논문 21-46-06-04 The Journal of Korean Institute of Communications and Information Sciences '21-06 Vol.46 No.06
https://doi.org/10.7840/kics.2021.46.6.956

5G MEC기반 스마트공장을 위한 기밀성을 갖는 블록체인 시스템

이 용 은◆, 김 영 수*, 김 영 식°, 서 창 호**

Blockchain With Confidentiality for Smart Factory Based on 5G MEC

Yong Eun Lee◆, Youngsoo Kim*, Young-Sik Kim°, Changho Seo**

요 약

스마트공장은 IoT를 기반으로 하는 4차 산업혁명의 핵심 기술 중 하나로 5G 이동통신을 스마트공장에 연동함으로써 공장의 장비, 데이터, 인력을 실시간으로 연결할 수 있다. 그러나 IoT기반 시스템에서 중앙 네트워크 및 데이터베이스 시스템을 활용하는 경우, 단일 시스템 문제가 전체 시스템으로 확산할 수 있으며, 시스템 참여자 간 신뢰성 확보를 위한 방안이 요구되고 있다. 이에 대한 대안으로 분산 구조의 노드 간 P2P 통신에 적용 가능한 블록체인 기술이 관심을 받고 있다. 본 논문에서는 5G 이동통신 기반의 IoT 스마트공장 환경을 위한 블록체인 기반 보안 기술을 제시한다. 블록체인 환경에서 사용자 간 데이터 교환 내역을 추적할 수 있는 보안을 제공한다. 특히 제안하는 방법에서는 암호화를 통해 프라이버시 문제를 해결하며, 공장 내 센서 정보를 암호화된 상태로 취합할 수 있는 덧셈 및 스칼라 곱셈에 대한 동형암호인 Paillier 암호를 사용하도록 설계하였다. 취합 정보는 다시 새로운 블록으로 저장되며 관련키 관리를 위해 계층적 비밀공유 기법을 사용한다. 제안하는 시스템은 정보이론적 분석으로 안전성을 증명하였고, 기존방법보다 저장 효율성 및 통신비용을 개선한 것을 비교 분석을 통해 확인하였다.

Key Words : Smart Factory, Blockchain, Homomorphic Encryption, Hierarchical Secret Sharing

ABSTRACT

By applying 5G mobile communication to smart factories, it is possible to connect factory equipment, data, and personnel in real time. However, when a centralized network and database system are used in an IoT-based system, single problem may propagate to the entire system, and a method for securing reliability among system participants is required. As an alternative to this, a blockchain technology applicable to P2P communication between nodes in a distributed structure is attracting attention. In this paper, we present a blockchain-based security technology for an IoT smart factory environment based on 5G mobile communication. It provides security to track the data exchange history between users in a blockchain environment. In particular, the proposed method solves the privacy problem through a homomorphic encryption for addition and

※ 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발)
◆ First Author : Chosun University, wet0146@naver.com, 학생회원
° Corresponding Author : Chosun University, Department of Information and Communication Engineering, iamyskim@chosun.ac.kr, 종신회원
* ETRI, blitzkrieg@etri.re.kr, 정회원
** Kongju National University, 정회원
논문번호 : 202101-010-B-RN, Received January 11, 2021; Revised February 16, 2021; Accepted February 22, 2021

scalar multiplication that can collect sensor information in the factory in an encrypted state without any decryption. The aggregated information is stored in a new block again, and a hierarchical secret sharing technique is used for related key management. The safety of the proposed system was proved through information theoretical analysis, and the storage efficiency and communication cost were improved compared to the existing method.

Ⅰ. 서 론

최근 IoT 기반의 스마트공장 기술이 주목받고 있으며 4차 산업혁명을 위한 차세대 핵심 기술 중 하나로 여겨진다. 5G의 MEC(mobile edge computing) 기능을 스마트공장에 접목하게 시켜서 이를 기반으로 소비자 맞춤형 주문 생산을 고품질 저비용으로 구현하고, 공장의 생산성 향상을 목표로 스마트공장을 구축하기 위한 다양한 연구개발이 진행되고 있다[1]. 특히 5G를 스마트공장에 연동하게 되면 공장의 장비, 데이터, 그리고 인력을 실시간으로 연결할 수 있는 정보교환이 가능해질 것이다.

기존의 IoT 기반 시스템들은 중앙 집중적인 클라이언트-서버 클라우드를 사용하여 매우 높은 성능의 데이터베이스 그리고 네트워크 기술을 활용하였다. 그러나 중앙 집중적인 IoT 시스템은 단일 시스템 오류를 통해서 전체 시스템 문제로 확산할 수 있으며 시스템에 참여하는 참여자 간 신뢰성 부족 문제를 안고 있을 수 있다. 이를 극복하기 위해 분산된 구조의 노드 간 P2P 통신에 적용할 수 있는 시스템으로 블록체인에 관한 연구가 관심을 받고 있다[2]. 이 경우 프라이버시 및 보안 문제를 해결해야 한다.

본 논문에서는 5G 기반의 IoT 스마트공장 환경을 위한 보안 기법을 제안하고 있다. 블록체인에서는 변조 불가능한 정보의 저장이 가능하고 중앙 집중의 데이터베이스가 필요하지 않다. 신뢰 환경에서 다양한 사용자 간 거래 내역을 추적하고 실행할 수단을 제공한다. 제안하는 방법에서는 암호화를 사용하여 프라이버시 문제를 해결하며 센서 정보의 취합(aggregation)을 암호화된 상태로 적용할 수 있도록 덧셈과 스칼라 곱셈에 대해서 동형성(homomorphism)을 제공할 수 있는 Paillier 암호 시스템을 사용한다[3]. 취합된 정보는 새로운 블록으로 암호를 복호하지 않은 채로 새롭게 다시 계산되어 저장된다. 관련된 비밀키는 계층적 비밀 공유기법인 로컬 비밀 공유(local secret sharing)를 사용하며, 이를 통해 저장되는 데이터의 효율적인 저장이 가능해진다[4].

본 논문은 다음과 같이 구성된다. 제2장에서는 논문에서 사용하는 여러 방식에 대한 기본적인 관련 소개를 제시하며, 제3장에서는 제안하는 블록체인 시스템을 설명한다. 제4장에서는 보안 특성 및 성능을 분석하고 제5장에서는 결론을 맺는다.

Ⅱ. 배 경

2.1 Paillier 암호 시스템

Paillier 암호는 P. Paillier에 의해서 1999년에 처음 제안된 것으로[3], 키 생성, 암호화, 복호화 알고리즘으로 구성되어 있다.

2.1.1 키 생성

다음 조건을 만족하는 랜덤 소수 p와 q를 생성한다.

$$\gcd(pq,(p-1)(q-1))=1.$$

그리고 다음 값을 modulus로 계산한다.

$$n=pq,\ \lambda=lcm(p-1,q-1).$$

$Z_{n^2}^*$에서 랜덤한 값 g를 선택하고 다음 값을 계산한다.

$$\mu=(L(g^{\lambda} \bmod n^2))^{-1} \bmod n$$

여기서 $L(x)=(x-1)/n$이고 이때 g에 따라 역원이 존재하지 않을 수 있는데, 그 경우 다시 g를 선택하여 계산을 반복한다. 이때 공개키는 (n,g)이고 개인키는 (λ,μ)이다.

2.1.2 암호화

m이 n보다 작은 암호화할 메시지라 하자. r이 n보다 작고 n과 서로소인 랜덤한 값이다. 그러면 암호문은 $c=g^m \cdot r^n \bmod n^2$이고 $c \in Z_{n^2}^*$이다.

2.1.3 키 생성

평문은 $m=L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n$으로 계산한다.

2.1.4 동형 연산

Paillier는 다음과 같이 덧셈과 스칼라 곱셈에 대해서 동형 특성이 있다. 즉, 서로 다른 두 암호문에 특정 연산을 적용하여 대응되는 각각의 메시지의 산술 덧셈에 대한 암호문을 얻을 수 있으며, 마찬가지로 암호문에 또 다른 특정 연산을 적용하여 대응되는 평문에 스칼라 곱셈을 한 평문의 암호문을 복호 과정 없이 얻을 수 있다.

1) 두 암호문이 주어지면 평문의 동형 덧셈

$$D(E(m_1,r_1)\cdot E(m_2,r_2) \bmod n^2) = m_1+m_2 \bmod n.$$

2) 암호문과 평문이 주어지면 평문의 동형 덧셈

$$D(E(m_1,r_1)\cdot g^{m_2} \bmod n^2) = m_1+m_2 \bmod n.$$

3) 스칼라 곱셈에 대한 동형 연산

$$D(E(m_1,r_1)^k \bmod n^2) = km_1 \bmod n.$$

2.2 계층적 비밀공유

2.2.1 파라미터 생성

[4]에서 제안한 계층적 비밀공유는 부분 복구 가능 부호와 함께 결합되어 있다. 정보 비트의 길이가 k비트이고 부호의 길이가 n인 부호로 부분 복구 가능 한계가 r인 부호를 (n,k,r) LRC라 부른다. 이를 위해서는 다음 조건을 만족하는 다항식 $g(x)$를 정의한다.

조건 1) $g(x)$의 차수는 $r+1$이다.

조건 2) 임의의 $x\in A_l$, $l\in[1,\frac{n}{r+1}]$에 대해서 $g(x)=c_l$를 만족하는 유한체 F_q의 부분 집합 A의 분할 $\{A_1,...,A_{n/(r+1)}\}$이 존재한다.

이와 같은 $g(x)$는 대표적으로 다음과 같이 생성할 수 있다. 먼저 유한체 F_q의 두 개의 부분집합 H, G에 대해서 G에 속한 원소와 H에 속한 원소를 곱한 값이 다시 H에 포함될 때, 즉, $\{hg : h\in H,g\in G\}\subseteq H$ 일 때 H는 G에 의해서 곱셈에 대해 닫혀 있다고 한다. p가 임의의 소수라 하고, l, s, m이 $l|s$와 $p^l \bmod m = 1$를 만족한 정수라 하자. 그러면 H는 F_{p^s}의 덧셈에 대한 부분군(subgroup)이 된다. 그리고 H는 F_{p^l}에서 곱셈에 의해서 닫혀 있다. 그러면 α_1, ..., α_m이 F_{p^s}에서의 1의 m차 거듭제곱근(mth roots of unity)이라 하자. 그러면 임의의 $b\in F_{p^s}$에 대해서 다음과 같이 생성한 다항식 $g(x)$은 H의 코셋의 합집합, $\cup_{1\le i\le m}(H+b\alpha_i)$에서 항상 상수가 된다[5].

$$g(x)=\prod_{i=1}^{m}\prod_{h\in H}(x+h+\alpha_i).$$

그리고 이 합집합의 크기는 다음을 만족한다.

$$|\cup_{1\le i\le m}(H+b\alpha_i)| = \begin{cases}|H| & \text{if } b\in H\\ m|H| & \text{if } b\notin H\end{cases}.$$

2.2.2 비밀 Share 생성

LRC로 부호화된 데이터에서 한 개의 심볼이 삭제되었을 때 다른 r개의 심볼을 사용해서 복구할 수가 있다. k와 n이 각각 r과 $r+1$로 나누어떨어진다고 할 때, 메시지 벡터 $a=(a_{i,j})\in F_q^k$에 대해서 인코딩 다항식은 다음과 같이 주어진다. 먼저,

$$f_i(x)=\sum_{j=0}^{k/r-1}a_{i,j}g(x)^j \tag{1}$$

이고 다시

$$f_a(x)=f_{r-1}(x)x^{r-1}+f_{r-2}(x)x^{r-2}+...\\ +f_1(x)x+f_0(x)$$

로 정의된다. 이때 다항식 $f_a(x)$에 집합 A에 속한 모든 원소에 대해서 계산하면 메시지 a에 대한 코드워드를 얻을 수 있다.

2.2.3 비밀 복구

만일 저장 장치 내에서 한 심볼이 손상되었다고 가정하면 $f_i(x)$는 (1)에서처럼 $g(x)$의 선형결합으로 정의되었기 때문에, $g(x)$가 상수이므로 $f_i(x)$ 역시 같은 집합 A내에서 상수가 된다. 따라서 인코딩 다항식 $f_a(x)$와 디코딩 다항식 $\delta(x)=\sum_{i=0}^{r-1}f_i(\alpha)x^i$가 정확히 일치하고, 디코딩 다항식 $\delta(x)$의 차수는 $r-1$보다 작다. 따라서 r개의 다른 심볼이 주어지면 $\delta(x)$ 다항식을 정확하게 구할 수가 있다. 즉, 관련된 정보가 복구된다.

로컬 비밀공유는 계층적 비밀공유 방식으로 두 개의 비밀 값이 존재한다[4]. 하나는 n개의 모든 피어들 사이에 공유되는 전역 비밀(global secret)이고, 다른 하나는 $r+1$개의 피어로 구성된 그룹 내에서 존재하는 로컬 비밀(local secret) 값이다. 여기서 $n/(r+1)$로 가정한다. 전역 공유된 비밀은 전체 피어 중에서 임의의 $k+k/r-1$개의 피어의 share를 모아 복구가 가능하며, 로컬 공유된 각 비밀은 해당 로컬 그룹 내 피어 중 임의의 r개의 피어로부터 share를 모아 복구가 가능하다. 이런 계층적 공유는 n개의 share를 전체 노드에 배포하면서 한 번에 이루어진다. 계층적 비밀공유를 그림 1.에서 도시하였다.

로컬 비밀공유에서는 다음과 같은 특징이 증명되었다.

특징 1) 전역 비밀 값은 임의의 $k+k/r-1$개의 피어들의 share를 모으면 복구 가능하다.

특징 2) 부분 비밀들은 대응되는 피어들의 그룹 내부에서의 임의의 r개의 피어의 share를 모으면 복구 가능하다.

특징 3) 만일 $k>r$이면, 한 피어들의 그룹의 r개의 피어들로는 다른 피어들의 그룹의 부분 비밀을 복구할 수가 없다.

특징 4) 전역 비밀은 k/r개의 피어들의 그룹에 포함된 부분 비밀들을 사용해서 복구할 수 있다.

특징 5) 전역 비밀은 k/r개의 피어들의 그룹에 있는 피어에 접근 가능하고 각 그룹 당 r개의 피어에 접근 가능하다면 k개의 피어에 접근함으로써 복구할 수 있다.

그림 1. 계층적 비밀공유
Fig. 1. Hierarchical Secret Sharing

Ⅲ. 제안하는 블록체인 방식

3.1 필요한 보안 서비스

블록체인에서는 무결성과 불변성이 중요한 보안 특성으로 다뤄진다. 무결성은 블록체인에 저장된 데이터는 대부분의 피어가 보안 손상이 되지 않는 이상 무결성이 보장된다. 특히 많은 응용에서 블록체인에 저장된 데이터의 불변성에 주목하고 있다. 대다수의 피어를 동시에 보안 손상을 일으키는 것이 현실적으로 어렵고, 일부 보안 손상이 일어날 때도 블록체인에 저장된 다른 정상 데이터를 사용해서 쉽게 복구할 수 있다. 이는 블록체인은 본질상 반복 부호(repetition code)의 속성이 있어서, 다수결 복호(majority decoding)가 가능하다. 블록체인을 만드는 과정에서 사용되는 해시값 생성에 추가 요건이 붙는 경우 무결성 보장이 강화될 수 있다. 하지만 원래 제안된 블록체인에서는 에너지의 과도한 낭비로 지속가능성(sustainability)에 문제가 제기되어 다른 형태의 증명 방식이 새롭게 개발됐다. 전통적인 블록체인 시스템에서는 같은 정보가 각 피어에 반복 저장됐다. 피어마다 같은 정보가 중복해서 그대로 저장되기 때문에 무결성이 보장되지만, 저장 공간 효율성 측면에서는 문제가 많이 있다. 따라서 반복 부호가 아닌 다른 대수적 부호화 방법을 적용하여 저장 공간을 효율화하기 위한 연구가 진행되었다.

비트코인으로부터 시작된 블록체인의 원 아이디어에서는 장부가 평문으로 저장되어 누구나 확인할 수 있도록 만들었기 때문에 기밀성에도 문제가 있었다. 기밀성을 보장하기 위한 블록체인으로서 암호화해서 저장되어야만 한다. 이 경우 복호를 위해서는 Paillier 암호의 개인키가 함께 저장되어야 한다[3]. Ramen 등은 Shamir의 비밀공유 방식과 MDS 부호를 사용해서 기밀성과 저장 공간을 효율적으로 제안할 수 있는 새로운 방법을 제안하였다[6,7]. Kim 등은 로컬 비밀공유 방법을 새롭게 제안하였고 로컬 비밀공유의 부분 복구 가능 부호(locally repairable code)의 특성을 사용해서 저장 공간 효율화를 동시에 달성하는 방법을 제시하였다[4].

스마트공장에서 사용되는 주요 데이터 생성원은 각종 센서값으로, 센서값은 개별 값이 의미가 있을 수도 있지만, 센서값의 집계값(aggregation)이나 통계값이 중요하게 활용된다. 이때 센서에서 수집된 정보는 생산 공정이나 기업의 핵심 지식 자산과 관련된 값일 수 있으므로 암호화되어 보호되어야 한다. 예를 들어 제조 공정에서 각 장치의 온도를 일정 수준으로 맞추는 것이 중요한데, 온도의 상태는 센서로부터 수집되고 수집된 정보가 집계되어 관리되어야 한다. 만일 온도가 변하면 이에 따라 수율이나 품질에 영향을 줄 수 있고, 반도체 공정이나 의약품 생산 공정 같은 경우 특정 단계의 정확한 온도 값이 기업 고유의 생산 비결 또는 핵심 기밀일 수 있다. 이 경우 주요 생산 데이터가 안전하게 기밀성을 유지하면서 관리될 필요가 있다.

3.2 제안하는 블록체인 시스템의 구조

제안하는 블록체인 시스템에서는 스마트공장 내에서의 5G MEC를 사용해서 연결된 각종 장치에서 발생하는 주요 측정 및 제어 데이터를 보관한다. 5G의 MEC이 기지국을 중심으로 형성된다고 가정한다. 하나의 MEC이 전체 스마트공장 시스템이 대응될 수도 있고, 규모에 따라 하나의 스마트공장에 단일 5G 네트워크의 여러 MEC이 포함될 수도 있다. 또는 사설 5G망으로 구성된 네트워크에 여러 MEC이 포함될 수도 있다.

각 MEC 내부에서는 각 부분별로 무결성을 보장하고 책임 추적이 필요한 정보가 생산되고 저장된다. 많은 정보를 효율적으로 저장하기 위해서 분산 저장 블록체인(distributed storage blockchain)을 사용하며[6,7], 특히 저장된 데이터의 비밀키 및 해시값을 저장하기 위해 로컬 비밀 공유[4] 기법을 사용해서 저장 공간을 효율화한다.

우선 각 노드에서는 스마트공장에서 저장 및 관리되어야 하는 각종 거래 내역의 사본을 블록으로 만들어 저장한다. 이때 t번째 공장에서 생성된 데이터 블록의 해시를 B_t라하고, 이때 각 블록의 해시 트리 값을 H_t라 한다. 여기서 $W_t=(H_{t-1}\|h_2(B_t))$라하고, 따라서 $H_t=h_1(W_t)$이다. 또한 $h_1(\cdot)$과 $h_2(\cdot)$는 암호학적 해시 함수이다.

그림 2. 스마트공장에서의 MEC 배치 예시
Fig. 2. Deployment of MEC in Smart Factory

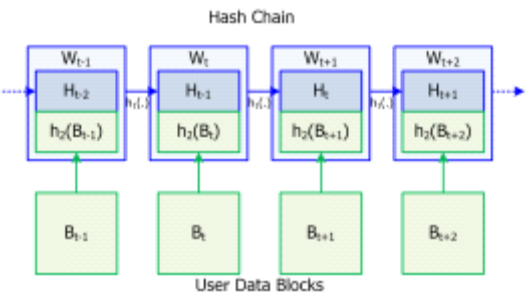

그림 3. 블록체인 블록 구조
Fig. 3. Chaining Structure of Proposed Block Chain

전통적인 블록체인 시스템에서는 모든 참여 노드들이 거래 내역의 사본을 저장하고 있으며 블록체인의 크기가 수시로 변하는 과정에서 과반의 참여 노드에 저장된 정보를 동시에 변조하기 어려우므로 저장된 데이터의 무결성이 보장될 수 있다. 그러나 이 경우 같은 정보가 반복 저장되어 매우 비효율적인 형태의 저장방식을 갖게 되는 문제가 있다. 예를 들어 B_t의 크기가 η비트이고 W_t의 크기가 q비트라 하자. 그러면 한 피어의 거래 당 블록체인의 저장 비용은 $q+\eta$ 비트가 된다.

DSB 시스템은 바로 이 비용을 줄이기 위해 고안된 것으로 매 트랜잭션이 서로 다른 암호화키로 암호화된 후에 일부 피어들로 분배된다. 암호화 키와 해시값들은 해당 피어들로 구성된 그룹 내부에서 비밀키 공유를 통해서 저장된다[6,7]. 비밀키 공유를 위해 전체 피어의 개수가 n이고 이 피어들을 L개의 집단으로 구분하고 각 집단에는 $r+1$개의 피어가 포함된다고 하자. 이때 $n/(r+1)=L$의 관계가 성립한다. 먼저 $E_{K_t^{(l)}}(m)$을 공개키가 (n,g)이고 개인키가 (λ,μ)인 Paillier 암호라 하고 개인키는 편의상 $K_t^{(l)}$로 나타내자. 여기서 $1\le l\le L$이다.

전통적인 블록체인의 경우에는 모든 피어들이 전체 원장을 저장하기 때문에 하나의 오류가 생긴 피어를 복구하기 위해서 다른 피어 하나만 참고하는 것으로 충분하다. 만일 서비스 거부 공격이 DSB 기반의 블록체인 시스템에 수행된다면, 단일 피어에서의 손실이 비밀키 자체의 손상으로 이어져 피어의 부분집합 하나에 저장된 데이터가 완전히 손상될 수가 있다. 이런 문제를 해결하기 위해서 LSS(Local Secret Sharing)-DSB 방식이 새롭게 제안되었다[4]. 제안하는 스마트공장을 위한 블록체인 시스템은 다음과 같이 구성된다.

먼저 피어들의 집합을 $A=\{A_1,\ldots,A_L\}$로 분할한다. 그리고 해시값 $W^{(t)}$를 전역 비밀 $s^{(t)}$로 지정한다. 그러면 F_q^{k-1}에서 하나의 랜덤 벡터 $a^{(t)}$를 고른다. 로컬 비밀들 $s_l^{(t)}$를 모두 계산한 후에 $f_a^{(t)}(\alpha_i)$를 다음과 같이 계산한다. 다항식 $g(x)$와 피어들의 분할 $A=\{A_1,\ldots,A_L\}$에 대해서 다음을 연산한다.

단계 1) 랜덤 벡터 $a\in F_q^k$에 대해서 $s_t^{(l)}=a_{0,0}$로 정한다.

단계 2) 모든 피어들의 그룹 A_i에 대해서 단계 2-1)과 단계 2-2)를 계산한다.

단계 2-1) 로컬 비밀을 $s_t^{(l)} = f_0(\beta) = \sum_{j=0}^{k/r-1} a_{0,j} g(\beta)^j$ 로 지정한다. 이때 $\beta \in A_l$이다.

단계 2-2) $C = \{(f_a(\alpha)) | \alpha \in A\}$를 계산한 후에 n개의 피어로 분배한다.

이때 하나의 거래에 대응되는 데이터 블록 B_t는 다음과 같은 절차를 통해 암호화된다.

단계 4) $s_t^{(l)}$로 B_t를 암호화하고 η비트 길이인 $c_t^{(l)} = E_{s_t^{(l)}}(B_t)$를 얻는다.

단계 5) $(r+1, r)$ MDS 인코딩으로 $s_t^{(l)}$를 인코딩해서 A_l의 각 피어에 저장한다.

이미 블록에 포함된 데이터에 대해서 스마트공장에서 데이터가 처리되면서 새로운 데이터가 생성될 수 있다. 예를 들어 B_{t_1}와 B_{t_2} 두 블록의 데이터를 전체를 더해서 새로운 블록을 만드는 경우 Paillier 암호로 암호화가 되어 있으므로, $B_{t_1} + B_{t_2}$는 그 자체로 같은 비밀키로 암호화된 유효한 암호문이 된다. 따라서 새로운 암호문에 대한 새로운 해시 체인을 다시 생성하면 새로 연산된 블록은 암호를 해제하지 않은 채로 추가 블록으로 그대로 저장하는 것이 가능하다.

Ⅳ. 성능 평가 및 분석

4.1 보안 분석

본 논문에서 고려하는 공격 모델은 크게 두 가지이다 [6,7]. 첫 번째는 랜덤 서비스 거부 공격이다. 이 공격에서는 블록체인에서 문제가 생긴 데이터 복구를 방해하여 손상된 데이터에 대한 손실이 실제로 일어나도록 만든다. 두 번째는 시스템 정보를 알고 있는 공격자에 의한 특정 목표 데이터에 대한 손상(corruption) 공격이다. 능동적인 공격자에 의해서 블록체인에 저장된 데이터에 잠재적인 교란이 일어날 수 있다. 공격자에 의한 데이터 손실 여부를 확인하기 위해 두 공격이 독립적이라 가정한다.

일부 피어들이 서비스 거부 공격을 당하면 데이터 손실이 일어날 수 있다. 공격자가 각 영역의 피어에 분포된 블록 B의 데이터를 손상하려 한다고 가정하자. 이때 손상 공격은 피어에서 독립적으로 ρ의 확률로 데이터 손실이 일어날 수 있다고 가정한다. 이때 $\bar{\rho} = 1 - \rho$라 가정한다. $r = n/k$가 피어 네트워크에서 데이터 사본의 개수이다. 이때 서비스 거부 공격이나 단일 노드 상의 오류로 데이터 손상이 발생한다. 먼저 서비스 거부 공격을 하는 비적응적(non-adaptive) 공격자는 시스템 파라미터에 대해 알지 못하며 피어 사이에서 데이터 분포에 대한 정보가 없다고 가정한다. 공격자는 C개의 피어를 랜덤으로 선택하고, C는 확률 분포 $P_d(\cdot)$에 따라 랜덤하게 선택된다. 서비스 거부 공격을 위해서 보안 손상된 피어는 요구된 데이터 블록에 대응되는 데이터를 반환하지 않는다. P_d의 선택은 자원 제약적인 공격자가 데이터 손실확률을 최대화하기 위해 선택한다. 영역 i에서 손상된 피어의 수가 X_i라하고 Y_i는 데이터 손상을 겪은 것의 개수라 하자. 그래서 $(X_i, ..., X_r)$은 n개의 객체, C번의 추출, r개의 형태 중 k개의 객체를 갖는 multivariate hyper geometric 분포를 따른다. 따라서 공격자가 C개의 피어를 공격해서 데이터 손상을 일으킬 확률은 다음과 같다.

$$P[DataLoss|C] = E[(1-\bar{\rho}^k)^{r-\sum_{i=0}^{r}\mathbf{1}(X_i>0)} | C]$$

여기서 $\mathbf{1}(\cdot)$은 파라미터 조건이 만족할 때 1을 반환하는 지시함수이다. 그러면 서비스 공격을 하는 공격자는 손상할 수 있는 피어의 기댓값의 총량 B_d에 의해서 제한되고 따라서 분포 P_d은 다음 선형 프로그램을 통해서 결정할 수 있다.

$$P_d \in \arg\max_p \sum_{c=0}^{n} p(c) E[(1-\bar{\rho}^k)^{r-\sum_{i=0}^{r}\mathbf{1}(X_i>0)} | C=c]$$

여기서 $\sum_{c=0}^{n} cp(c) \le B_d$, $\sum_{c=0}^{n} p(c) = 1$, 그리고 모든 c에 대해 $p(c) \ge 0$를 만족한다. 영역의 대칭성을 가정하면 하나 이상의 손상이 일어난 영역의 수에 대한 pmf(probability mass function)는 다음과 같다.

$$P(\sum_{i=1}^{r}\mathbf{1}(X_i>0) = \tilde{r}) = \binom{r}{\tilde{r}}\binom{\tilde{r}k}{c} / \binom{n}{c}$$

두 번째로 능동적 공격자는 저장된 블록 데이터 B_t에 변조를 가해서 B_t'을 만들고자 시도한다. 이 경우 성공적인 파괴의 의미를 다음과 같이 정의한다. 피어

를 파괴하는 공격자는 1) 피어에 저장된 내용을 알고 2) 피어가 해당 블록에 접근권을 갖고 있을 때 블록을 변조하고 3) 체인의 무결성을 보존하는 해시값을 변조한다. 즉 공격자들은 과정 중의 다른 거래 내역을 무효로 할 수 없다. 이때 공격자는 계산적으로 제한되어 있으므로, 메시지/해시 공간에서 전수 조사를 수행할 수 없다. 또한, 지역적 데이터 손실이 특정 피어에 대한 능동적인 공격 동안 일어나지 않는다고 가정한다. 추가로 공격자는 데이터 저장을 정의하는 파라미터에 대한 값을 알고 있다고 가정한다. 공격자가 네트워크상의 어떤 피어를 파괴할 능력은 파라미터 P_{tc}로 표현하고 이 값은 0과 1 사이의 실수이다. 네트워크는 모두 균일하고 손상은 피어간에 독립적이고 동등한 (independently and identically distributed) 방식으로 일어난다고 가정한다.

각 데이터의 사본들이 k개의 피어에서 일어나고 복구 알고리즘은 블록체인상의 d이전 블록까지를 찾게 된다. 이 경우 공격자가 성공적으로 손상할 피어의 총 개수는 $n/2+2dm$이다. 그러면 공격자가 각 영역의 절반의 데이터를 먼저 훼손하고, 적어도 이후에 $2dm$ 피어를 추가로 손상하기 위해서 $r/2$개의 영역의 집합을 찾아야 한다. 최악의 경우를 가정하여 공격자가 정확히 이후의 $2dm$개의 피어를 손상한다고 가정하자. 그러면 공격자가 각 네트워크에서 이의의 피어를 손상할 확률을 P_{tc}라 정의했으므로, 각 시스템에서 목표 블록을 변경할 확률은 다음과 같다.

$$P_{TA}=\binom{r}{r/2}P_{tc}^{n/2+2dm}$$

여기에서 d가 커지면 이 공격 확률이 줄어들게 된다. 또한 k의 크기가 커지면 r이 작아져 공격 확률이 줄어든다. 하지만 데이터 손실확률이 높아진다.

4.2 성능 분석

각 피어들의 그룹에 대해서 암호화를 위한 비밀키는 부분 비밀을 통해 분배되고 해시값은 모든 피어들에 공유될 수 있는 전역 비밀로 분배된다[4]. 암호화된 데이터 블록은 $(r+1,r)$ MDS 코드를 사용해서 암호화된 데이터 블록 $m_l^{(t)}$를 인코딩한다. 이 코딩을 통해서 단일 피어에 오류가 발생한 경우에 복구를 위한 통신비용을 줄일 수 있으며 외부의 의도적인 서비스 거부 공격에 대해서 저항성을 갖게 된다.

그러면 DSB의 하나의 피어의 거래 블록당 저장 비용은 다음과 같이 나타낼 수 있다. 먼저 $c_t^{(l)}$은 η비트이고 총 $r+1$개의 피어로 분산되어 저장된다. 만일 $c_t^{(l)}$이 η비트이고 $r+1$개의 피어에 나누어 저장되는 경우, 그리고 $s_t^{(l)}$이 q비트라 하면, DSB 하나의 피어의 트랜잭션당 저장 비용은 다음과 같이 계산할 수 있다.

$$S_{DSB}=\frac{\eta}{r}+q$$

만일 비밀키 크기가 데이터 블록의 크기보다 훨씬 더 작다면 (즉, $q \ll \eta$) DSB는 저장 비용을 크게 줄일 수 있게 된다. [6],[7]에서 제시한 분산 블록체인 저장 시스템에서는 단일 피어에 저장된 데이터에 문제가 발생하는 경우 해당 피어들이 포함된 그룹의 암호화를 위한 비밀키와 해시값이 복구되지 않기 때문에, $r+1$개의 다른 피어들로 문제가 확산한다. 하지만 계층적 비밀공유에서는 단일 피어에 저장된 데이터에 문제가 생기는 경우 로컬 내의 데이터를 활용하여 복구할 수 있으므로 복구를 위한 통신비용을 크게 줄일 수 있다.

제안하는 시스템에서의 통신비용은 새로운 트랜잭션을 저장하는 데 드는 비용과 피어 오류를 복구하기 위한 비용으로 나눌 수 있다. 전자를 트랜잭션 통신비용이라 하고 후자를 복구 통신비용이라 하자. 그러면 각 피어는 새로운 트랜잭션을 위해서 S개의 데이터를 수신해야 하므로 피어 당 통신비용은 트랜잭션당 한 피어의 저장 비용에 비례한다. 이때 복구를 위한 통신비용은 다음과 같이 구할 수 있다. 서비스 거부 공격하에서의 한 피어는 요청에 응답할 수 없으며 해당 데이터를 사용할 수 없게 된다. 단일 피어의 오류가 가장 일반적인 시나리오로, 고전적인 블록체인에서 모든 피어는 트랜잭션들의 전체 원장을 저장하기 때문에 단일 피어 오류는 다른 피어의 저장된 원장을 전달받아 복구할 수 있다. 전통적인 방식에서는 다음과 같은 복구 통신비용이 발생한다.

$$C \propto \eta+q$$

이것은 가장 작은 복구 비용으로 사실상 전통적인 블록체인은 반복 부호에 대응되기 때문에 가장 적은 복구 통신비용을 갖는다. 본래의 DSB 방식에서는 단일 피어 오류는 해당하는 피어들의 그룹 전체를 마비시키게 된다. 이를 복구하기 위해서는 다른 그룹들의 $r+1$개의 피어에 접근해야 한다. 따라서 이 경우 ρ를

다른 그룹에 접근하는 데 드는 비용이라 할 때, 복구 통신비용은 다음과 같다.

$$C \propto \eta + 2(r+1)q + \rho$$

이때 계층적 비밀공유를 사용하게 되면 각 데이터 블록이 같은 그룹 내의 다른 r개의 피어에 접근하여 해결할 수 있으므로 다음과 같은 값을 갖는다.

$$C \propto \eta + rq$$

계층적 비밀공유를 사용하면 피어들의 오류에 더 안정적으로 동작할 수 있다. 우선 전통적인 블록체인의 경우 통 $n-1$개의 피어 오류를 감내할 수 있지만, DSB의 경우 피어들의 모든 그룹에서 하나의 피어들이 오류를 일으킨 경우 L개의 오류만으로 전체 데이터 손실이 발생할 수 있다. 계층적 비밀공유와 함께 사용하게 되면 각 피어들의 그룹들은 단일 피어 오류를 스스로 해결할 수 있고 따라서 $2n/(r+1)-1$개의 오류가 발생하더라도 그룹 내의 통신만으로 문제없이 손상된 데이터를 복구할 수가 있다. 물론 모든 피어 그룹 내에서 2개 이상씩 피어들이 손상된 경우에는 복구할 수 없는 한계가 있다. 다음 표 1에서 저장 비용과 통신비용과 피어 오류에 대한 안전성을 비교하고 있다.

표 1. 블록체인 시스템의 비용 비교
Table 1. Cost Comparison between Blockchain Systems

	Storage Cost	Recovery Cost	Stability
Conventional Blockchain	$\eta+q$	$\eta+q$	$n-1$
DSB	$\eta/(r+1)$ $+2q$	$\eta+2(r+1)q$ $+\rho$	$L-1$
Proposed LSS-DSB	$\eta/r+$ q	$\eta+rq$	$2L-1$

V. 결 론

본 논문에서는 5G 기반의 IoT 스마트공장 환경을 위한 보안 기법을 제안하고 있다. 블록체인에서는 변조 불가능한 정보의 저장이 가능하고 중앙 집중의 데이터베이스가 필요하지 않다. 신뢰 환경에서 다양한 사용자 간 거래 내역을 추적하고 실행할 수단을 제공한다. 제안하는 방법에서는 암호화를 사용하여 프라이버시 문제를 해결하며 센서 정보의 취합(aggregation)을 암호화된 상태로 적용할 수 있도록 덧셈과 스칼라 곱셈에 대해서 동형성(homomorphism)을 제공할 수 있는 Paillier 암호 시스템을 사용한다[3]. 취합된 정보는 새로운 블록으로 다시 저장된다. 관련된 비밀키는 계층적 비밀 공유기법인 로컬 비밀 공유(local secret sharing)를 사용하며, 이를 통해 저장되는 데이터의 효율적인 저장이 가능해진다.

References

[1] T. Taleb, I. Afolabi, and Miloud Bagaa, “Orchestrating 5G network slices to support industrial internet and to shape next-generation smart factories,” *IEEE Network*, vol. 33, no. 4, pp. 146-154, Jul./Aug. 2019.

[2] J. Wan, J. Li, M. Imran, Di Li, and Fazal-e-Amin, “A blockchain-based solution for enhancing security and privacy in smart factory,” *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, pp. 3652-3660, Jul. 2019.

[3] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proc. EUROCRYPT*, pp. 223-238, 1999.

[4] Y. Kim, R. K. Raman, Y.-S. Kim, L. R. Varshney, and N. R. Shanbhag, “Efficient local secret sharing for distributed blockchain systems,” *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 282-285, Feb. 2019.

[5] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4661-4676, May 2014.

[6] R. K. Raman and L. R. Varshney, “Distributed storage meets secret sharing on the blockchain,” in *Proc. Inf. Theory Appl. Wkshop.* (ITA), Feb. 2018.

[7] R. K. Raman and L. R. Varshney, “Dynamic distributed storage for blockchains,” in *Proc. IEEE Int. Symp. Inf. Theory* (ISIT), pp. 2619-2623, Jun. 2018.

이 용 은 (Yong Eun Lee)

2005년 2월 : 숭실대학교 정보통신전자공학부 졸업 학사
2018년 8월 : 조선대학교 소프트웨어융합공학과 졸업 석사
2019년 3월~현재 : : 조선대학교 정보통신공학부 재학 박사
<관심분야> 사물인터넷, IoT 보안, 스마트팩토리 보안, 스마트시티 보안
[ORCID:0000-0003-4982-7554]

김 영 수 (Youngsoo Kim)

1998년 2월 : 성균관대학교 정보공학과 졸업 학사
2000년 2월 : 성균관대학교 컴퓨터공학부 공학석사
2009년 8월 : 성균관대학교 컴퓨터공학과 공학박사
2000년~현재 : 한국전자통신연구원 책임연구원
<관심분야> 5G보안, 네트워크보안, 디지털포렌식, 암호프로토콜

김 영 식 (Young-Sik Kim)

2001년 2월 : 서울대학교 전기공학부 졸업
2003년 2월 : 서울대학교 전기컴퓨터공학부 공학석사
2007년 2월 : 서울대학교 전기컴퓨터공학부 공학박사
2007년 3월~2010년 8월 : 삼성전자 책임연구원
2010년 9월~현재 : 조선대학교 정보통신공학과 교수
<관심분야> 포스트양자암호, 동형암호, 자동차보안, 스마트공장 보안, 정보이론, 오류정정부호, 하드웨어 보안
[ORCID:0000-0003-4114-4935]

서 창 호 (Changho Seo)

1990년 2월 : 고려대학교 수학과 졸업
1992년 2월 : 고려대학교 수학과 이학석사
1996년 2월 : 고려대학교 수학과 이학박사
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 융합과학과 교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보안, 시스템 보안 등
[ORCID:0000-0001-9680-8490]