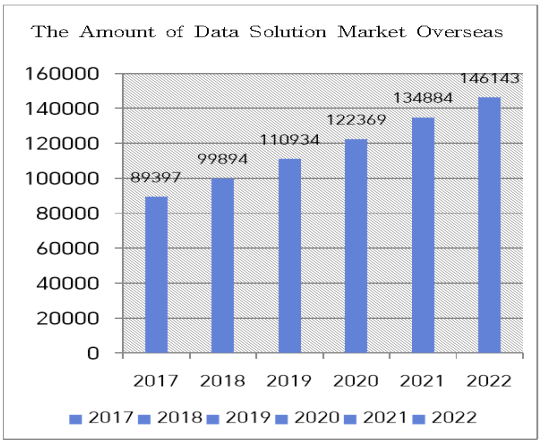
		2016	2017	2018
Data Security	License	-	789	831
	Development	-	133	128
	Maintenance	-	291	320

2018년 데이터 보안 영역 중 라이선스와 유지/보수 분야는 2017년보다 각각 6.3%, 10% 상승하였지만, 개발 부분에서는 오히려 3.7% 감소하였다. 2017 OWASP 1위가 SQL Injection으로 밝혀진 때, 보안 개발 분야의 비중이 감소하였다는 것은 데이터 보안에 대한 인식이 많지 않다는 것을 보여준다.

2.2 데이터 산업의 국외 동향

한국 데이터 산업 진흥원(Kdata)에 따르면, 2019년 해외 전체 솔루션 시장은 약 1,109억 달러의 규모를 갖고 있으며, 2017년부터 2022년까지의 연평균 성장률이 10.3%에 가까울 것이라고 하였다. 아래의 Figure 2와 같이 2022년에는 해외 데이터 솔루션 시장 규모가 약 1,461억 달러에 달할 것이라고 예상하였다[1].

이중 가장 큰 시장은 'Operational Databases' 시장으로 2018년 기준 약 400억 달러 이상의 시장규모를 갖고 있으며 두 번째로는 'Reporting and Analytics' 시장으로 200억 달러, 세 번째로는 'Analytic Data Platforms' 시장으로 150억 달러 내외로 평가되었다. 국내와 마찬가지로 DBMS, 데이터 분석과 데이터 분석 플랫폼 시장이 제일 큰 것으로 나타났다. 국내와 달리 해외 솔루션 시장 규모 조사에는 데이터 보안 분야가 포함되지 않았다.



[Fig. 2] The Amount of Data Solution Market Overseas

2.3 데이터 산업 동향 결론

국내/외 데이터 산업은 전체적으로 상승세를 보여주었다. DBMS, 데이터 분석 및 플랫폼 시장이 대부분을 차지하고 있었지만, 데이터 보안 분야는 다른 분야에 비해 시장 규모가 가장 적었다. 데이터 분석 및 플랫폼 시장도 중요하지만, 사용자의 데이터 정보 보안을 신경 쓰지 않는다면 데이터 노출, 유출 또는 손실이 일어났을 경우, 사용자들의 신뢰 및 피해에 대한 막대한 손실을 막을 수 없을 것이다.

3. 2017년도 OWASP - Injection

3.1 SQL 인젝션(Injection) 공격

2017년도 OWASP(Open Web Application Security Project) Top 10의 순위를 살펴보면, 인젝션(Injection) 공격이 1위를 차지하고 있다. 인젝션 공격은 공격자가 보안상의 취약점을 이용하여 비정상적인 SQL 문을 삽입하여 데이터베이스가 비정상적으로 동작하게 하는 공격 기법을 말한다. 이 공격은 데이터 유출, 파괴 등을 초래할 수 있으며, 권한이 없는 사용자에게 정보가 노출될 수 있다. 최악의 경우, 인젝션 공격으로 호스트 권한을 공격자에게 빼앗길 수 있다. 이를 해결하기 위해서는 명령어와 쿼리를 구분, 분리해야 한다[2]. 또한, SQL 인젝션(Injection) 공격을 탐지하는 방법 중 동적 분석 방법, 정적 분석 방법 등이 있지만 각 방법들의 단점이 명확히 존재하기에 모든 공격을 방어하기 위한 하나의 공격 탐지 방법을 하나만 고르기가 어렵다[3]. 하지만 아래에 제안하는 하이브리드 블록체인을 이용한 데이터베이스 보안 기법은 새로운 공격 방어 방법을 제시해 줄 것이다.

3.2 SQL Injection 인증 우회

SQL Injection 실습을 위해 JAVA로 작성한 간단한 로그인 소스 코드 구문은 아래와 같다.

```
String query = "SELECT * FROM members
WHERE username= '" + userId+ "'
AND password = '" + password + "'";
```

Souce Code 1. Login [4]

JAVA로 짜여진 위의 Source Code 1을 살펴보면 userId를 넣는 부분과 password를 넣는 부분이 있다. 이중 userId에 admin을 입력하고, password에 ' or 1=1 같은 무조건 참으로 반환이 되는 구문을 넣는다면, password 부분이 무조건 참으로 인식되어 admin 아이디로 로그인에 성공하게 된다[3,5,6]. 이뿐만 아니라 password를 넣는 구문에 ' or 1=1 # 혹은 ' or 1=1 -- 와 같은 주석을 넣어주어 패스워드의 입력 없이 로그인 절차를 생략할 수 있다[3,5,7].

3.3 시큐어 코딩(Secure Coding)

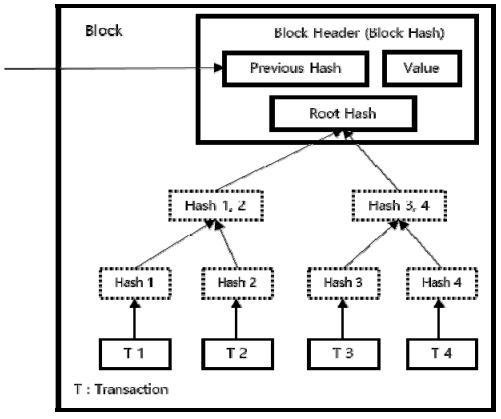
간단한 SQL 인젝션 실습을 위에서 진행하였다. SQL 인젝션을 막기 위한 방법 중 하나는 바로 시큐어 코딩이다. 이는 취약점을 막는 가장 근본적인 방법으로, 서비스 개발을 완료하기 전 취약점을 제거하는 편이 완료 후 취약점을 찾고 보안 약점을 제거하는 것보다 더욱 효과적이다[8]. 국내에서는 행정자치부에서 개발에 필요한 시큐어 코딩 가이드를 배포하고 있다[4,9]. 한국인터넷 진흥원에서는 시큐어 코딩을 위한 웹 서버 구축 보안 점검 안내서 등 기술문서를 배포하고 있다[6].

4. 블록체인

4.1 블록체인(Blockchain)

처음의 블록체인(Blockchain)의 개념은 사토시 나카모토 라는 인물에 의해 제안되었다. 사카시 나카모토는 탈 중앙관리를 지향한 비트코인 기술을 제안하였는데, 이는 기본적으로 블록체인이라는 기술을 바탕으로 소개하

였다. 기본적으로 블록체인이란 데이터를 다수의 블록(Block)에 저장하고 저장한 블록들을 서로 연결(Chaining)하는 것을 말한다. 블록들은 복호화가 불가능한 해쉬함수로 암호화가 되며, 고정된 길이의 해쉬값을 갖는다. 하나의 블록은 이전 블록의 해쉬값과 루트 해쉬값을 갖고 있는데, 루트 해쉬는 1:1 대응으로 각 블록이 생성한 해쉬값을 가지고 생성이 된다. 즉, 루트 해쉬값을 다른 블록과 비교하여 값이 다를 경우, 데이터가 변조되었다는 것을 쉽게 알 수 있다[10]. 블록체인의 구조는 아래 Figure 3과 같다[11].



[Fig. 3] Blockchain Structure

이처럼 단순히 해쉬값을 비교하는 것으로 어떠한 블록의 데이터가 위조 및 변조되었는지 확인할 수 있다. 또한, 해쉬를 복호화하는 것은 불가능하고, 더욱이 블록체인 기술상 하나의 블록을 바꾸기 위해서는 그 뒤에 붙어 있는 블록의 데이터까지 바꿔야 하므로 블록 안에 있는 데이터를 변조하는 것은 불가능하다고 볼 수 있다[11]. 이러한 블록체인의 특성은 데이터의 무결성을 보장해준다[12,13].

4.2 퍼블릭 블록체인(Public Blockchain)

퍼블릭 블록체인(Public Blockchain)은 누구든지 쉽게 참여할 수 있는 개방형 블록체인 네트워크로, 조직이나 기관의 승인 없이 누구든지 컴퓨터, 노트북, 스마트폰 등의 IT 기기를 이용하여 블록체인 네트워크에 참여할 수 있다. 하지만, 퍼블릭 블록체인의 경우, 블록들의 프라이버시가 완벽하게 보호되지 않기 때문에 제3자 가 노드(node)의 정보를 알 수 있다는 단점이 존재한다[14].

대표적인 연구로는 이더리움(Ethereum)이 있고, 스마트 컨트랙트(Smart Contract)의 개념이 최초로 탑재되었다[10,15].

4.3 프라이빗 블록체인(Private Blockchain)

프라이빗 블록체인(Private Blockchain)은 퍼블릭 블록체인(Public Blockchain)과 다르게 폐쇄적이며 기업이나 조직에 의해 허가된 유저들만 참여할 수 있다. 허가받지 못한 참여자 혹은 기업은 블록체인 네트워크에 참가할 수 없으며 따로 참여를 위한 암호화폐를 발행하지 않아도 된다는 점이 퍼블릭 블록체인과 다르다. 그러나, 퍼블릭 블록체인과 다르게 프라이빗 블록체인은 참가 권한을 허가해 주는 조직이 필요하여 참여를 허락해 주는 조직이 블록체인을 관리한다는 단점이 있다[14,16]. 이는 사토시 나카모토가 의도한 탈중앙화를 위한 블록체인 기술에 반(反)하게 되는 기법이다.

대표적인 연구로는 리눅스 파운데이션(Linux Foundation)이 주도한 연구로 하이퍼 레저 패브릭(Hyper Ledger Fabric)이 있으며 신원 관리, 개인정보 보호 및 기밀 유지 및 체인 코드 등의 네트워크 기능을 지원한다[10,15].

4.4 하이브리드 블록체인(Hybrid Blockchain)

하이브리드 블록체인(Hybrid Blockchain)은 퍼블릭 블록체인과 프라이빗 블록체인을 서로 연결한 혼합형 블록체인이다[17]. 즉, 프라이빗 블록체인의 기술은 노드들의 정보 노출을 막아주며 더 효율적인 블록체인의 사용을 도와주고, 퍼블릭 블록체인 기술이 주는 편리한 접근성을 결합시킨 것이다.

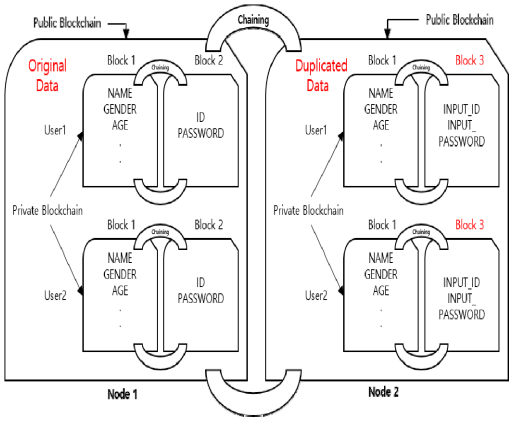
이를 사용한 대표적인 예제는, IoT(Internet of Things)에서, 가정에서 쓰이는 IoT는 프라이빗 블록체인으로 사용하고, 자동 결제 시스템을 위해 퍼블릭 블록체인에 연결하는 방식이 있다[17].

5. 제안 방법

하이브리드 블록체인(hybrid Blockchain)을 이용하여 데이터베이스(Database)를 만들어 사용자들의 정보들을 안전하게 저장하는 방법을 제안한다. 일반 데이터베이스를 이용한 웹 서비스 및 애플리케이션들은 사용자의 아이디와 비밀번호 데이터베이스의 정보와 비교해 로그인 등의 서비스를 제공한다. 이는 관리가 미숙한 혹은 관리자가 알아채기 어려운 취약점에 노출되어 있는 웹 서

비스의 경우 사용자들의 정보가 무방비하게 노출되어 있을 가능성이 크다. 하지만 블록체인을 이용하여 정보를 저장하게 된다면 직접적인 데이터베이스가 노출된다고 하더라도 복호화가 불가능한 해쉬(Hash)함수로 암호화가 되어 있기 때문에 전혀 피해가 없다.

이 하이브리드 블록체인을 이용한 데이터베이스의 저장 구조는 아래 Figure 4와 같다.

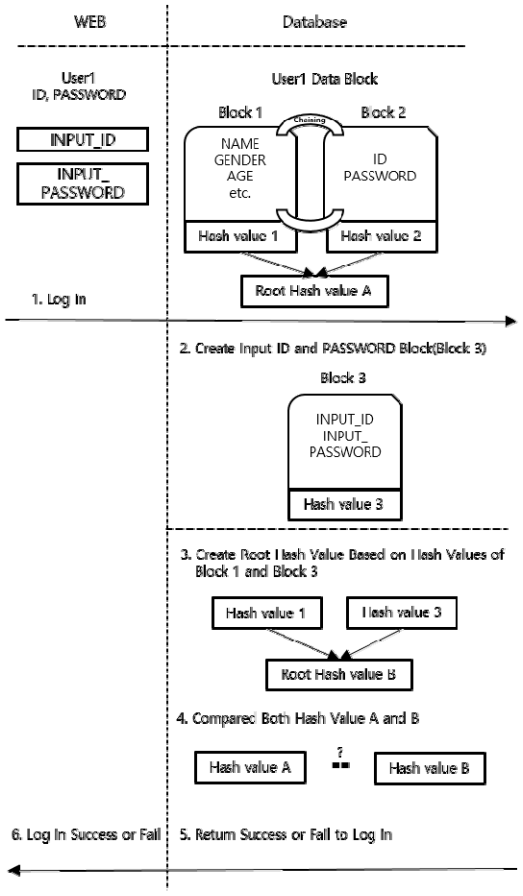


[Fig. 4] Database Structure Based On Hybrid Blockchain

Figure 4에서 Node 1과 2 안에는 사용자 1의 정보들은 블록1(Block 1)과 블록2(Block 2)에 나누어 저장된다. 블록 1에는 이름, 성별, 나이 등의 정보들이 저장되며 블록 2에는 사용자의 아이디 및 비밀번호가 저장된다. 사용자2의 데이터 또한 마찬가지이며, 블록 1과 블록2는 서로 연결(Chaining)되어 있다. 단, 사용자 1과 사용자 2의 블록은 서로 연결되어 있지 않다. 사용자의 정보를 저장하는 블록을 두 개로 나눈 이유는, 추후 웹에 로그인 시, 아이디와 비밀번호를 해쉬한 값을 가지고 비교하기 위함이다. 이를 위해 Node 2에는 Node 1과 같은 사용자의 정보를 바탕으로 한 복사된 블록 1을 갖고 있다. 여기에 웹 로그인 시 사용자가 입력한 아이디와 비밀번호 값을 Node 2 안의 블록 1에 연결하여 해쉬값을 만들고 Node 1 안에 있는 사용자 1의 블록 해쉬 값과 비교하여 로그인의 성공 여부를 따지는 것이다.

이러한 블록들은 프라이빗 블록체인으로 되어 있으며, 이 블록들을 다시 퍼블릭 블록체인으로 암호화하여 프라이빗 블록체인의 단점인 탈중앙화와 개인정보 노출을 을 막았다.

상세 로그인 절차는 아래의 Figure 5와 같다.



[Fig. 5] Web Login Process

Step 1. ID, PASSWORD를 입력하여 로그인을 시도한다.

Step 2. 입력한 ID, PASSWORD를 바탕으로 한 블록(Block 3)을 생성한다.

Step 3. 이미 저장되어 있던 사용자 1의 블록 1을 복사한다.

Step 4. 복사한 블록 1과 블록 3을 연결한다.

Step 5. 데이터베이스에 저장되어 있던 블록1과 블록2의 해쉬값을 블록1과 블록3이 연결된 해쉬값을 서로 비교한다.

Step 6. 해쉬값을 서로 비교하여 일치하면 로그인을 허가해 주고, 불일치 시 로그인을 막는다.

위의 Figure 5는 제시한 하이브리드 블록체인을 적용한 데이터베이스를 가지고 웹 서비스 로그인 절차를 설명한 그림이다. 위와 같은 방식을 가지고 데이터베이스를 구축할 시, SQL 인젝션 공격을 통한 데이터 유출 및 노출 또는 손실을 막을 수 있으며, 관리자에 의한 위/변조

의 위험 또한 막을 수 있어, 사람에 의한 데이터 침해는 불가능하다.

6. 결론

데이터를 가지고 행하는 플랫폼 및 분석 시장 규모는 점차 커지고 있지만, 데이터를 안전하게 관리 및 보관하는 보안 기술 시장은 데이터 시장 중 제일 작은 것을 확인할 수 있었다. 데이터 분석을 통한 서비스 품질이 좋다고 하여도 데이터 자체의 탈취나 손실이 있을 경우, 사업체의 타격은 클 것이고, 사용자들의 기업에 대한 신뢰도 또한 낮아질 것이다. 이러한 데이터 유출 및 노출을 막기 위해 퍼블릭 블록체인과 프라이빗 블록체인의 기술을 합친 기술인 하이브리드 블록체인을 이용한 데이터베이스 보안 솔루션을 소개하였다. 프라이빗 블록체인에 사용자들의 정보를 저장 후 이러한 블록들을 가진 집합체를 다시 퍼블릭 블록체인으로 만들어 기존에 있던 퍼블릭 블록체인의 단점과 프라이빗 블록체인의 단점을 상쇄시키고 장점을 부각하게 하여 더욱 뛰어난 데이터베이스 보안 구조를 만들었다. 이러한 제안 방법은 2017년 OWASP이 발표한 위험도 1위인 인젝션 공격을 간단히 막아줄 것이며 데이터의 무결성 또한 보장해 줄 것이다.

REFERENCES

[1] Korea Data Agency(Kdata), “Data Industry White Paper”, 2019.

[2] H.K.Park, Y.S.Kang, C.Y.Park, J.Cho, S.W.Shin, Y.G.Kim, S.Y.Park, M.W.Lee, C.A.Jung, K.Y.Cho, H.D.Choi, “OWASP Top-10 -2017”, 2017.

[3] I.Y.Lee, J.I.Cho, K.H.Cho and J.S.Moon, “A Method for SQL Injection Attack Detection using the Removal of SQL Query Attribute Values”, Journal of the Korea Institute of Information Security & Cryptology Vol.18, No.5, pp.135-147, 2008.

[4] Ministry of the Interior and Safety, “JAVA Secure Coding Guide”, 2012.

[5] S.H.Choi, "HDefence method SQL injection attack using by hacking tools", 2011.

[6] KISA, “Building Web Server and Security Guide Line”, 2010.

[7] J.W.Oh and K.G.Doh, “Implementation and Experiment of An Automated Penetration Testing Tool for SQL/NoSQL Injection Vulnerabilities”, The Korean Institute of Information Scientists and Engineers, pp.727-729, 2014.

[8] B.K.Kim, “Open Source Software Security Issues and Applying a Secure Coding Scheme“, KIISE Transactions on Computing Practices Vol.23, No.8, pp.487-491, 2017.

[9] Ministry of the Interior and Safety, “C Secure Coding Guide”, 2012.

[10] D.Y.Lee, J.W.Park, J.H.Lee, S.R.Lee and S.Y.Park, “Core Technologies of Blockchain and Trends at Home/Abroad”, Communications of the Korean Institute of Information Scientists and Engineers Vol.35, No.6, pp22-28, 2017.

[11] S.Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.

[12] T.H.Kim, “Blockchain Concept and Activities by Sector”, Journal of Electrical World Monthly Magazine Vol.487, pp.58-65, 2017.

[13] J.H.Hong, K.H.Lee and S.H.Yun, "A Scheme for ECU Application Technique using Blockchain", The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.34-35, 2019.

[14] K.H.Kim, “Understanding of Blockchain Technology and applied status”, Industrial Engineering Magazine Vol.25, No.1, pp13-19, 2018.

[15] W.S.Shin and K.H.Kim, ”Hybrid Blockchain System for Public Institutions“, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.630-631, 2019.

[16] K.W.Bae, K.H.Lee and D.H.Kim, “A Scheme for IoT Authentication Using BlockchainForgery/Tamper Protection”, The Korea Internet of Things Society Comprehensive Conference 2019, Vol.4, No.1, pp.46-48, 2019.

[17] B.Sana and H.S.Lim, “Hybrid Blockchain: An Approach for Combining Public and Private Blockchain“, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.956-958, 2018.

배 근 우(Keun Woo Bae) [학생회원]

■ 2014년 3월 ~ 현재 : 백석대학교

〈관심분야〉

모의 해킹, 리버스 엔지니어링, 개인정보보호

이 근 호(Keun Ho Lee) [정회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

〈관심분야〉
이동통신 보안, 융합보안, 개인정보보호