IoT 네트워크에서 프라이버시 보호를 위한 동형암호화에 기반의 안전한 다자간 계산

진호천*, 김태우*, 박지수**, 박종혁*
*서울과학기술대학교 컴퓨터공학과
**전주대학교 컴퓨터공학과
*{chahot, tang_kim, jhpark1}@seoultech.ac.kr, **jisupark@jj.ac.kr

Secure Multi-Party Computation Based on Homomorphic Encryption for Privacy Preserving in IoT Networks

Hao-Tian CHEN*, Tae Woo Kim*, Ji Su Park**, Jong Hyuk Park*
*Dept. of Computer Science and Engineering, Seoul National University of Science and Technology
**Dept. of Computer Science and Engineering, Jeonju University

요 약

5G와 사물인터넷(IoT) 시대에 데이터의 크로스컴퓨팅은 연구, 의료, 금융, 민생 분야 등에 더 많은 지원을 할 수 있고 프라이버시 안전성이 중요해지고 있다. SMPC (Secure Multi-party Computation)은 서로 믿지 않는 참여자 간의 프라이버시 보호 시너지 컴퓨팅 문제를 해결하고, 데이터 수요자에게 원본 데이터를 누설하지 않는 범위 하에서의 다자간 컴퓨팅 능력을 제공한다. IoT 장치는 전력 소모와 지연에 제한을 받기 때문에 대부분의 장치가 여전히 경량화 보안 메커니즘에 속하고 IoT에서 트래픽의 데이터 통합관리가 어렵기 때문에 통신 중 신원인식과 데이터를 주고받는 단계에서 프라이버시 유출의 문제가 발생할 수 있고 심지어 DDOS공격, RelayAttack공격 등 사이버의 목적이 될 수도 있다. 본 논문에서 IoT 네트워크 데이터 통신 특징을 분석하고 동형 암호에 기반의 SMPC 연산 아키텍처를 제안한다. 제안하는 이키텍처에서 동형 암호를 사용함으로써 장치 데이터의 안전을 보장하는 동시에 전체 네트워크 안전성도 확보한다. SMPC 및 동형암호 기술의 지속적 발전에 따라 제안하는 아키텍처가 계속 개선할 잠재력이 있다.

1. 서론

2009년부터 '사물인터넷' '스마트시티'로 대표되는 정보화 개념이 세계적으로 등장하면서 통신 산업의 발전 방향을 제시하였고 현재 IoT에 대한 여러 가지 연구가 활발하게 진행되고 있다. 5G 시대에서 높은 대역폭 및 낮은 지연을 지원하고 있다. 보안 리스크가 점점 명확해지고 있고 개인 데이터에 대한 보호 요구가 더욱 엄격하게 된다 [1]. IoT 시스템이 수집한 데이터는 사용자의 많은 프라이버시 정보를 저장하는데 프라이버시와 안전은 IoT가 직면한 문제이다.

안전한 다자간 계산 (Secure Multi-party Computation (SMPC))은 암호화 원어의 일종이고 각 분포가 공동으로 임의의 기능을 같이 계산할 수 있도록 허용하며, 그들 자신의 개인 입력과 출력을 폭로하지 않다 [2]. 최근 몇 년간 클라우드 컴퓨팅, 모바일 컴퓨팅, 사물인터넷 등 새로운 기술이 보급되면서 SMPC의 인기가 다시 높아지고 있다. SMPC가 개인 데이터 컴퓨팅을 위한 범용 도구로 이들 분야의 보안과 프라이버시 문제를 해결하는 데 자연적인 이점을 가지고 있다.

본 논문에서 최근 연구되고 있는 IoT 통신 및 프라이버시 보안 동향에 대한 조사를 진행하고, 기존 연구를 바탕으로 IoT 네트워크에서 발생하는 전통적인 프라이버시 보안 문제에 대해 고찰한다. 고 IoT 통신 방식과 적합한 아키텍처를 제안하고 동형 암호 기반으로 SMPC를 구현하는 이론을 서술한다. 마지막으로 제안하는 아키텍처를 수학적인 이론 지지를 제공하고 지속적 발전 가능한 이점을 제시한다.

2. 관련연구

2.1. IoT 프라이버시 리스크

프라이버시가 IoT에서의 정의를 살펴보면 전통적인 네트워크 보안 절차부터 입수해야 한다. 네트

워크 정보보안은 요소별로 보면, 신분, 응용, 데이터를 포함하고 있으며 정보화시스템이 위치한 환경에서 신분·응용·데이터가 보장되는 네트워크 정보보안 체계의 핵심이며, 이 환경은 주로 단말기·인터넷·백그라운드 시스템을 포함한다 [3]. 현재 IoT 네트워크 정보보안체계 구축과정에서 일련의 방법론적 모델들이 종심방어체계, 생애주기 이론, WPDRCC 모델, 공방중심의 이론 등 보장체계를 뒷받침하고 있다.

IoT 보안 계층	
응용 계층	구체적인 기능을 제공하는 과정
전송 계층	네트워크에 데이터를 주고받는 과정
인식 계층	IoT 장치가 네트워크에 가입하기 위한 신분 인식하는 과정

<표 1> IoT 보안 계층 [4]

표1과 같이 데이터 정보의 유출은 주로 인식계층과 네트워크계층에서 일어나는데, 인식계층이 데이터를 수집하는 단계에서 가장 쉽게 데이터가 유출되고, 네트워크 계층에서도 데이터 전송 과정에서 유출될 위험이 있다 [4]. 인식계층은 주로 데이터의 조회·통합·전송을 하기 때문에 무선 센싱 (sensing) 네트워크와 주파수 인식 기술로 두 가지가 인식계층의 프라이버시 데이터 보안 위험이 된다.

2.2. 안전한 다자간 계산 (SMPC)

안전한 다자간 계산 (Secure Multi-party Computation, SMPC)은 서로 신뢰 여부를 불문하고 함수 $f(x_1, x_2, \ldots, x_n) = y(y_1, y_2, \ldots, y_n)$을 n명인 참여자가 같이 계산해 보고 함수의 n개 입력은 n개의 참여자가 각자 소지한다. 계산한 결과를 보면 계산 과정에서 부실한 참여자가 있어도 임의 참여자 P_i가 x_i의 입력에서 항상 y_i를 얻을 수 있다. 계산 참여자 P_i가 x_i 및 y_i 외에 모든 정보를 얻을 수 없고 y_i가 P_i에게 x_i에 기반한 소용이 있고 얻고 싶은 결과값이다. 즉 SMPC의 두 가지 주요 속성은 정확성과 사유이다. 정확성은 알고리즘에서 출력한 결과가 예상과 똑같이 나와야 한다는 것이고 사유는 임의 참여자의 비밀 입력 x_i가 절대 노출되지 않다는 것이다.

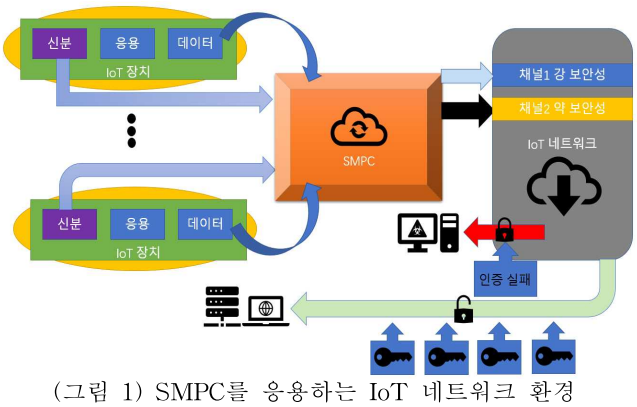
David 등은 키부터 데이터베이스까지 SMPC를 기반한 실제 어플리케이션 (Real-World Applications)에 대한 조사하였다 [5]. 실제 어플리케이션에서 3가지의 작용 영역을 나눠볼 수 있다. 첫째는 전통적인 데이터베이스 프로그램이 Sharemind 및 Jana 등이고, 둘째는 전형적인 키 관리 프로그램 Sepior와 Unbound 제품 등이고, 셋째는 구체적인 대표 예제 등이다. 즉 현실적으로 SMPC를 어플리케이션 단위로 동작하자고 하면 이런 3개의 방면에 입수해야 한다.

Kang 등은 갱신 한계치를 설정함으로써 데이터 갱신 후의 민감도를 다시 계산하여 프라이버시 예산의 손실을 감소시킨다. 후면함수 처리 소음 결과집추가, 데이터 가용성 향상시킨다는 연구 결과를 제시하였다 [6]. 실제 생활에서는 대부분의 사무 데이터 집합이 동적이며, 동적 데이터는 사무의 변화 과정을 더 잘 반영한다. 예를 들면 로그 데이터, 일일 판매 데이터 등 동적 데이터는 정적 데이터보다 연구 가치가 있다. 동적 데이터 방송은 실효성과 프라이버시 유출에 따른 여러 문제로 제약되어 왔다. 그리고 정적 환경에서의 프라이버시 보호 프레임은 동적 데이터에도 그대로 적용되지 않는다. 즉 프로그램을 개발할 때에 데이터 자신의 성질에 대해서 분류하여 처리하는 필요가 있다.

3. SMPC 기반 IoT 아키텍처

3.1. 기본 구조

본 논문에서 SMPC를 활용하는 IoT 네트워크를 제안한다. 그림1과 같게 IoT 네트워크에서 데이터 유형을 크게 2가지로 나눠볼 수 있다. 하나는 신분 정보 등인 정적 데이터이고 또 하나는 데이터 통신에 구체적인 기능을 실현하기 위해 동적 데이터이다.

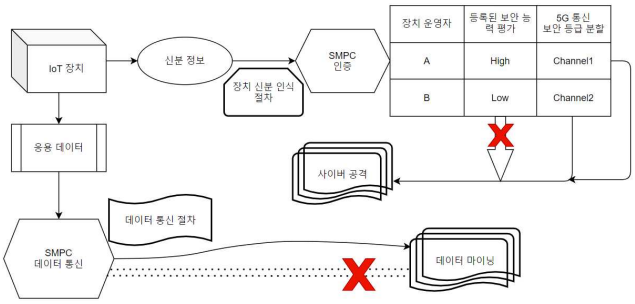


(그림 1) SMPC를 응용하는 IoT 네트워크 환경

정적 데이터가 통신 절차에서 상대적 변경 회수 및 데이터 수정 량이 적다. SMPC에 기반하는 인증 단계에서 해당 IoT의 장치의 운영 회사 등 법적 등록 정보를 얻고 장치의 유형 및 보안성능을 조회할

수 있다. 입력 단계에서 해당 장치만 자체의 정보를 가지고 있어 IoT 인식계층에서 프라이버스 정보를 노출하는 경우를 피할 수 있다. 장치의 보안 정보를 얻은 후에 성능에 따라서 5G 네트워크에서 등급을 나눠서 적당한 보안 통신 절차를 붙여 있으면 더욱 좋은 안전성을 제공할 수 있다.

동적 데이터는 항상 단말 간에 주고받아야 하니까 수학적인 연산이 상대적 더욱 많다. 그래도 프라이버시에 관한 민감한 정보를 객체 단위로 가지고 있어 필요한 정보만 SMPC를 이용하여 통신한다. 그러면 해당 통신의 기밀성을 유지할 수 있고 외부에 직접 간섭할 수 있는 공격 행위도 줄일 수밖에 없다.



(그림 2) SMPC 신분-데이터 통신 분할 처리

그림2와 같게 IoT 장치의 신분 인증은 5G 하의 높은 전송속력 기준 하에서 통신 성능을 조금 희생하고 먼저 수많은 IoT 장치의 운영 회사 등 공인 정보를 통해서 장치의 기존 보안성능을 조회한다. 조회과정도 SMPC를 사용하여 장치 자체가 정보를 판단한 후에 보안성을 고려하여 5G 다중 보안 채널로 나눠서 데이터 통신 채널을 요청한다. 그러면 장치가 소질이 부족해도 네트워크 특성으로 부분적으로 보완할 수 있다. 그리고 실제 응용 데이터를 통신할 때 프라이버시를 SMPC를 분할하여 계산하고 서로 암호문을 메시지를 교환하면 공격자가 부분적인 정보를 얻어도 동형암호 특성에 결과적으로 데이터 무결성을 보장할 수 있다. 뿐만 아니라 실제 네트워크에서 통신 중인 가치가 있는 데이터 량이 적어서 빅데이터 기반의 데이터 마이닝에 기반의 프라이버시 노출 문제도 저항력을 가져서 부분적 해결할 수 있다.

5G 시대의 고속 및 저 지연의 환경에서 IoT 경량화 장치가 인증, 데이터 통신도 시간이 무척 짧아서 데이터 노출이 쉽다. 그래서 네트워크 환경에서 부분적 노출해도 무방한 네트워크 생태를 구축할 수 있으면 네트워크 전체적인 보안성 및 안정성을 다 강화할 수 있고 개인 정보 및 장치 프라이버시를 다 보장할 수 있다. 그리고 SMPC가 동형 암호로 구현하게 되면 추후 동형 암호에 관한 연구 촉진에 따라서 SMPC 자체도 보안 능력 및 처리 속도 등 다방면에서 지속 최적화가 가능하게 된다. 심지어 수학적 분야에서 다른 암호화 가능한 이론 지식이 나타나면 암호화 알고리즘에 대해서도 변경 및 수정이 가능하다. 즉 SMPC에게 지속적인 성장할 수 있는 잠재력이 존재한다는 것을 설명할 수 있다.

3.2. 동형암호 기반 SMPC 알고리즘

덧셈과 동형을 갖춘 문한 암호 체제는 SMPC 협의를 구성하는 기본 도구이다. 동형암호의 매개변수는 표2에서 확인 가능하다.

매개변수	부호 표시
비밀키	Ks
명문	M
암호문	C
암호화 알고리즘	E
복호화 알고리즘	D
공개키	Kp

<표 2> 계산 과정 중의 매개변수

본 논문에서 구현하려고 하는 동형암호문은 Paillier 암호에 기반한 것이다. 임의의 입력 m1, m2 ∈ M, E(m1)*E(m2)=E(m1+m2)가 있어 한계치(t,n)은 n개 참가자 중 최소한 t개인이 연합해야 복호화 가능하여 명문을 풀 수 있다는 것이다. 네트워크 환경에서 공개키 Kp를 공유하고, 비밀키 Ks를 Shamir(t,n)에 따라서 공유해야 한다. 계산 과정은 다음과 같다.

단계1. 입력 단계: 모든 참여자 $P_i(1 \le i \le n)$가 $E_{Ks_i}(x_i) = C_i$에 따라서 암호화된 메시지를 얻고 나서 네트워크에 공유한다.

단계2. 계산 단계: 함수 f가 어떤 치역에서 K의 다항식을 가지고 있다고 가정한다.

$$E(x+y) = E(x) \times E(y),\ x, y \in K \quad \text{... (식 1)}$$

"x+y"에 대한 계산은 동형암호 덧셈의 특징에 따라 참여자가 서로 데이터를 교환하는 필요없고

E(x)*E(y)를 통해서 E(x+y)를 얻을 수 있다.

"x*y"에 대한 계산은 모든 참여자 $P_i(1 \le i \le n)$가 각자 임의로 하나의 무작위 수 $d_i \in$M를 고르고 E(d_i)를 공개한다. 그 때에 모든 참여자가 식(2)와 같게 암호문 c′을 얻는다. 서로 연합하여 c′를 식(3)과 같게 사전 공유한 공개키 Kp로 복호화하면 d를 얻을 수 있다. P_i가 식(3)(4)(5)에 따라 하면 식(5)과 같은 결과가 나온다. 그 후에 모든 참여자가 각자 $E(a_i y)$를 얻고 서로 공유하면 프라이버시에 관한 정보 계산이 완성된다.

$$c' = E(x + d1 + \ldots + dn) \quad \ldots (식\ 2)$$

$$d = d1 + \ldots + dn + x \quad \ldots (식\ 3)$$

$$a_1 = d - d1,\ a_i = -d_i, 2 \le i \le n \quad \ldots (식\ 4)$$

$$x = \sum_{i=1}^{n} a_i \quad \ldots (식\ 5)$$

암호문 공간이 대응하는 연산 법칙은 곱셈이면 $E(a_i y) = E(y)^{a_i}$라는 공식이 존재한다. 그러면 식(6)과 같은 계산 방법을 사용하여 E(x*y)의 계산 방법을 얻을 수 있다.

$$E(\sum_{i=1}^{n} a_i y) = E(xy) \quad \ldots (식\ 6)$$

-단계3: 출력 단계

마지막까지 모든 참가자가 마지막 함수 값인 암호화 결과 $E(f(x_1, \ldots, x_n))$를 받았기 때문에 마지막 함수 값을 복호화하면 서로 프라이버시 유출하지 않는 동시에 필요한 연산 결과를 얻을 수 있다.

SMPC의 참여자 P_i가 IoT의 장치라서 데이터 처리량이 상대적 부족해서 성능도 고려해야 한다. 그래서 식(6)과 같은 다항식 연산은 현대 일반 컴퓨팅 처리할 수 있는 기준으로 설계하기 필요하다.

5. 결론 및 고찰

5G 시대에서 IoT 프라이버시가 고속 통신 환경에서 쉽게 정보 노출이 되어서 큰 리스크가 직면하고 있다. 본 논문에서 기존 IoT 통신 구조에서 정보 유형에 따라서 데이터를 분할하여 여러 가지 종류의 데이터를 동형암호로 실현하는 SMPC 구조를 제안한다. 통신 절차에서 데이터 교환이 적고 데이터 마이닝에 대한 저항력도 있으면서 IoT 장치의 성능에 따라 보안 등급을 할당하여 5G 보안 통신 배정하여 전체 네트워크 안전성을 유지하는 동시에 프라이버시를 보호하는 목적을 달성한다. 그리고 SMPC를 기반한 IoT 구조가 암호학 기술에 기반한 것이라서 암호학 발전에 따라서 SMPC의 성능 및 확장성도 좋고 앞으로 더 깊은 연구를 가이드라인을 제시한다.

향후 본 아키텍처에서의 개선할 수 있는 점을 간략히 살펴보면 동형암호 알고리즘에 최적화하거나, SMPC 차원에서 IoT 구조에 대한 적합한 특성을 재설계할 것이다. IoT 영역 및 암호학의 관련 기술의 발전에 따라서 지속적 발전하는 잠재력이 있다.

Acknologyment

이 연구는 강원테크노파크가 후원하는 양자정보기술 동향 조사 및 분석 및 지역전략 수립 연구용역 사업의 지원으로 수행되었습니다.

참고문헌

[1] J. S. Park and J. H. Park, "Future Trends of IoT, 5G Mobile Networks, and AI: Challenges, Opportunities, and Solutions," JIPS, vol. 16, no. 4, pp. 743-749. (2020).

[2] Salim, M. M., Shanmuganathan, V., Loia, V., & Park, J. H., "Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks.", HCIS, (2021).

[3] Liu Zhicheng, "A new theory on the construction of Internet of Things Network information security ecosystem." Cyberspace Security vol. 9, pp. 12, (2020).

[4] Wu hongying, "Research on privacy data security for Internet of Things." Wireless Internet Technology, vol. 17, No. 8, pp. 21-22. (2020).

[5] Archer, David W., et al. "From keys to databases－real-world applications of secure multi-party computation." The Computer Journal Vol. 61, No. 12, pp. 1749-1771. (2018)

[6] Kang HY, and Ma YL., "A review of the application of differential Privacy Protection in Data Mining." Journal of Shandong University (Natural Science) Vol. 52, No. 3, pp. 16-23. (2017)