충전 인프라 환경에서 안전한 연합학습 모델 학습기반 Smart Contract의 보안성 강화 방안연구

전정민° 홍충선*

경희대학교 컴퓨터공학과

{jmjeon0212°, cshong* }@khu.ac.kr

Enhanced Security Using Smart Contract for Learning Based on Secured Federated Learning Model in a Charging Infrastructure Environment

Jeongmin Jeon°, ChoongSeon Hong*

Department of Computer Science and Engineering, Kyung Hee University

요 약

미래사회는 충전 인프라 환경에서도 인공지능 기반으로 에너지를 공유하고 더 나아가 에너지 사용과 온실가스 사용을 최소화하는 제로 에너지 지향사회로 나아갈 것이다. 이에 따라 에너지 효율을 최대화할 수 있는 인공지능 기반 스마트 전기 자동차의 패러다임으로 변화하고 있다. 이러한 변화 흐름에 적용될 수 있는 기술로서, 현재 충전 인프라 환경에서 센서의 사용정보를 종합하여 에너지 효율을 높이기 위한 연합학습 기술이 발전하고 있다. 본 논문에서는 연합학습 메커니즘을 전기차 충전 인프라에서 사용 시 악의적인 클라이언트의 보안 위협을 방지하기 위한 솔루션을 설계하고 공격자가 글로벌 모델 공격을 방지하는 알고리즘을 구현한다. 연합학습을 이용하면 EVSE(Electric Vehicle Supply Equipment)에서의 민감한 충전 정보 데이터 및 차량 내 센서 데이터를 통해 자가정비, 효율적인 충전 등을 사용할 수 있지만, 우려되는 보안 문제를 해결하기 위해서 본 논문에서는 이더리움 메인넷에서 스마트 계약(Smart Contract)을 이용하여 연합학습 시 학습된 글로벌 모델을 Smart Contract를 통해 자동 실행하는 프레임워크를 제안한다. 본 논문에서 새로 제시하는 연합학습과 Smart Contract를 활용한 FLSC(Federated Learning Smart Contract) 알고리즘을 통해 더 안전한 충전 인프라 구축할 수 있다.

1. 서 론

최근에 제안된 연합학습[1]은 수천 또는 수백만 명의 참가자들과 딥러닝 모델에 대한 대규모 분산 훈련을 위한 프레임워크이다. 따라서 참가자의 프라이버시를 보장하면서 훈련 데이터를 의도적으로 설계된 연합학습은 참가자의 로컬 데이터 및 학습에 가시성을 제공하지 않는다. 학습 과정에서 개인 데이터가 교환되지 않기 때문에 연합학습은 참여 고객에게 개인정보 보호를 제공하며 충전 인프라, 엣지 컴퓨팅, 금융 및 건강 관리 분야에서 광범위한 응용 프로그램으로 개발되고 있다[2]. 하지만 연합학습 시스템은 악의적인 클라이언트의 공격에 취약하며 실제 배포의 중요 장애물이 되고 있다[3].

연합학습 기반에 충전 인프라 환경에서 중앙 Aggregator 는 동작을 제어하거나 개인 충전 데이터에 접근할 수 없다. 결과적으로 악의적인 클라이언트는 유해한 모델 업데이트를 전송하여 글로벌 모델에 대해 공격을 함으로써 중앙 Aggregator 을 속일 수 있다. 이러한 머신러닝 연구에서는 비잔틴 공격에 대한 방어를 시작으로 광범위하게 연구되어 왔다[4]. 기존 연구에서 높은 모델의 성능을 달성할 수 없음을 발견하였다.

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 70300038) *Dr. CS Hong is the corresponding author.

본 논문에서는 악의적인 클라이언트들의 Back door, 중간자 공격(man in the middle attack, MITM) 등을 방지할 수 있는 이더리움 메인넷에 Smart Contract 메커니즘을 활용하여 미리 정해진 규칙에 따라 실행되도록 하여 공격자가 글로벌 모델을 공격 방지하는 것을 목표로 한다.

본 논문에 2장에서는 연합학습의 개념과 Smart Contract에 관한 내용을 다루고, 3장에서는 문제 정의와 시스템 모델에 대한 설명하려 한다. 4장에서는 제안된 알고리즘에 대한 분석에 관한 내용을 다루며, 마지막 5장은 본 논문의 결론 및 향후 연구 방향을 제시한다.

2. 관련연구

2.1 연합학습

연합학습(Federated Learning; FL)은 중앙서버에서 딥러닝 모델을 m명에 사용자에게 배포하고 사용자는 자신의 데이터로 모델을 학습시킨다[1]. 이후 각 사용자 단말에서 학습된 모델은 중앙으로 통합된다. 학습에 각 Round (t)에서 중앙서버는 m개의 참가자(S_m) 의 서브셋을 무작위로 선택하고 그들에게 현재 Joint Model(G^t)을 전송한다. m을 선택하는 것은 학습의 효율성과 속도 사이의 균형을 포함한다. 선택한 참가자는 ① 을 사용하여 개인 데이터를 학습한다. 로컬 모델을 새로운 로컬 모델 L^{t+1}을 업데이트하고 $L_i^{t+1} - G^t$ 차이를 중앙서버

로 다시 보낸다.

글로벌 학습률 η는 매 Round (t) 마다 업데이트되는 Joint Model의 비율을 제어한다. $\eta = \frac{n}{m}$인 경우 모델은 로컬 모델의 평균으로 완전히 대체된다[3]. 위에 설명한 연합학습 시스템에 따라 중앙서버가 클라이언트 동작을 제어하거나 개인 데이터를 액세스할 수 없으므로, 악의적인 클라이언트는 글로벌 모델을 수정하여 유해한 모델 업데이트를 전송하는 공격이 가능하다.

따라서 서버를 속일 수 있는 취약점을 가지고 있다. 본 논문에서는 Federated Learning Smart Contract(FLSC) 알고리즘을 통해 보안성을 향상시키는 프레임워크를 제안하고, 기존 연구가 진행되고 있는 비잔틴 공격에 관한 광범위한 연구보다 보안성이 성능을 평가하고자 한다.

2.2 스마트 계약

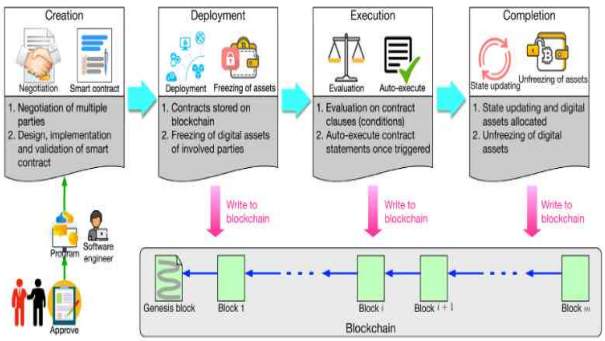

그림 1 Smart Contract System Structure.

Smart Contract는 블록체인 기술의 발전으로 간주 될 수 있다. 1990 년대 Smart Contract는 계약의 계약 조건을 실행하는 전산화 된 거래 프로토콜로 제안되었다 [6]. Smart Contract에 포함된 계약 조항은 조건이 충족되었는지 확인하면 자동으로 시행된다 (예 :계약을 위반한 당사자는 자동으로 처벌됩니다).(예 : if-else-if statement).

각 계약의 실행은 블록 체인에 저장된 불변의 트랜잭션으로 기록된다. 그림 1은 Smart Contract의 전반적인 구조에 관해 설명한다. Smart Contract는 스마트 전기 자동차와 EVIE 간의 미리 정의된 규칙을 기반으로 감시 가능한 다중 상대 트랜잭션을 지원하는 자동화된 Smart Contract를 가능하게 한다[5].

3. 제안 사항

3.1 문제 정의

기존 전기차 충전 인프라의 연합학습 적용 구조는 다수의 클라이언트가 FedAvg 알고리즘[1]을 사용하여 중앙서버에서 유지관리 하는 머신러닝 모델을 공동으로 훈련하는 전형적인 연합학습 설정을 고려한다. 그림2와 같이 공격자는 일반적으로 학습된 글로벌 모델을 수정하여 유

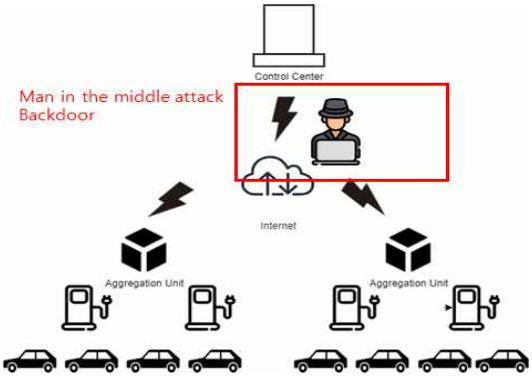

그림 2 Existing EV charging network topology

해한 모델 업데이트를 Control Center로 전송하는 통신 메시지 조작, 충전 데이터 도청 및 도용, 분쟁 및 부인, 악성코드 삽입과 같이 전기차 충전 인프라의 보안을 위협할 수 있다.

3.2 시스템 모델

그림 3은 FLSC Algorithm을 활용한 연합학습기반 이더리움 Smart Contract로써 EVSE에 대해 제안된 충전 시스템 모델을 나타내며, 충전 시스템은 각 EVSE에서 충전 Data, 유효성, 차량 정보, 충전계약 및 사용자 초기화, 등록, 인증 및 청구 4단계로 다음과 정의한다.

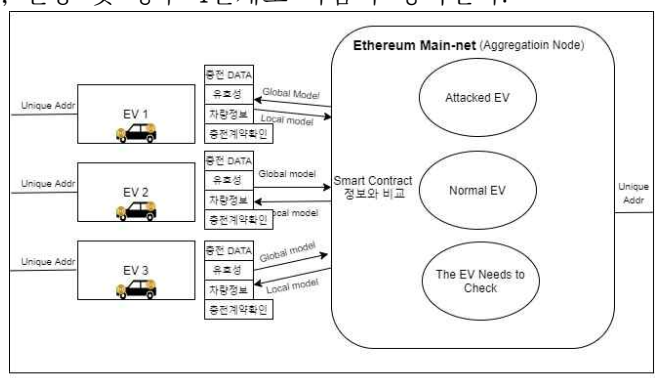

그림 3 Proposed FLSC Algorithm based charging system model for EVSE

1. *최초 EV는 충전 서비스에 액세스하기 위해 Smart Contract에 신원을 등록한다.*
2. *EV 와 Aggregation node는 서로 인증을 한다.*
3. *Aggregation node는 트랜잭션을 생성한다.*
4. *Aggregation node는 거래가 유효한지 확인하고 이더리움 블록체인 네트워크에 거래를 기록한다. FLSC알고리즘의 각 학습 파라미터는 Algorithm 1과 2에서 나타내었다.*

Algorithm 1. Aggregation node side:
Federated Learning-SmartContract(FLSC)

i) A possibility of Man in the middle attack. the local model or global model.
ii) Perserving the privacy between the UEs and aggregation node..
Set ContractAddress = 0;
GlobalModel =0:
Whild(true) {
ContractAddress = receive it From a UE

ContractAddress.put(contractAddress)
C= load Contract+(contractAddress)
UEModel += UELocalModel

}
Foreact c in ContractAddress send it to UEs.

Algorithm 2. Charger (User Equipments) node side:
Federated Learning-SmartContract(FLSC)

While (| stopping CriteriaNotMet() | {
M = Build Local Model from local data + global model
C = Create instance of Contract ModelContract over the Ethereum MainNet network.
C.initContract(ueAddress, aggAddress)
C.setModel(M):
Send c.getAddress() to Aggregat Node;
}

4. 성능평가

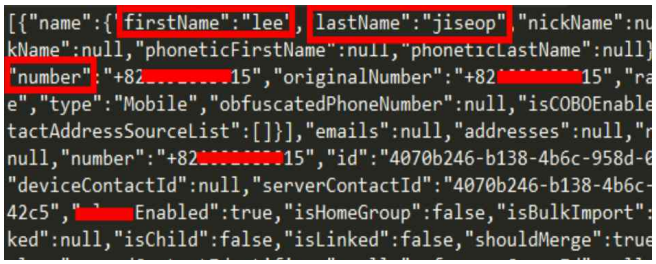

그림 4 Smart-Contract information in EVSE

본 논문의 시뮬레이션에서는 하나의 Aggregation node와 이더리움 메인넷을 사용하였고, Smart Contract에서 100개의 EV에 가능한 계약을 제공하는 시나리오를 고려하였다. EV Type의 상한 하한은 각 1과 0으로 설정된다. 데이터는 Public Charging Stations in Hawaii 데이터를 사용하였고 매개 변수는 ω는 model weight. ue는 클라이언트 aggregation Node는 g로 지정한다.

그림5 는 FLSC 알고리즘 보안성을 비교하는 그래프이다. 100개의 가능한 계약을 사용하여 전통적인 연합학습과 [4] 에서 제안한 비잔틴 공격에 대한 보안성 평가는 본 논문에서 제시한 FLSC 알고리즘이 더 좋은 것을 볼 수 있다.

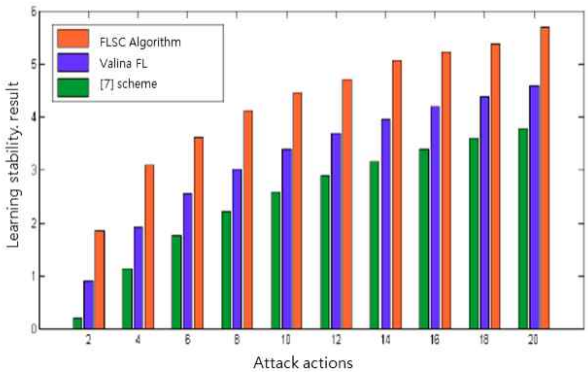

그림 5 Security Evaluation result.

5. 결론 및 향후 연구

본 논문에서는 FLSC 알고리즘 이용하여 충전 인프라 환경에서 개인 충전 정보 및 민감한 데이터를 통해 학습할 때 학습 모델 변조가 발생할 수 있는 위협을 막고 보안성을 향상함을 보여준다. Smart Contract를 통해 모든 인증을 거쳐서 기존 비잔틴 공격에만 연구가 되었던 것을 중간자 공격, 백도어 공격도 방지 할 수 있는 이점을 보였다. 향후 연구로는 제안된 시스템에서 다른 딥러닝 알고리즘에서 발생할 수 있는 보안 문제에 대해 해결을 하는 것을 연구할 계획이다.

6. 참고문헌

[1] Li, Q., Wen, Z. and He, B., 2019. Federated learning systems: Vision, hype and reality for data privacy and protection. arXiv preprint arXiv:1907.09693.

[2] Liping Li, Wei Xu, Tianyi Chen, and et al. RSA: Byzantine-robust stochastic aggregation methods for distributed learning from heterogeneous datasets. In Proceedings of AAAI' 19, Jan. 2019.

[3] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, and et al. How to backdoor federated learning. arXiv preprint arXiv:1807.00459v3, Aug. 2019.

[4] Yudong Chen, Lili Su, and Jiaming Xu. Distributed statistical machine learning in adversarial settings:\ Byzantine gradient descent. Proceedings of ACM MACS' 17, 2017.

[5] Jeon Min Jeon, Sun Moo Kang, Choong Seon Hong, "MicroGrid Energy Sharing Framework using Permissioned Blockchain," KNOM 2019.

[6] J. Ream, Y. Chu, D. Schatsky, Upgrading Blockchains: SmartContract Use Cases in Industry, Deloitte Press, 2016, https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/

[7] Long, C., Wu, J., Zhou, Y. and Jenkins, N., 2018. eer-to-peer energy sharing through a two-stage ggregated battery control in a community Microgrid. Applied energy, 226, pp.261-276.