자금세탁방지(AML) 모델 학습을 위한 SMPC와 연합학습의 활용 방안

하유성, 김기천*

건국대학교

everna12@konkuk.ac.kr, *kckim@konkuk.ac.kr

Training Anti-Money Laundering(AML) Models Using SMPC and Federated Learning

Ha Yu Seong, Kim Kee Cheon*

Konkuk Univ.

요 약

본 논문은 자금세탁방지(AML) 모델 학습을 위해 보안 다자간 연산(SMPC)과 연합학습(Federated Learning)을 결합하는 새로운 접근법을 제안한다. 이 방법은 금융 기관 간 민감한 데이터를 공유하지 않으면서도 공동의 머신러닝 모델을 학습할 수 있게 하여 데이터 프라이버시를 보호하고 자금세탁 탐지의 효율성을 높인다. SMPC와 연합학습의 결합은 국제적인 프라이버시 규제를 준수하며 금융 기관 간 협업을 강화한다. 본 연구는 이러한 접근법의 효과와 실질적인 적용 가능성을 탐구하며, 글로벌 금융 환경에서 보다 정교한 자금세탁 방지 시스템 구축에 기여할 수 있을 것으로 기대된다.

Ⅰ. 서 론

글로벌 금융 시스템은 자금세탁과 테러 자금조달과 같은 불법적인 금융 활동에 지속적으로 노출되어 있다[1]. 이러한 위협은 금융 기관뿐만 아니라 국가 경제 전반에 부정적인 영향을 미치며, 효과적인 자금세탁방지(AML) 시스템 구축의 필요성이 증가하고 있다. 그러나 기존의 AML 시스템은 데이터 공유의 제한성과 프라이버시 우려로 인해 한계를 보이고 있으며, 특히 금융 기관 간 협업의 부족은 자금세탁 패턴의 복잡성과 국제적 확산을 고려할 때 큰 문제로 작용한다[2].

이 문제를 해결하기 위해 보안 다자간 연산(Secure Multi-Party Computation, SMPC)과 연합학습(Federated Learning)의 통합이 주목받고 있다[3]. SMPC는 참여자 간 민감한 데이터를 노출하지 않고도 공동 연산을 수행할 수 있게 하고, 연합학습은 로컬 데이터를 중앙 서버로 전송하지 않고도 글로벌 머신러닝 모델을 학습할 수 있는 기술이다. 두 기술의 결합은 데이터 프라이버시에 대한 우려를 해소하면서 금융 기관 간 협업을 촉진하여 더 강력한 AML 시스템 구축을 가능하게 한다[4].

본 논문에서는 이러한 SMPC와 연합학습을 활용한 새로운 AML 모델 학습 방안을 제시한다. 이 접근법은 금융 기관들이 민감한 데이터를 공유하지 않고도 공동의 AML 모델을 구축할 수 있게 하여, 데이터 프라이버시를 보호하면서도 협업을 강화한다. 이를 통해 자금세탁 탐지의 효율성을 높이고, 국제적인 프라이버시 규제에도 부합하는 솔루션을 제공한다[5]. 또한, 제안하는 방법이 AML 분야에서 특히 유용한 이유와 그 기대 효과를 분석하여 자금세탁 방지의 효과성을 향상시킬 수 있는 방안을 제시한다.

Ⅱ. 본론

기존의 자금세탁방지(AML) 시스템은 각 금융 기관들이 독립적으로 데이터를 수집하고 분석하여 자금세탁 활동을 탐지하는 방식으로 운영된다. 이러한 접근 방식은 데이터 공유의 제한성과 금융 기관 간 협업의 부재로 인해 국제적이고 복잡한 자금세탁 패턴을 효과적으로 탐지하는 데 한계가 있다[6]. 특히, 각 금융 기관이 개별적으로 데이터를 관리하기 때문에 자금세탁 활동의 전체적인 흐름을 파악하는 데 어려움을 겪으며, 데이터 프라이버시와 보안에 대한 우려는 금융 기관 간의 데이터 공유를 더욱 어렵게 만든다.

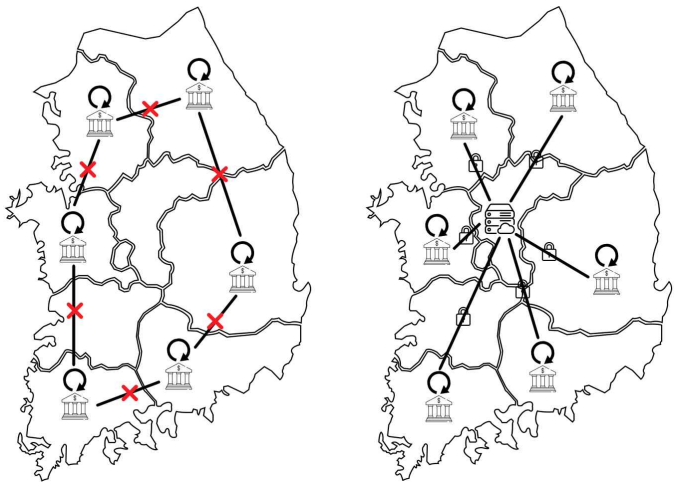

그림 1. 기존 AML 시스템과 제안하는 시스템의 비교

그림 1에서 볼 수 있듯이, 기존의 AML 시스템에서는 각 금융 기관이 개별적으로 자금세탁 의심 활동을 탐지하고, 다른 기관과의 협력 없이 분석을 수행한다. 이러한 방식은 기관 간 정보의 단절을 초래하며, 자금세탁이 여러 국가와 금융 기관에 걸쳐 이루어지는 경우 그 탐지가 매우 어렵다. 이러한 문제를 해결하기 위해, 본 연구에서는 보안 다자간 연산(Secure Multi-Party Computation, SMPC)과 연합학습(Federated Learning)을 결합한 새로운 접근법을 제안한다.

보안 다자간 연산은 여러 참여자가 자신의 데이터를 노출하지 않고도 공동 연산을 수행할 수 있는 기술이다. 이를 통해 금융 기관들은 각자의 민감한 데이터를 보호하면서도 협력하여 필요한 계산을 수행할 수 있다. 예를 들어, 각 금융 기관은 자체적으로 수집한 데이터를 활용하여 연산을 수행하고, 그 결과를 암호화된 형태로 다른 기관들과 공유함으로써 자금세탁 의심 패턴을 보다 효과적으로 분석할 수 있다. 이는 기존 시스템에서의 데이터 공유 문제를 해결할 수 있는 중요한 기술적 장점이다.

연합학습은 중앙 서버에 데이터를 모으지 않고, 각 참여 기관에서 로컬로 머신러닝 모델을 학습하고 그 업데이트만을 중앙 서버로 전송하여 글

로벌 모델을 구축하는 방식이다. 이러한 접근법은 데이터가 각 금융 기관의 로컬 서버에 머물러 있기 때문에 데이터 유출 위험을 줄일 수 있으며, 금융 기관 간의 협업을 통해 보다 정교한 자금세탁 탐지 모델을 개발할 수 있다.

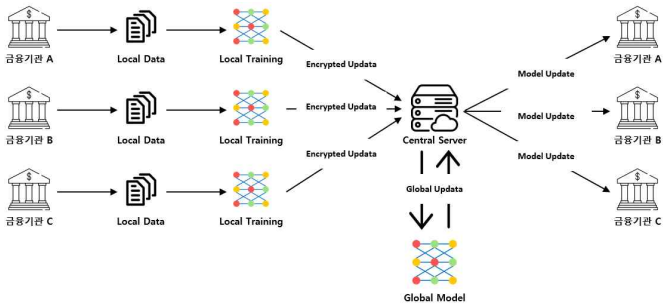

그림 2. 제안하는 AML 모델 학습 방안의 전체적인 아키텍처

그림 2에서 제시한 바와 같이, 각 금융 기관은 로컬 데이터를 이용해 모델을 학습하고, 중앙 서버는 이를 통합하여 글로벌 모델을 업데이트한다. 이 과정에서 각 기관의 데이터는 노출되지 않으며, 암호화된 업데이트만이 공유된다.

SMPC와 연합학습의 결합은 금융 기관 간의 협업을 강화하면서도 데이터 프라이버시를 보호할 수 있는 강력한 솔루션을 제공한다. 제안된 모델은 기존의 AML 시스템의 한계를 극복하고, 국제적이고 복잡한 자금세탁 패턴을 보다 정확하게 탐지할 수 있게 한다. 특히, 각국의 프라이버시 규제에 부합하기 때문에 글로벌 금융 환경에서도 적용 가능성이 높다. 그림 2(제안하는 AML 모델 학습 방안의 전체적인 아키텍처)에서 제시된 아키텍처는 이러한 접근법의 전체적인 흐름을 시각적으로 보여주며, 각 금융 기관이 민감한 데이터를 중앙 서버로 전송하지 않고도 공동의 목표를 달성할 수 있음을 나타낸다.

이러한 기술적 통합은 금융 기관들이 서로 협력하여 자금세탁 탐지의 효율성을 높이고, 데이터 프라이버시를 보장하며, 국제적인 규제 준수를 가능하게 한다. 본 연구에서 제안하는 새로운 AML 모델 학습 방안은 금융 기관 간의 신뢰를 기반으로 하며, 자금세탁 탐지의 정확성을 크게 향상할 것으로 기대된다.

Ⅲ. 결론

본 논문에서는 자금세탁방지(AML) 모델 학습을 위해 보안 다자간 연산(SMPC)과 연합학습(Federated Learning)을 결합한 새로운 방안을 제시하였다. 기존의 AML 시스템이 데이터 공유의 제한성과 프라이버시 우려로 인해 한계를 보였던 반면, 제안된 접근법은 민감한 데이터를 공유하지 않고도 금융 기관 간의 협업을 가능하게 하여 보다 정교하고 효과적인 자금세탁 탐지가 가능하게 한다. 특히, SMPC와 연합학습의 결합을 통해 국제적이고 복잡한 자금세탁 패턴을 효과적으로 탐지하며, 각국의 프라이버시 규제를 준수하면서도 AML 시스템의 효율성과 신뢰성을 향상시킬 수 있다.

본 연구는 자금세탁방지 분야에서 기술적 한계를 극복하고 금융 기관 간 협업을 통해 보다 안전하고 강력한 AML 모델 구축에 기여할 것으로 기대된다. 향후 연구에서는 제안한 방법의 실제 적용 가능성을 검증하기 위한 시뮬레이션 및 실험적 분석이 필요하며, 이를 통해 금융 산업 전반의 자금세탁 방지 역량을 한층 강화할 수 있을 것이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학·석사연계ICT핵심인재양성 지원을 받아 수행된 연구임(IITP-2024-RS-2020-II201834)

참 고 문 헌

[1] Yousufi, Zmarialy, and P. N. Harikumar. "An Overview of Anti-Money Laundering Practice in the Indian Financial System." i-Manager's Journal on Economics & Commerce 3.3 (2023): 33.

[2] Monye, Ogochukwu, and Louis De Koker. "Strengthening financial integrity in Nigeria: the national identification harmonization project." Journal of Financial Crime 29.4 (2022): 1137-1154.

[3] Geng, Tieming, Jian Liu, and Chin-Tser Huang. "A Privacy-Preserving Federated Learning Framework for IoT Environment Based on Secure Multi-party Computation." 2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT). IEEE, 2024.

[4] Ahmed, Ahmed Abdelmoamen, and Oluwayemisi Alabi. "Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review." IEEE Access (2024).

[5] Reite, Endre Jo, Johan Karlsen, and Elias Grefstad Westgaard. "Improving client risk classification with machine learning to increase anti-money laundering detection efficiency." Journal of Money Laundering Control (2024).

[6] Huong, Huu, et al. "Money Laundering Detection Using A Transaction-Based Graph Learning Approach." 2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM). IEEE, 2024.