디지털산업정보학회 논문지 제17권 제4호-2021년 12월
http://dx.doi.org/10.17662/ksdim.2021.17.4.043

IoT 네트워크에서 스토리지와 트랜잭션 보호를 위한 이중 블록체인 구조*

박 종 순** · 박 찬 길***

A Double-blockchain Architecture for Secure Storage and Transaction on the Internet of Things Networks

Park jongsoon · Park chankil

〈Abstract〉

IoT applications are quickly spread in many fields. Blockchain methods(BC), defined as a distributed sharing mechanism, offer excellent support for IoT evolution. The BC provides a secure way for communication between IoT devices. However, the IoT environments are threatened by hacker attacks and malicious intrusions. The IoT applications security are faced with three challenges: intrusions and attacks detection, secure communication, and compressed storage information. This paper proposed a system based on double-blockchain to improve the communication transactions' safety and enhance the information compression method for the stored data. Information security is enhanced by using an Ellipse Curve Cryptography(ECC) considered in a double-blockchain case. The data compression is ensured by the Compressed Sensing(CS) method. The conducted experimentation reveals that the proposed method is more accurate in security and storage performance than previous related works.

Key Words : Internet of Things, Blockchain, Information security, Encryption

Ⅰ. 서론

기술의 혁신과 인공지능 알고리즘의 성장은 사물인터넷 개발환경에 매우 중요한 요소이다. 사물인터넷 환경 개발 IoT는 스마트워치, 스마트홈과 같은 다양한 분야에서 융합되어 발전하여왔다. 헬스케어기반 IoT 및 비즈니스기반 IoT[1, 2]에 활용된 통계에 따르면, IoT 기기는 2030년 말까지 240억대 이상이 연결될 것으로 보고 있다. 이러한 예상은 IoT 애플리케이션이 원격제어와 모니터링 기능을 완성했음을 보여주며, 연결된 IoT 장치들은 외부공격에 대비한 보안 문제를 고려해야 한다. 침입 공격은 IoT의 기능을 손상 시킬 수 있으며, 스푸핑 공격을 통해 시스템까지 차단되게 할 수 있다. 더 나아가 분산 데이터베이스에 기반한 기존 시도 IoT 요청을 지원하기 위해 보안 취약점 발생[3]으로부터 보안 전략이 요구된다. 개인정보 보호와 IoT 시스템의 작동을 보장을 위해 기존

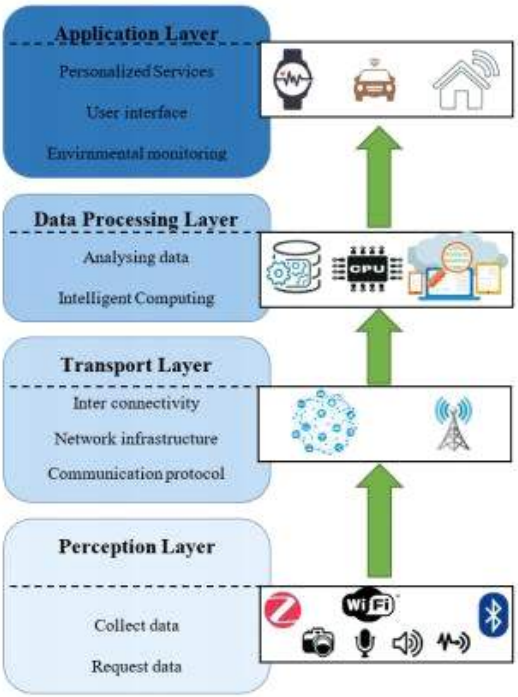
* 본 논문은 서일대학교 학술연구비에 의해 연구되었음
** 서일대학교 소프트웨어공학과 교수
*** 숭실사이버대 정보보안학과 교수(교신저자)

시스템은 사용자 이름으로 보호되며, 암호 트랜잭션을 선택한 보안 메커니즘은 해커들의 IoT 시스템 공격을 허용할 수 있다.

2016년 Mirai 악성코드는 많은 IoT 기기를 감염시켰으며, 그 공격은 분산 서비스 거부(DDoS)로 판명되었다[4, 5]. Mirai 악성 프로그램을 이용하여 원격으로 공격을 시도했다. 대규모 네트워크에서 봇넷의 일부로 사용되는 장치 공격으로 바이러스가 침입했을 때 Mirai 공격은 컴퓨터 제어 서버에 대한 접근을 허용하였고, IoT 장치 및 서버[6]에서 컴퓨터 암호가 유출되어, 공격의 대상이 되었다. 서버는 IoT 기기에 Mirai 바이러스를 보낼 수 있었으며, 기본 사용자 이름 및 암호는 변경되지 않는다. 대부분의 IoT 시스템 사용자가 이 악성코드를 통해 침입했으며, 기본 인증을 변경하지 않았다.

사용자 아이디 및 패스워드가 오랫동안 업데이트 되지 않으면 위험한 공격을 피할 수 있는 보안 메커니즘 사용자 이름 이외의 보안 방법 제공 및 비밀번호가 요청된다. 정보 보안에 대한 최근연구는 <그림 1>과 같이 4개의 단계로 구성된 아키텍처인 인식계층, 전송계층, 처리계층 및 응용계층이며, 인식계층은 센서로 구성하여 제안한다. 인식계층은 센서, 게이트웨이, 라우팅 및 무선, 블루투스, ZigBee, WiFi와 같은 네트워크 기술로 구성된다 [7]. 센서 노드는 제한된 자원과 처리 용량으로 인식 계층에 쉽게 정보획득을 지원 할 수 있도록 가벼운 수준의 보안 방법으로 처리한다. 인터넷 및 모바일과 같은 네트워크 인프라는 전송계층에 속한다 [8]. 이 방법은 지속적으로 서로다른 네트워크와 연관되어 인터넷의 보안 접근에 연결된다. 데이터처리계층에서는 클라우드를 통한 데이터 처리를 보장하는 것을 목표로 하는 계층으로 컴퓨팅 플랫폼 또는 공통 프로세스에서 보안스토리지 데이터의 주요 목적은 안전한 보호이다. 응용계층 보안은 다양한 프로그램들을 지원한다.

IoT에서 개인정보보호 및 모바일장치 접근에 대한 보안기술은 상이하고 각 제품별 전용분석도구가 존재하기 때문에 전용분석자료 수집에 따른 시간·인력·비용 문제가 존재하며, 전용분석도구를 제공받지 못할 경우 영상 확인이 불가능하다는 문제점이 있다. 저장자료의 안전한 보안은 개별보안과 모바일 보안 기술을 포함한다.



<그림 1> 정보 보안 아키텍처

IoT는 하드웨어 및 소프트웨어 보안 서비스 기반 [9]의 저비용이 특징이다. 쌍방 인증 서버와 장치는 연결 보안의 주요 아이디어다.

Huawei 회사에서 보안 솔루션은 하드웨어 레벨 [10] 센서 칩과 네트워크 게이트웨이로 하드웨어 보안 모델을 추가하였다.

블록체인[11, 12]은 분산을 통해 정의하였다. 비대칭 암호화 알고리즘 접근법은 전자 화폐 시스템의 보안을 위해 제안되었고, 비트코인은 안전성을 보장하

는 것을 목표로 했다. 더 낮은 위험과 비용으로 거래 프로세스를 수행할 수 있다. 이 연구는 정확한 보안을 제공하려 P2P 모델을 결합한 블록체인 접근 및 암호화 메커니즘 아키텍처를 기반으로 제안하였다. 이 논문은 2장에서 관련연구를 하였으며, 제안된 설계는 3장에서 (1)설계 구조 기반 이중블록체인 구조 설계, (2) 타원곡선암호화 알고리즘을 활용하여 비대칭 이미지 암호를 연구하고, (3) 정보 압축 및 재구성 방법을 제안하였다. 실험 결과는 4장에서 설명하고, 5장에서 결론으로 정리하였다.

II. 관련 연구

블록체인 개념을 기반으로 IoT 시스템의 보안 모델을 다루는 사례들을 간략히 분석하였다.

Zyskind 등[13]은 다자간 연산으로 구성된 에니그마 연산 모델을 도입했다. 제안된 모델은 저장을 위해 수정된 분산 해시테이블 방법을 사용했다. 외부 블록체인은 네트워크 제어, 접속 관리 등 보안 부분을 보장하였다. 저자가 제공한 에니그마 모델은 비트코인에 사용되는 보안 모델과 유사했다. Y. Zhang 외 연구진[14]은 IoT 환경을 기반으로 한 새로운 E-비즈니스 플랫폼을 제시했다. 저자들은 제안된 E-비즈니스 모델을 전통적인 비즈니스 모델 요구사항에 따라 설계하였다. 블록체인과 스마트 계약은 P2P 거래를 수행하는 데 사용하였다.

Bahga 등[15]은 제조 서비스를 지원하기 위해 산업 시스템을 위한 IoT 모델을 제안했다. 이 모델은 클라우드 기반 제조 개념을 사용하여 설계되었다. 저자는 P2P 전략과 블록체인 기술을 활용한 BPIIoT 플랫폼을 발표했다. BPIIoT 플랫폼에서 보장된 상호 작용은 신뢰할 수 있는 중개자를 요청하지 않은 블록체인에 의해 지원하였다.

Christidis 등[16]은 블록체인과 IoT 기술 집계의 이점을 연구하려고 시도했다. 저자들은 블록체인이 신뢰할 수 없는 사용자들을 위한 분산 P2P 네트워크를 지원했음을 증명한다. 또한 블록체인은 서비스와 자원을 공유하기 쉬운 방법을 암호화 방식으로 자동화할 수 있다. 실험을 통해 블록체인-IoT가 강력하고 안전한 기술이라는 사실이 밝혀졌다.

이번 연구는 트랜잭션과 스토리지에 대한 보안 수준을 개선하고, 계산 복잡성을 줄이며, 암호화 단계를 향상시키는 연구를 진행하였다. 따라서 본 논문은 완전한 서비스를 제공하고 트랜잭션과 스토리지를 안전하게 보호하기 위해 더블블록체인을 사용하는 IoT 플랫폼을 제안함으로써 이러한 문제를 해결하려 하였다.

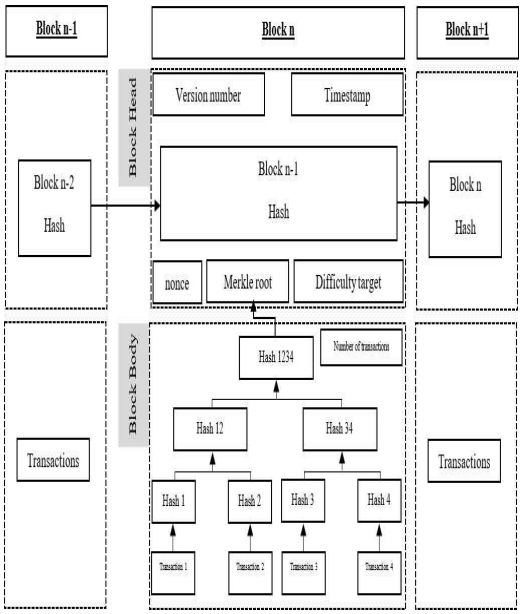
III. 제안된 시스템 구조

이 절에서는 제안된 시스템 구조를 분석한다. 먼저 블록체인의 일반적인 개념이 제시되고, 이어 타원곡선암호화알고리즘이 적용된 더블블록체인 기반 솔루션이 세분화한다. 마지막으로 스토리지 보안을 위한 압축 감지 방법을 설명한다.

3.1 일반개념

상태 시스템의 복제 프로토콜로 정의된 블록체인은 분산 또는 분산 데이터베이스 시스템을 제공한다[17]. 복제 프로토콜로 정의된 블록체인은 보다 높은 안전성과 효율적인 합의 메커니즘이 특징이다. 블록체인 시스템은 일반적으로 (1) 응용계층, (2) 지능형 계약 계층, (3) 데이터 계층, (4) 컨센서스 계층, (5) 네트워크 계층의 5개 계층으로 구성된다. 1계층은 블록체인 시스템의 기초업무를 수행하고, 두 번째 계층은 입력 데이터를 작동시키기 위한 코드의 실행을 보장한다. 세 번째 계층은 블록체인의 데이터 구조를 포

함한다. 각 컴퓨팅 노드는 자체 스토리지를 보장한다. 네 번째 계층은 적절한 합의 프로토콜을 배포한다. 마지막 계층은 P2P 프로토콜을 사용하여 노드 간의 통신을 보호한다.



<그림 2> 블록체인구조

블록체인은 데이터를 순차 블록으로 나눈다. 블록 n은 이전 블록(n-1)과 그 다음 블록(n+1)이 연결된다. 블록은 <그림 2>와 같이 블록 헤드와 블록 본체로 구성되어 있다. 모든 블록 헤드는 이전 블록의 해시 값과 현재 버전 번호, Merkle 루트 및 타임스탬프와 같은 정보를 포함한다. 블록 본문에는 트랜잭션 수와 모든 트랜잭션 레코드가 포함된다.

블록체인은 RSA 알고리즘, 시그니처 알고리즘, 국가 기밀 알고리즘과 같은 많은 암호화 알고리즘을 구현할 수 있다. 노드 간 트랜잭션은 (1) 공용 키와 개인 키를 사용하여 비대칭 암호화 방법을 수행한다. 이 단계는 블록체인의 부정 방지 및 권한을 보장한다. (2) 수신된 트랜잭션의 유효성을 확인한다. 유효한 트랜잭션만 후속 노드로 전송된다. (3) 노드에서 유효한 트랜잭션을 수집하여 타임스탬프가 있는 후보 블록으로 패키징한다. (4) 블록에 유효한 트랜잭션이 포함되어 있고 해시 포인터가 이전 블록에 해당하는 경우 블록을 해당 체인에 추가한다. (5) 트랜잭션을 실행하고 자료를 업데이트 한다.

3.2 시스템 구조

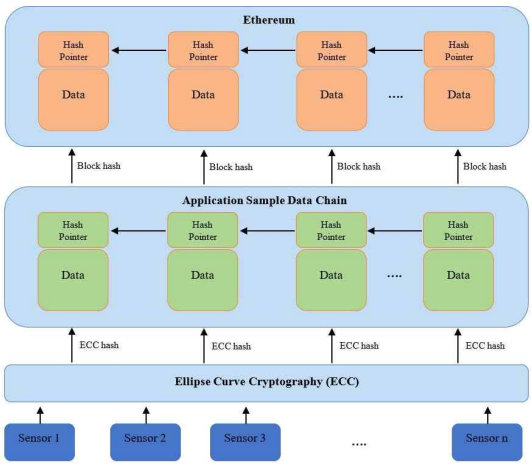
제안한 시스템 구조는 <그림 3>과 같이 서로 다른 단계의 데이터 처리와 관련된 3개의 네트워크 계층으로 구성된다. 첫 번째 계층은 타원 곡선 암호화(ECC)를 기반으로 한다[18]. 이 단계에서 센서는 저장될 샘플링된 데이터를 전송한다. 데이터 센터로서 이 계층은 데이터를 이해하고 처리하고 저장한다. ECC는 공개키 암호알고리즘과 타원 곡선 이산 문제에 기초한 암호화를 통해 정보 보안을 보장한다. 이 솔루션은 타원 곡선의 유한 점 그룹을 사용하여 유한 주기 그룹을 대체하려 시도하였다. ECC 알고리즘은 스토리지 크기를 줄이고, 계산을 줄이고, 보안을 강화하여, 대역폭을 낮춘다는 특징이 있다. 타원 곡선 방법은 Weiestrass 방정식(1)을 기반으로 정의하였다.

$$y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6 \qquad (1)$$

식(1)에서 x와 y는 곡선의 x와 y값을 나타내며, a_i는 실수, 복소수, 유리수 또는 선형수와 관련이 있다. 네트워크의 고유 번호가 각 센서를 나타내고, 센서가 실시간 샘플링된 데이터를 수집하면 이를 정제해 더블 블록체인 시스템으로 전송한다. ECC 네트워크 계층은 콘텐츠 기반 검색을 기반으로 한 보안 수준을 제공한다. 해시가 확인되면 이 프로세스는 ID 세부 정보를 제공하지 않고도 통신을 보장한다. ECC 네트워크에 저장된 데이터는 가져오기 단계에서 콘텐츠

해시를 통해 액세스할 수 있다.

상호 연결된 IoT 장치가 물리적 노드로 간주되며, 시스템에는 수천 개의 노드가 포함된다. 센서에 의해 많은 양의 이기종 데이터가 생성되고, 하루에 생성되는 공간 스토리지는 1TB에 도달하게 된다. 클라우드 스토리지는 정형 데이터 저장 서비스, 블록체인 저장 서비스 및 파일 레벨 저장 서비스를 요구한다. 다음 절에서 설명하는 압축 감지 알고리즘에 의해 데이터 전송이 보장된다. 그런 다음 ECC 메서드(ECC 해시)에 의해 제공된 해시 값이 ASDC(Application program Sample Data Chain)에 해당하는 두 번째 계층에 업로드된다. 이 수준에서 블록은 ECC 해시 값을 저장한 다음 각 블록을 ASDC 체인으로 계산하여 블록 해시 값을 얻는다. 따라서 ECC 해시는 더 적은 스토리지, 더 적은 계산 및 더 높은 안전하게 저장된다.

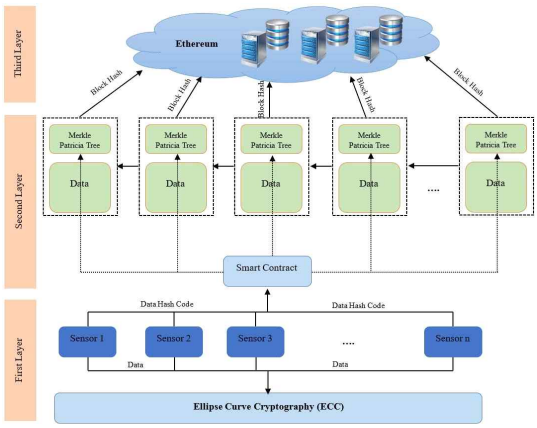


<그림 3> 이중블록체인을 기반으로 한 시스템 구조

결국, 2세대 블록체인인 이더리움에 적용하여보면, 블록 해시는 ASDC 체인에 의해 이더리움으로 업로드된다[19]. 세 번째 계층은 백업 및 공개 쿼리를 보장하는 것을 목표로 한다. 객체 계정과 해시 레코드를 추적 및 검색 활동을 위해 공개적으로 유지하기 위해 특정 메모리를 할당한다.

이중 블록체인 접근법에 기반한 제안된 시스템 구조의 이점은 다음과 같이 요약할 수 있다.

(1) 실시간 이더리움은 샘플링된 데이터와 두 개의 해시 함수, (2) 이더리움 및 ECC 계층에서 수행할 수 있는 데이터의 추적성, (3) 샘플링 동작 및 데이터를 악성 위험 및 변조로부터 보호한다. <그림 4>는 제안된 이중 블록체인의 논리적 흐름을 설명합니다. 이 센서는 두 가지 동작을 수행한다. (1) 샘플링된 데이터를 ECC에 업로드하고, (2) 해시 함수를 계산하여 ASDC 계층으로 전송한다. 데이터 해시는 계정 도메인에 저장되며, ASDC 시스템이 블록해시를 이더리움으로 전송해 저장한다. ASDC 계층에서는 작업 증명이라는 합의 알고리즘을 사용하여 데이터 보호를 제공한다. 제안된 블록체인에 거래 기능이 없으면 공격은 줄어든다. 마지막으로 블록 해시는 주요 체인(이더리움)에 업로드되며, 두 블록 체인 사이의 통신 메커니즘은 Polkadot 기술에 의해 지원된다 [20]. 이 기술을 사용하면 시스템 이중화를 줄일 수 있다. Polkadot 기법은 해시값이 인증되면 블록 높이와 해시값을 이더리움에 업로드해 저장하며, 블록 주소를 포함하는 피드백 프로토콜이 스마트 계약으로 전송된다. 시스템이 해시 값의 변동을 감지하면 블록 제



<그림 4> 제안된 이중 블록체인의 논리적 흐름

거 방법으로 진행한다. 따라서 사용된 Polkadot 방법으로 악의적인 침입을 줄일 수 있었다.

3.3 압축감지

제안된 모델은 압축된 감지 방법을 사용하여 저장된 데이터를 압축한다[21].

압축 감지는 높은 압축률로 압축 신호를 정확하게 복구하는 것이 특징으로 알고리즘은 저장 전에 완료되어야 한다. x는 실제 신호를 나타낸다. 식 (2)는 직교 기저에 선형으로 표시된다.

$$x = \sum_{i=1}^{N} Si\,Vi \qquad (2)$$
$$S_i = V_i^T x$$

여기서 Si는 희소 계수이고, V는 도메인이다. 그런 다음 $\delta_{M\times N}$은 직교 기저행렬 V와의 관계없이 관측행렬로 수행된다. 여기서 C는 감지 매트릭스를 나타낸다. 달성된 관측치는 방정식 (3)에서 y로 나타내었다.

$$y = \delta V x = Cx$$
$$y \in R^M \qquad (3)$$

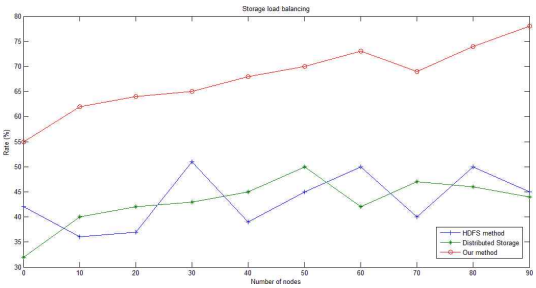
압축 감지 이론은 현재 관측 방정식의 값보다 낮기 때문에 신호를 재구성하도록 요청한다. 여기에서 잘못된 조건의 역 솔루션을 사용하여 해결할 수 있다. 재구성 신호는 방정식 (4)에 의해 $\hat{x}$는 최소값으로 표현될 수 있다.

$$\hat{x} = argmin \| x \|$$
$$y = \delta x \qquad (4)$$

IV. 실험

실험을 통해 프레임워크 설계를 자세히 설명하고 공동 시뮬레이션 접근방식을 기반으로 달성된 검증 결과를 논의한다[22, 23]. 실험에서는 200개의 스토리지 노드를 고려하고, 각 노드는 최대 2TB를 할당하며, 데이터 스토리지와 정보 채널을 포함한 네트워크 속도는 1기가비트/s로 설정되며, 대상 스토리지에는 10TB가 필요하다.

제안된 시스템의 평가는 스토리지 로드 밸런싱 및 스토리지 용량 기준에 따라 수행된다. 압축 감지를 기반으로 제안된 저장 방법의 성능을 더 이해하기 위해 HDFS 저장 방법 및 분산 스토리지로서의 기존 방법과의 비교를 <그림 5>에 나타냈다. HDFS 저장 방법의 표준 편차 곡선이 가장 크다. 이는 HDFS 방법이 가장 불충분한 로드 밸런싱 성능을 달성함을 나타낸다. 반면에, 제안된 압축 감지 방법의 표준 편차 곡선이 가장 완만했다. 따라서 <그림 5>에 그려진 곡선은 제안된 로드 밸런싱 성능이 가장 우수하고 상승 추세가 더 느리다는 것을 증명한다.

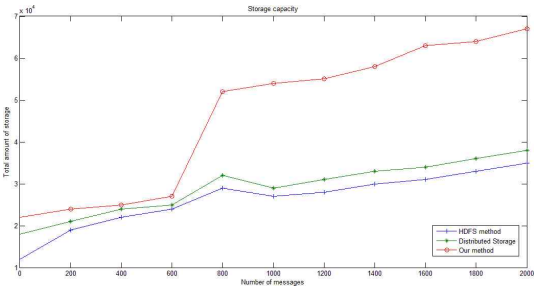


<그림 5> 스토리지 로드밸런싱의 결과 비교

저장 용량은 처리방법의 효율성을 강조하기 위해 계산된다. <그림 6>은 저장용량에 대한 성능비교에 필요한 항목이다.

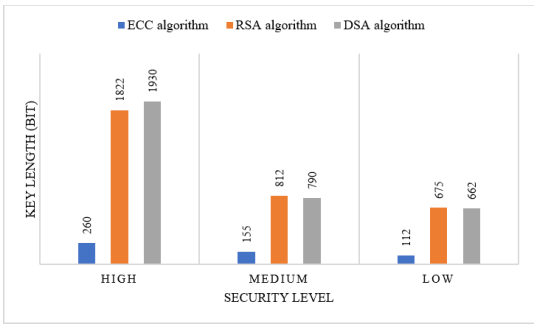
네트워크에 의해 전송되는 데이터의 양에 해당하는 저장 공간으로 <그림 6>에 나타난 세 가지 방법은 정보의 양이 600보다 작을 때 유사한 저장 용량을 지원한다. 그러나 제안한 방법은 HDFS 스토리지 및 분산 스토리지 방법보다 높은 스토리지 용량을 달성했다. <그림 6>에 표시된 결과는 NAT의 접근 방식이

정보를 잃지 않았으며 대규모 데이터에 대한 스토리지를 지원한 것으로 나타났다.



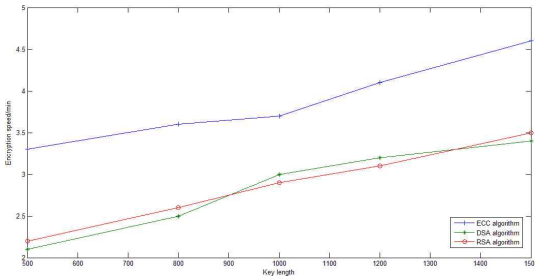
<그림 6> 저장 용량 비교

사용된 ECC 알고리즘의 성능을 평가하기 위해 DSA 암호화, RSA를 비교하여 암호화 알고리즘으로 제시하였다. 평가는 보안 수준과 암호화 속도를 기준으로 실험에서 하위, 중간, 상위의 세 가지 수준의 보안을 고려하였다.



<그림 7> 키 길이에 따른 비교 보안 수준

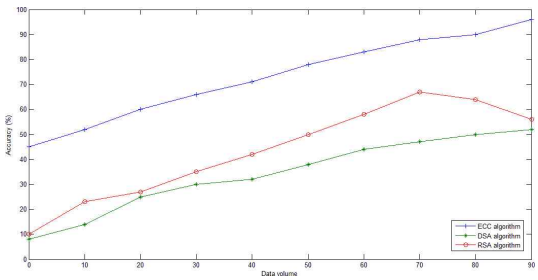
<그림 7>은 보안 수준에 따라 요청된 키 길이를 보여준다. 동일한 수준의 보안을 위해 RSA 알고리즘과 DSA 알고리즘은 ECC 알고리즘에 비해 긴 키가 필요하다. 예를 들어 RSA 및 DSA 알고리즘은 높은 수준의 보안을 보장하기 위해 1800비트 이상을 요청하였으며 ECC 알고리즘은 약간의 키 길이(약 300비트)만 사용하여 높은 수준의 보안을 보장하였다.



<그림 8> 속도 암호화 결과 비교

암호화 결과의 속도는 <그림 8>에 나온 것처럼 키 길이가 늘어날수록 암호화 속도가 빨라진다. 결론적으로, ECC 암호화 알고리즘은 DSA 알고리즘과 RSA 알고리즘에 비해 가장 빠른 방법임을 보여 주었다.

보안 데이터 저장 방법은 일반적인 운영 체제 공격 도구를 사용하여 검증하였으며, (1) 공유 메모리 공격, (2) 가상 시스템 공격, (3) DoS 공격의 세 가지 공격이 고려되었다. 달성된 결과는 RSA 알고리즘과 DSA 알고리즘이 액세스를 막지 못한다는 것을 증명하였으며, ECC 알고리즘은 모든 종류의 공격을 차단하는 데 성공하였다.



<그림 9> 정확도 비교 결과

<그림 9>는 ECC 알고리즘을 기반으로 제안된 암호화 방법의 효과와 실현 가능성을 평가하는 정확도 결과를 보여주었으며, 달성된 결과는 DSA 알고리즘이 약 52%의 정확도에 도달했음을 나타내었다. RSA 알고리즘은 약 56%의 정확도를 얻었지만 데이터 볼

륨이 증가하면 정확도가 떨어진다. <그림 9>는 ECC 알고리즘을 기반으로 제안된 암호화 방법이 96%로 최고의 정확도에 도달했음을 증명했으며, ECC 알고리즘을 사용하면 더 높은 보안을 제공한다고 결론 내릴 수 있다.

Ⅴ. 결론

전 세계적으로 사물인터넷 애플리케이션의 성장과 네트워크에 연결되는 IoT 기기 수의 증가는 큰 과제가 되고 있으며, 기존 분산 시스템은 사용자 이름과 암호 방법을 사용함으로써 발생하는 보안 수준의 취약점을 가지고 있다. 본 논문은 낮은 보안, 대규모 컴퓨팅 및 저속 암호화라는 단점을 극복하려고 시도하였다. 이 논문에서는 이중 블록체인을 기반으로 한 시스템이 사용되었으며, 타원 곡선 암호화 알고리즘은 정보 보안을 보장하며 데이터 압축은 압축 센싱 방식으로 수행하였다.

실험 결과는 스토리지 로드 밸런싱, 스토리지 용량 및 암호화 속도 측면에서 제안된 시스템의 효과를 입증하였으며, 정확도는 96%에 도달하여 RSA 알고리즘 및 DSA 알고리즘보다 우수했음을 확인할 수 있었다.

참고문헌

[1] M. Ben Ayed, A. Massaoudi, and S. A. Alshaya, “Smart Recognition COVID-19 System to Predict Suspicious Persons Based on Face Features,” J. Electr. Eng. Technol., 2021, pp.1-6.

[2] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, “Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies,” IEEE Internet Things J., 2021.

[3] Z. Ellouze, N. Louati, M. Ben Ayed, S. A. Alshaya, and R. Bouaziz, “Design, Implementation, and Evaluation of a Real- Time Object-Oriented Database System,” Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 10, 2019, pp.125–137.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer (Long. Beach. Calif)., vol. 50, no. 7, 2017, pp.80–84.

[5] D. Arivudainambi, V. K. KA, and S. S. Chakkaravarthy, “LION IDS: A meta-heuristics approach to detect DDoS attacks against Software-Defined Networks,” Neural Comput. Appl., vol. 31, no. 5, 2019, pp.1491–1501.

[6] Š. Koprda, Z. Balogh, M. Magdin, J. Reichel, and G. Molnár, “The Possibility of Creating a Low-Cost Laser Engraver CNC Machine Prototype with Platform Arduino,” Acta Polytech. Hungarica, vol. 17, no. 9, 2020.

[7] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, “A new wireless communication paradigm through software-controlled metasurfaces,” IEEE Commun. Mag., vol. 56, no. 9, 2018, pp.162–169.

[8] Q. Jiang, X. Zhang, and J. You, “SnO2: a wonderful electron transport layer for perovskite solar cells,” Small, vol. 14, no. 31, pp.154-165., 2018, pp.154-165.

[9] B. Peng, “Research On Detection Of Malicious Software,” in 2021 2nd International Conference on E-Commerce and Internet Technology (ECIT), 2021, pp.400–403.

[10] M. Busch, J. Westphal, and T. Mueller, “Unearthing the TrustedCore: A Critical Review on Huawei’s Trusted Execution Environment,” in 14th Workshop on Offensive Technologies, 2020.

[11] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, “A survey on blockchain for information systems management and security,” Inf. Process. Manag., vol. 58, no. 1, 2021, pp.397-407.

[12] S. Bouraga, “A taxonomy of blockchain consensus protocols: A survey and classification framework,” Expert Syst. Appl., vol. 168, 2021, pp.384-395.

[13] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentralized computation platform with guaranteed privacy,” arXiv Prepr. ar Xiv1506.03471, 2015.

[14] Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of bitcoin,” in 2015 18th international conference on intelligence in next generation networks, 2015, pp.184–191.

[15] A. Bahga and V. K. Madisetti, “Blockchain platform for industrial internet of things,” J. Softw. Eng. Appl., vol. 9, no. 10, 2016, pp.533–546.

[16] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” Ieee Access, vol. 4, 2016, pp.2292–2303.

[17] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, “Core concepts, challenges, and future directions in blockchain: a centralized tutorial,” ACM Comput. Surv., vol. 53, no. 1, 2020, pp.1–39.

[18] Y. El Housni, “Introduction to the Mathematical Foundations of Elliptic Curve Cryptography,” 2018.

[19] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz, and Y. Smaragdakis, “Madmax: Surviving out-of-gas conditions in ethereum smart contracts,” Proc. ACM Program. Lang., vol. 2, no. OOPSLA, 2018, pp.1–27.

[20] I. Scott, M. de Castro Neto, and F. L. Pinheiro, “Bringing trust and transparency to the opaque world of waste management with blockchain: a Polkadot parathread application,” Available SSRN 3825072, 2021.

[21] A. Bora, A. Jalal, E. Price, and A. G. Dimakis, “Compressed sensing using generative models,” in International Conference on Machine Learning, 2017, pp.537–546.

[22] M. Ben Ayed, A. Massaoudi, S. A. Alshaya, and M. Abid, “System-level co-simulation for embedded systems,” AIP Adv., vol. 10, no. 3, 2020, pp.113-125.

[23] 옥인준, “완전 자동화를 위한 주차관제시스템에 관한 연구”, 디지털산업정보학회논문지 15권 3호, 2019.09, p79~88.

■ 저자소개 ■

박 종 순
Park, Jongsoon

1993년 3월 ~ 현재
서일대학교 소프트웨어공학과 교수
2005년 2월 한국외국어대학교 경영학박사
1990년 2월 한국외국어대학교 경영학석사
1985년 2월 성균관대학교 행정학사

관심분야 : e-business, 기술경영, 시스템분석설계
E-mail : jspark@seoil.ac.kr

박 찬 길
Park, Chankil

2010년 2월 ~ 현재
숭실사이버대학교 정보보안학과 교수
2006년 2월 숭실대학교 공학박사
1994년 8월 서울과학기술대학교 공학석사
1991년 2월 서울과학기술대학교 공학사

관심분야 : 이동통신, IoT, 정보보안, 전자상거래
E-mail : ksdim@naver.com

논문접수일 : 2021년 12월 9일
수 정 일 : 2021년 12월 14일(1차)
2021년 12월 17일(2차)
게재확정일 : 2021년 12월 20일