Secure Aggregation with Federated Learning

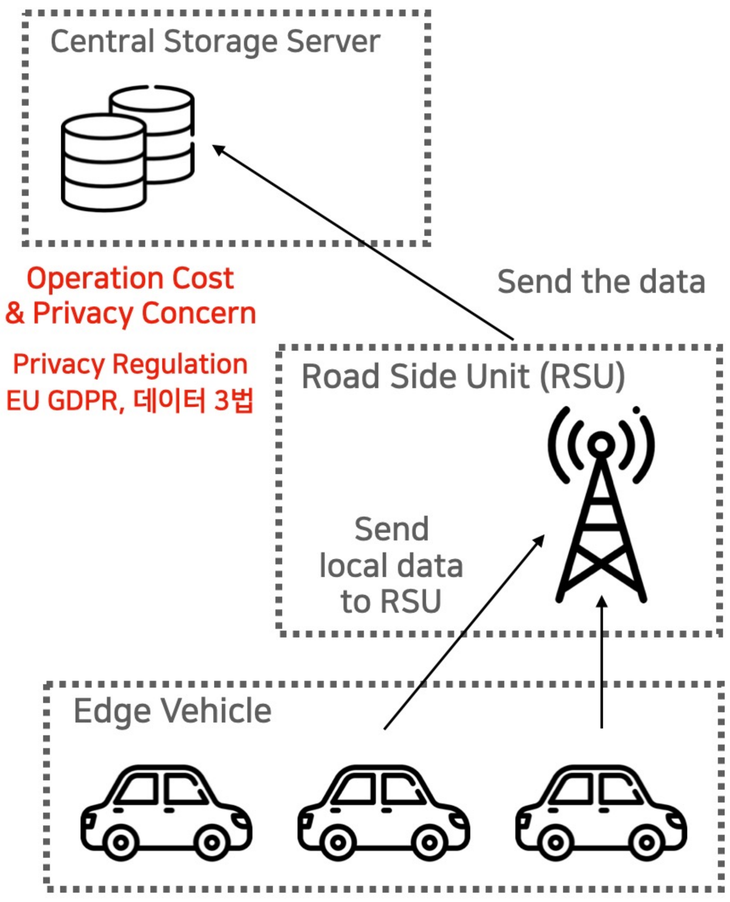
이 름 최지헌 지도교수 오상윤

연구배경

사물 인터넷 기술의 발전으로 방대한 양의 시계열 데이터 관리의 중요성이 커지고 있으며, 자율주행 차량의 주행으로 생성되는 다양한 종류의 센서 데이터 처리를 위한 분산 아키텍처 설계 필요

기존 연구에서는 '분산 딥러닝'을 활용하여 대규모 모델 혹은 데이터를 처리하였지만, 이러한 방법은 중앙 저장소 운영 비용과 민감 개인정보 수집의 문제 해결에 어려움

이를 해결하기 위해 구글에서 처음 제안한 연합 학습[1]을 구현하고 실제로 자율주행 산업에 적용하기 위해 발생 가능한 문제 정의 목표



제안 시스템

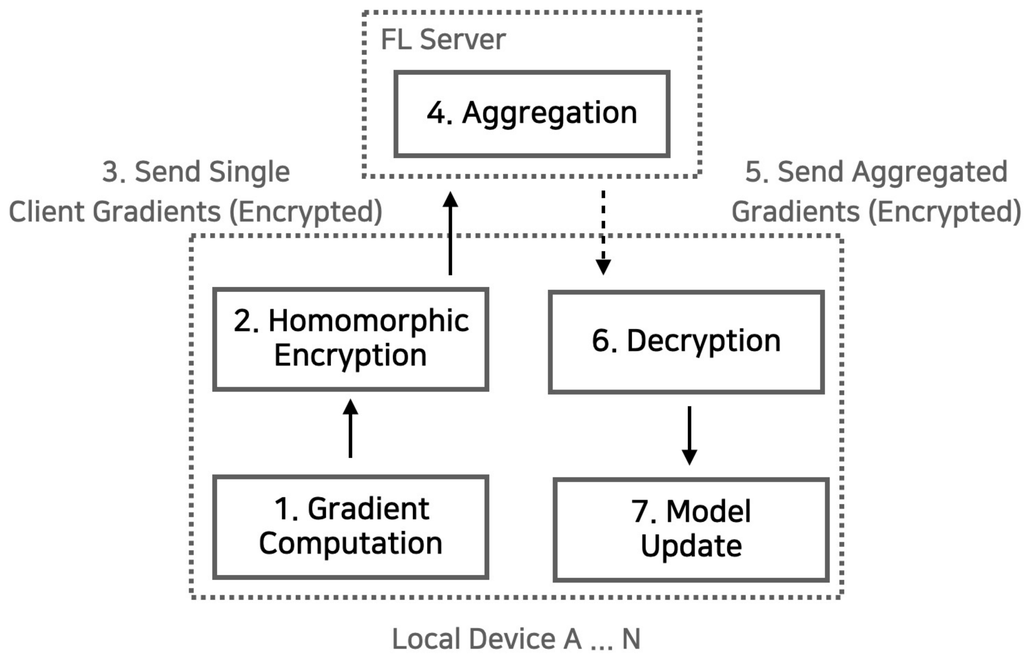
제안 시스템은 연합 학습 환경에서 Secure Aggregation을 구현하고, 전송 받은 모델을 안전하게 Model Averaging하는 것을 목표

Algorithm 1: Client $i = 1, 2, \cdots, N$

```
gradientComputation(i) /* local model training */
encryptedGradients = homomorphicEncrypt(i)
sendToServer(encryptedGradients) /* client N's */
```

Algorithm 2: FL Server (Aggregator)

```
eg = encryptedGradients 1, 2, ··· , N
Aggregation(eg)
SendToClients(eg)
```



관련 연구 및 문제 정의

관련 연구[2-3]를 분석하여 연합 학습이 자율주행 도메인에 적용된 사례를 조사하였고, 연합 학습 구조에서 로컬의 학습한 모델을 중앙으로 전송 과정에 잠재적인 보안 취약점 발견

V2X (Vehicle to Everything) 통신에서는 각각의 차량에서 서명한 인증서를 전체적인 인프라 안에서 인증 수단으로 활용하지만, 로컬 인증서 위/변조 문제 존재

클라이언트가 외부 공격자에 의해 생성된 악성 인증서를 통신에 사용할 경우 SSL Session 생성 후 중간에서 Sniffing 가능

이를 해결하기 위해 로컬 모델을 Homomorphic Encryption 과정을 거친 후 전송하는 방법을 선택하였고, 암호화된 문자열 상태에서도 연산 가능 [4-5]

연합 학습의 Global Aggregation에서 Decryption 과정 없이 연산을 수행 가능하여 큰 장정이 될 것

(주요 알고리즘: Paillier, FAHE1)

결론 및 향후 연구계획

본 연구를 통하여 중앙 저장소에 적재하는 접근 방식에서 벗어나 데이터 보안을 고려하고 분산 시스템에서 가능한 기계학습 시스템 제안

이후 계획으로 제안 시스템을 실제 구현해서 기존의 접근 방식과 실험 결과 비교 예정이며, 각각의 로컬 디바이스가 소유한 적은 양의 데이터 활용을 위해 Data Augmentation 적용 방안에 대한 연구 고도화

참고문헌

[1] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 2017.

[2] Nguyen, Anh, et al. "Deep federated learning for autonomous driving." 2022 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2022.

[3] Han, Mu, et al. "Federated learning-based trajectory prediction model with privacy preserving for intelligent vehicle." International Journal of Intelligent Systems (2022).

[4] Bonawitz, Keith et al.. "Practical secure aggregation for privacy-preserving machine learning." In proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175-1191. 2017.

[5] Stehlé, Damien, and Ron Steinfeld. "Faster fully homomorphic encryption." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2010.