동형암호 기반의 블록체인을 통한 프라이버시 보호 기법 동향

강예준*, 김현지*, 김원웅*, 임세진*, 서화정*†
* 한성대학교 대학원 IT융합공학부

요 약

● 최근 빅 데이터를 활용한 연구가 다수 진행되면서 데이터 프라이버시 보호 문제 대두되고 있다. 이에 대한 대응책으로 각 분야에서 다양한 기술들이 개발되고 있고 블록체인에서는 동형암호 기반의 블록체인을 통한 프라이버시 보호 기법이 제안되고 있다. 엣지 컴퓨팅, 병렬 블록체인과 같이 다양한 환경에서의 동형암호 기반의 블록체인 기술들이 개발되고 있으며, 이 외에도 스마트 그리드를 위한 블록체인 등과 같이 동형암호 기술이 적용된 다양한 블록체인 애플리케이션들이 연구되고 있다. 현재 수행된 대부분의 연구들은 데이터 집계 (블록체인 지갑의 잔액, IoT 기기로 부터 수집한 데이터 등)를 위해 Paillier 동형암호를 적용하였다. 이를 통해 프라이버시를 보호할 수 있음을 보였다.

관련 연구

● 블록체인

블록체인이란 네트워크 내의 참여자들이 peer-to peer 방식으로 모두 같은 원장을 공유 하는 데이터 분산 처리 기술을 말한다[1]. 중앙 서버가 장부를 관리하는 기존 방식에서 벗어나, 암호화된 전자 장부를 네트워크 내의 참여자와 모두 공유함으로써 탈중앙화가 실현된다. 따라서 블록체인 네트워크 상에서는 제 3자인 중앙서버가 존재하지 않으며, 데이터를 위조하기 위해 서는 중앙 서버를 해킹하는 것이 아닌 과반수 이 상의 네트워크 참여자가 가지고 있는 원장을 위조해야한다. 이는 사실상 불가능하기 때문에, 데이터를 조작할 수 없으며 무결성을 보장한다. 블록체인은 네트워크에 누구나 참여할 수 있는 퍼블릭 블록체인과 서비스 제공자의 허가를 받아야만 네트워크에 참여할 수 있는 프라이빗 블록체인이 있다.

● 동형 암호

동형암호란 평문과 암호문의 동일한 성질로 인해 평문에 대한 연산 결과와 암호문에 대한 연산 결과가 같은 값을 가지는 암호화 방식이다[2]. 동형암호는 정보의 노출 없이 암호화된 데이터를 제 3자가 연산을 수행할 수 있다는 점에서 민감 데이터를 유용하게 활용할 수 있다. 이러한 특징으로 인해 클라우드 환경에서 민감 데이터를 노출시키지 않고 클라우드 회사에 위탁할 수 있다. 또한 여러 데이터가 결합되는 기계학습을 수행할 시 동형암호는 매우 유용하게 사용할 수 있다. 현재 동형암호 오픈소스 라이브러리는 IBM에서 개발한 HElib와 마이크로소프트에서 개발한 SEAL 등이 있으며, 국내에는 서울대학교에서 개발한 HEAAN이 있다.

동향

● A homomorphic encryption and privacy protection method based on blockchain and edge computing[3]

엣지 컴퓨팅과 완전 동형 암호 시스 템을 도입한 블록체인 기반의 분산형 개인정보 보호 아키텍처를 설계하였다. 블록체인의 운영 효율성을 보장하고 클라이언트의 컴퓨팅 부담을 완화시키기 위해 컴퓨팅, 저장 및 통신 능력이 있는 일부 엣지 노드가 데이터를 체인에 쓰고 전 체 블록체인을 유지하고 업데이트 한다. 에스크 로 상에서 발생할 수 있는 데이터 보안 문제를 해결하기 위해 Paillier 및 RSA 암호 시스템을 기반으로 한 블록체인 네트워크를 제시하였다. 해당 시스템에서는 엣지 노드들이 수신한 암호화 된 데이터에 대한 연산을 수행한다. 해당 데이터 는 동형암호를 통해 암호화 되어 있으므로 암호 화된 상태로 연산을 수행할 수 있다. 그 후 연산 결과를 클라이언트에게 반환한다. 이를 통해 개 인정보를 보호할 수 있고 익명성을 확보할 수 있 다. 하이퍼 레저 패브릭을 통해 구현하여 실험한 결과 1분에 120개의 블록이 생성될 수 있음을 확인하였다.

● Homomorphic encryption in 5ire blockchain.[4]

프라이버시를 보호하고 확장성 문제를 해결하기 위해 5ire BlockChain을 제안하였다. 5ire BlockChain에서는 확장성 문제를 해결하기 위해 병렬체인을 사용하였으며, 트랜잭션 정보가 유출되는 문제를 해결하기 위해 동형암호를 사용 하였다. 즉, 프라이버시를 보호하기 위해 동형암호를 사용하여 지갑의 잔액을 암호화하도록 함으로써 지갑 데이터에 대한 무결성 검사와 개인 정 보 보호가 가능한 블록체인 네트워크를 설계하였다. Paillier 동형암호 라이브러리를 사용하였고, 1KB 크기의 트랜잭션에 대해 512-bit 키를 통해 암호화할 경우 8070 milliseconds가 소요되었 고, 1024-bit 키를 통해 암호화할 경우에는 63062 milliseconds가 소요된다.

●Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption.[5]

IoT에서 생산된 데이터는 일반적으로 활용도가 높지만, 이를 활용할 경우 프라이버시 유출 문제가 있다. 일반적으로 IoT 데이터 집계 프로세스는 중앙 집중식 서버를 통해 이루어진다. 하지만 중앙 집중식 서버의 경우 제 3자가 방대한 양의 개인 데이터를 수집한다는 문제점이 있다. 또한 중앙 집중식이 아닌 분산화된 방식으로 데이터를 집계할 경우에는 신뢰할 수 없는 노드가 있을 경우 문제가 발생한다. 블록체인과 동형암호를 통해 이러한 문제를 해결한 PrivDA를 제안하였다. 해당 시스템은 프라이버시를 보호한 채로 IoT 데이터를 집계하는 기술 이다. 블록체인을 기반으로 하기 때문에 악의적 인 노드가 있더라도 데이터 집계가 용이하다. 또 한 동형암호를 통해 데이터를 집계하는 동안 원본 데이터를 공개하지 않고 암호화된 데이터를 통해 연산을 가능하게 하여 프라이버시를 보호할 수 있다.

결론

● 본 논문에서는 동형암호 기반의 블록체인 기술을 통한 데이터 프라이버시 보호 기법에 대해 살펴보았다. 엣지 컴퓨팅, 병렬 블록체인과 같이 다양한 환경에서의 동형암호 기반의 블록체인 기술이 연구되고 있다. 또한, 동형암호 기반의 딥 러닝과 블록체인을 활용한 스마트 그리드 시스템 [6]과 같이 애플리케이션에 관한 연구들도 진행되고 있다. 현재 수행된 대부분의 연구들은 데이 터 집계 (블록체인 지갑의 잔액, IoT 기기로부터 수집한 데이터 등)를 위해 동형암호를 적용하였다. 이를 통해, 원본 데이터가 공개되지 않도록 하여 데이터 프라이버시 보호가 가능하도록 할 수 있으며, 이를 위해 동형암호인 Paillier 라이브러리를 사용하였다. 앞으로 동형암호 기반의 블록체인을 활용함으로써 더욱 다양한 분야에서 블록체인이 활용될 수 있을 것으로 생각된다.

참고문헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.
[2] Acar, Abbas, et al. "A survey on homomorphic encryption schemes: Theory and implementation." ACM Computing Surveys (Csur) 51.4 (2018): 1-35.
[3] Yan, Xiaoyan, Qilin Wu, and Youming Sun. "A homomorphic encryption and privacy protection method based on blockchain and edge computing." Wireless Communications and Mobile Computing 2020 (2020).
[4] Mattila, Vilma, et al. "Homomorphic encryption in blockchain." International Social Sciences and Review 5 (2022). 5ire Journal of Man-agement
[5] Loukil, Faiza, et al. "Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption." Sensors 21.7 (2021): 2452.
[6] Singh, Parminder, et al. "Blockchain and homomorphic privacy-preserving data aggregation model in smart Electrical Engineering 93 (2021): 107209. encryption-based grid." Computers & Electrical Engineering 93 (2021): 107209.