

블록체인 기반 전자상거래 시스템에서의 개인정보보호 적용 방안

이진수¹, 김지혜², 이종혁³

¹세종대학교 정보보호학과 & 지능형드론 융합전공 석사과정

²세종대학교 정보보호학과 학부생

³세종대학교 정보보호학과 & 지능형드론 융합전공 교수

jinsue@pel.sejong.ac.kr, jihye@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

Privacy-preserving Approach in Blockchain-based e-Commerce Systems

Jinsue Lee¹, Jihye Kim², Jong-Hyouk Lee³

¹Dept. of Computer and Information Security &
Convergence Engineering for Intelligent Drone, Sejong University

²Dept. of Computer and Information Security, Sejong University

³Dept. of Computer and Information Security &
Convergence Engineering for Intelligent Drone, Sejong University

요 약

블록체인 기반 전자상거래 시스템은 탈중앙화된 P2P(Peer-to-Peer) 방식으로 데이터를 처리하고 합의 메커니즘을 통해 동기화되는 분산원장에 기록할 수 있다. 그러나, P2P 운영에 기반하여 전자상거래 과정에서 파생되는 고객의 외부 노출에 민감한 정보로 인해 고객의 개인정보가 공개되거나 유출되는 위험이 발생할 수 있다. 이에 따라, 본 논문에서는 블록체인 기반 전자상거래 시스템에서 고객의 개인정보를 보호하기 위한 PET(Privacy Enhancing Technology)를 식별하고, 블록체인 기반 전자상거래 시스템에 적용하기 위한 방안을 분석한다.

1. 서론

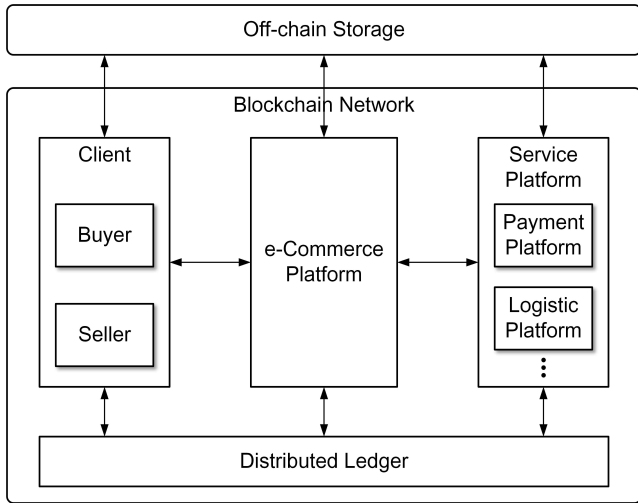
전자상거래(e-Commerce)는 거래 주체 및 형태에 따라 기업 간 거래, 기업과 고객(Client) 간 거래, 고객 간 거래 유형으로 구분된다. 이러한 거래 유형 가운데 고객은 구매자(Buyer)와 판매자(Seller)로 구성될 수 있다. 구매자는 온라인으로 제품 혹은 서비스를 구매하고 이용할 수 있으며, 판매자는 다양한 경로를 통해 제품 혹은 서비스를 판매할 수 있다. 그러나, 전자상거래에서는 데이터 관리, 계좌 및 금액 변조, 신뢰할 수 있는 제3자(TTP, Trusted Third Party)의 부재로 인한 보안 위협 등의 잠재적인 위협이 발생할 수 있다. 특히, 전자상거래 운영자가 고객에게 개인화된 서비스를 제공하기 위해 개인정보를 수집하는 과정에서 개인정보보호 침해 사례가 발생할 수 있다[1].

중앙화된 전자상거래에서는 이러한 보안 위협에 대응하기 위해 블록체인을 활용하기 위한 노력이 이어지고 있다. 블록체인 기반 전자상거래는 P2P(Peer-to-Peer) 방식의 탈중앙화된 데이터 처리와 암호화 기술을 사용하여 보안성을 확보하고, 분산원장에 기록된 데이터의 위조 및 변조가 어려운 특성에 따라,

데이터에 대한 투명성과 무결성을 보장할 수 있다[2]. 그럼에도 불구하고, 블록체인 기반 전자상거래 플랫폼(e-Commerce Platform)의 거래, 판매자 평점 분석, 결제 및 운송 등의 과정에서 파생되는 다양한 유형의 고객 개인정보 침해 사례가 발생할 수 있다. 이에 따라, 본 논문에서는 블록체인 기반 전자상거래에서의 개인정보보호 위협을 완화하기 위한 PET(Privacy Enhancing Technology) 적용 방안에 대해 분석한다.

2. 블록체인 기반 전자상거래 시스템

블록체인 기반 전자상거래 시스템은 프라이빗 블록체인을 기반으로 고객의 물품 판매 및 등록, 판매자 평점 분석, 전자 마케팅, 거래 정보 처리 등의 서비스를 제공한다. 서비스 플랫폼(Service Platform)은 결제 플랫폼(Payment Platform), 물류 운송 플랫폼(Logistic Platform) 등으로 구성될 수 있으며, 해당 서비스 플랫폼을 통해 전자상거래 플랫폼은 원활한 전자상거래 서비스를 지원할 수 있다.



(그림 1) 블록체인 기반 전자상거래 시스템

블록체인 기반 전자상거래 시스템에서는 고객 거래 정보의 신뢰성과 무결성을 보장하기 위해 거래 내역을 분산 저장하고 체인 구조로 연결한다. 또한, 대용량의 데이터를 원활히 처리하기 위해 블록체인 네트워크 외부에서 동작하는 오프체인 저장소(Off-chain Storage) 형태의 IPFS(InterPlanetary File System)가 적용될 수 있으며, 권한을 가진 시스템 사용자에게 한해 저장된 데이터에 접근하고 분석할 수 있다.

3. 블록체인 기반 전자상거래 시스템에서의 개인정보보호 위협 요인 및 PET 적용 방안

전자상거래 플랫폼 및 서비스 플랫폼에서 고객의 거래 정보를 관리하는 과정 가운데 거래 정보, 소비 성향, 소비 특성, 생활 패턴 등의 개인정보가 파생될 수 있음에 따라, 고객의 개인정보가 노출될 가능성이 존재하며 이를 완화하기 위한 방안이 요구된다.

이러한 개인정보 위협을 완화하기 위한 PET로 동형암호(Homomorphic Encryption)와 SMPC(Secure Multi Party Computation)의 적용을 고려할 수 있다. 동형암호는 암호화된 데이터를 복호화하지 않고 연산 및 분석을 가능하게 할 수 있다. 이는 전자상거래 플랫폼과 서비스 플랫폼 간의 고객 개인정보를 제공하거나 분석하는 과정에서 암호화된 값 간의 계산을 수행하여 잠재적 개인정보 침해 발생 구간을 최소화함에 따라 고객 개인정보보호를 강화할 수 있다.

또한, 동형암호를 통해 암호화된 데이터로 개인정보 노출 없이 다양한 연산을 가능하게 하는 블록체인 기반 전자상거래 플랫폼에서는 SMPC를 동형암호와 결합하는 것을 고려할 수 있다. SMPC는 왜곡 회로(garbled circuits), 비밀 공유(secret sharing) 등의 기법을 기반

으로 둘 이상의 여러 조직이 민감한 데이터를 공유하지 않고 공동 분석을 수행할 수 있다. 이를 통해, 무작위로 데이터를 암호화하고, 양 측이 공유한 데이터의 일부분을 재결합하여 의도한 통계 결과를 획득할 수 있음에 따라, 고객의 결제 정보, 물류 운송 정보 등과 같은 개인정보를 외부에 노출하지 않고 분석할 수 있다.

따라서, 블록체인 기반 전자상거래 시스템에서는 전자상거래 플랫폼 운영자가 동형암호와 SMPC를 활용하여 고객의 거래 정보, 소비 성향과 같은 고객 개인정보를 보호할 수 있다. 전자상거래 플랫폼 운영자는 서비스 품질 개선을 위해 고객 개인정보를 제3자에게 안전한 방법으로 제공하고, 외부 기관과의 공동 분석을 수행하는 상황에서 고객의 개인정보를 보호할 수 있는 장점이 존재한다.

4. 결론

본 논문에서는 블록체인 기반 전자상거래 시스템을 나타내고, 해당 시스템에서 발생할 수 있는 고객의 개인정보 위협 지점을 식별하였다. PET는 고객의 개인정보보호를 강화하고 외부 유출을 최소화할 수 있는 장점을 가지며, 고객의 개인정보가 여러 플랫폼에서 다루어지는 지점에 적용될 수 있다. 향후 연구에서는 본 논문을 바탕으로 블록체인 기반 전자상거래 플랫폼에 대한 동형암호, SMPC와 같은 PET 기술을 적용한 블록체인 기반 전자상거래 시스템을 설계 및 개발하고자 한다.

Acknowledgement

이 논문은 2024년도 정부(개인정보보호위원회)의 재원으로 한국인터넷진흥원의 지원을 받아 수행된 연구임 (No.1781000011, 블록체인 환경에서의 개인정보보호 표준개발). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신방송혁신인재양성(메타버스융합대학원)사업 연구 결과로 수행되었음 (IITP-2023-RS-2023-00254529).

참고문헌

- [1] H. Taherdoost, M. Madanchian, "Blockchain-Based E-Commerce: A Review on Applications and Challenges", *Electronics*, vol. 12, no. 8, pp. 1889, 2023.
- [2] J. Jiang, J. Chen, "Framework of Blockchain-supported E-Commerce Platform for Small and Medium Enterprises", *Sustainability*, vol. 13, no. 15, pp. 8158, 2021.