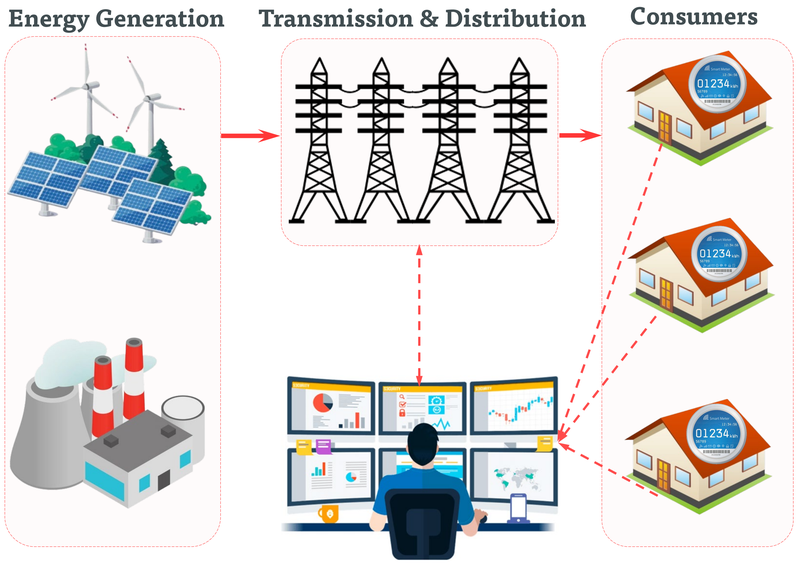
Does Detecting Energy Theft in Smart Grids Matter? Privacy-Preserving and Secure Federated Learning for Enhanced Grid Security

Mohamed Elmahallawy, Assistant Professor, Computer Science & Cybersecurity Department,
School of Engineering and Applied Science | Email: mohamed.elmahallawy@wsu.edu

Introduction



Security and Privacy Threats

✓ Insider Threats

Definition:

Fraudulent consumers engage in electricity theft by manipulating their smart meter readings through cyber attacks to unlawfully lower their utility bills.

Attackers' Goals:

- To cause financial losses and degrade grid performance by injecting false readings that mislead grid management systems.

✓ Outsider Threats

Definition:

An adversary or eavesdropper on the communication channel between customers and the billing center can compromise consumers' privacy by inferring their lifestyle from their daily usage patterns.

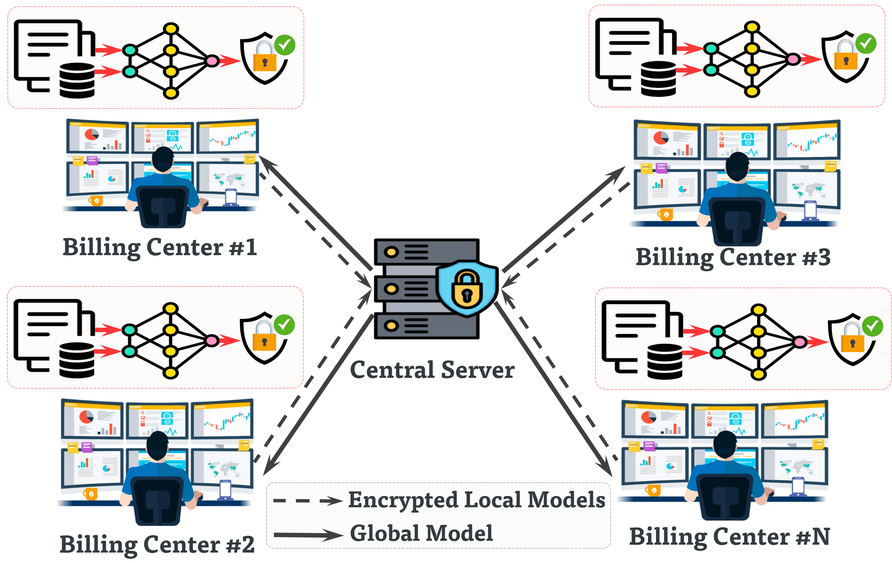
Attackers' Goals:

- Disclose the original data of billing centers or customers for malicious purposes through membership inference attacks.
- Expose customers' daily lifestyle patterns through model inversion attacks.

Methodology

✓ *Federated Learning (FL)*

- ***Distributed Training:*** FL operates as a decentralized learning paradigm, effectively achieving a balance between safeguarding customers' information and fostering collaborative learning.
- ***Data Privacy:*** FL customers don't need to send their raw data, like daily electricity readings. Instead, each customer can train a local machine learning (ML) model and only share the model parameters with the billing center.



✓ Addressing Security and Privacy Threats

▪ Privacy Preserving

We propose FedEncrypt, an approach for secure and privacy-preserving FL for smart metering infrastructure

- Each billing center after training its local machine learning (ML) model, it securely encrypts its ML model using ***the anonymous-veto*** (AV) protocol [1] without the need for a key distribution center (KDC) to generate its public or private keys.
- Billing centers transmit their encrypted ML models until they reach the centeral server, ensuring eavesdroppers cannot launch model inversion or membership inference attacks.
- Once the central server receives all billing centers' models, it aggregates them using an ***inner product functional encryption*** (IPFE) [2] scheme to generate a global model in plaintext without the need to decrypt each individual model or gain an ability to leak any sensitive information about the original satellite data.

▪ Security Verification

- To safeguard the global model against alterations or manipulation during transmission over insecure communication channels, the central server utilizes a robust symmetric key cryptosystem, namely the ***advanced encryption standard*** (AES).
- Furthermore, to maintain the integrity of the global model parameters, the central server implements a **signature-verification algorithm**, allowing it to verify the integrity of the received model parameters and ensure their trustworthiness.

Performance Evaluation

We compare our proposed scheme, FedEncrypt, with a recent approach called FedDetect [3]. The results are as follows:

▪ Security and Privacy Analysis

- FedEncrypt uses IPFE to aggregate billing centers' models without a trusted KDC or secure channel for key transfer, increasing resilience with the same security level as literature.
- FedEncrypt is resistant to eavesdroppers who can intercept ciphertexts but cannot access billing centers' local parameters (encrypted using inaccessible secret keys)
- FedEncrypt resists collusion threats as central server aggregates only encrypted parameters from billing centers, learning nothing about individual parameters

▪ Computation Overheads

- We measure the computational overhead as the message composition time by each billing center.
- FedEncrypt encrypts its ML model's parameters in just 1ms, primarily due to a single exponentiation operation. In contrast, FedDetect takes around 23ms, demonstrating a 23-fold improvement in speed with FedEncrypt.

▪ Communication Overheads

- We measure the communication overhead by analyzing the size and quantity of messages exchanged between the billing centers and the central server during the FL process.
- FedEncrypt reduces the communication overhead to 497 MB, down from 6258 MB in FedDetect, demonstrating a 13-fold improvement.

References

[1] B. King, "A point compression method for elliptic curves defined over gf (2n)," in Public Key Cryptography. Springer, 2004
[2] M. Abdalla et al.,"Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings," in Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Proceedings, Part I 38. Springer,2018
[3] Wen, Mi, et al. "FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid." IEEE Internet of Things Journal 9.8 (2021): 6069-6080.