A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT

Rongxing Lu, Kevin Heung, Arash. H. Lashkari, and Ali A. Ghorbani

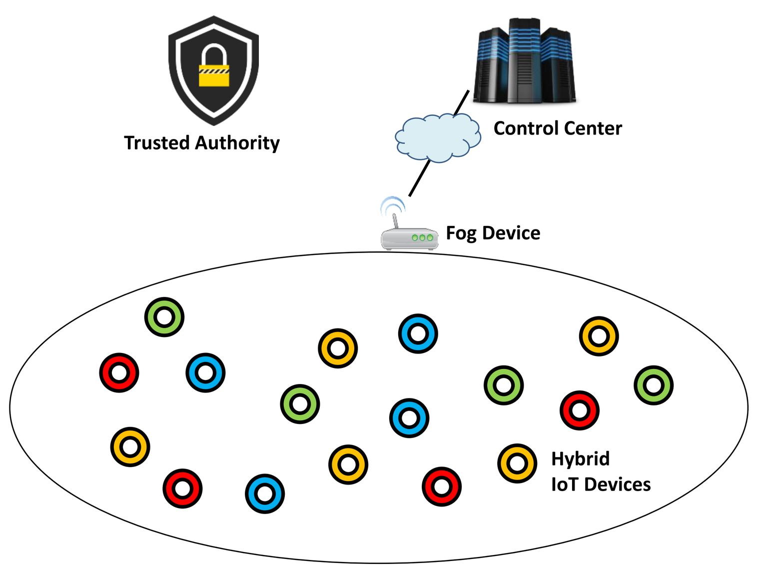
Website: http://unb.ca/cic/

Canadian Institute for Cybersecurity (CIC), University of new Brunswick (UNB)

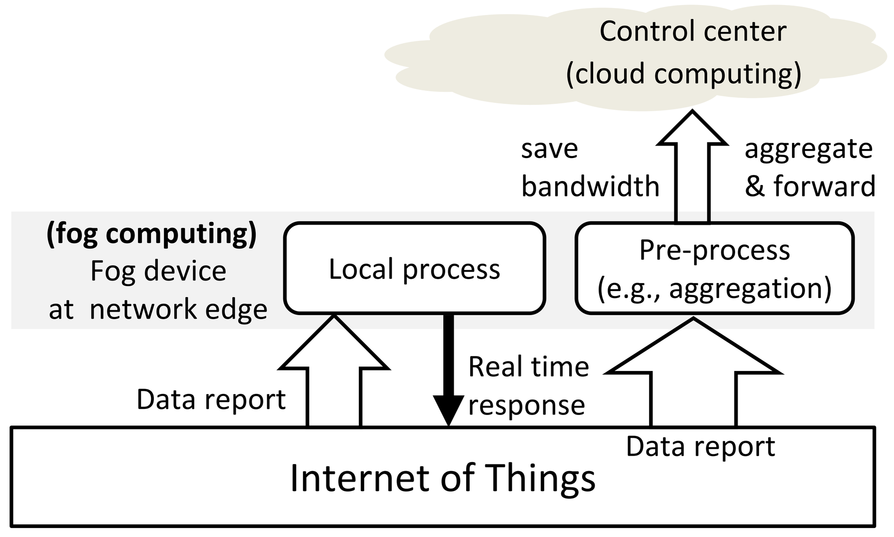
ABSTRACT

Fog computing-enhanced Internet of Things (IoT) has recently received considerable attention, as the fog devices deployed at the network edge can not only provide low latency, location awareness but also improve real-time and quality of services in IoT application scenarios. In this work, we present a lightweight privacy-preserving data aggregation scheme, called Lightweight Privacy-preserving Data Aggregation, for fog computing-enhanced IoT. The proposed LPDA is characterized by employing the homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash chain techniques to not only aggregate hybrid IoT devices' data into one, but also early filter injected false data at the network edge. Detailed security analysis shows LPDA is really secure and privacy-enhanced with differential privacy techniques. In addition, extensive performance evaluations are conducted, and the results indicate LPDA is really lightweight in fog computing-enhanced IoT.

System Model



- **IoT devices:** a set of hybrid IoT devices $D = \{D_1, D_2, \cdots, D_n\}$ are deployed at an area of interest.
- **Fog device:** is deployed at the network edge, which performance the aggregation operations and filter injected false data
- **Control Center:** is a control entity deployed at a cloud platform.
- **Trust authority:** is a fully trusted entity in the system.



Design Goals

- Privacy
- Security
- Fault-Tolerance
- Efficiency

Technical Background

- Chinese Remainder Theorem
- One-way hash chain
- Properties under the modulo n^2

1) For any $x \in \mathbb{Z}^*_{n^2}$, we have $x^{n\lambda} \equiv 1 \bmod n^2$.
2) For any $x_i \in \mathbb{Z}_n$, $i = 1, 2, \cdots, m$, we have

$$\prod_{i=1}^{m}(1 + n \cdot x_i) \equiv (1 + n \cdot \sum_{i=1}^{m} x_i) \bmod n^2$$

- Differential privacy techniques

LPDA: Lightweight Privacy-Preserving Data Aggregation Scheme

- System Initialization:
- IoT Device Report Generation:
- Fog Device Report Aggregation:
- Control Center Report Reading and Analytics

$$c_{is} = [1 + n \cdot \alpha_j \cdot (x_i \cdot \alpha_0 + x_i^2)] \cdot H(T_s)^{n \cdot s_i} \bmod n^2$$

$$C_s = \left(\prod_{i=1}^{N} c_{is}\right) \cdot H(T_s)^{n \cdot s_{N+1}} \bmod n^2$$

$$M = \sum_{j=1}^{k} \alpha_j \left(\sum_{i=1}^{N_j}(x_i \cdot \alpha_0 + x_i^2)\right) \bmod Q$$

$$M_j = M \bmod q_j = \sum_{i=1}(x_i \cdot \alpha_0 + x_i^2)$$

$$E(\mathcal{D}_j) = \frac{M_j - (M_j \bmod \alpha_0)}{\alpha_0 \cdot N_j}$$

$$Var(\mathcal{D}_j) = \frac{M_j \bmod \alpha_0}{N_j} - E(\mathcal{D}_j)^2$$

Security Analysis

- can resist against the false data injection from the external attacks.
- privacy preservation enhanced with differential privacy techniques

✓ An algorithm A(.) can achieve ε-differential privacy, if for any two data sets DS1 and DS2 differing on a single element, for every subset S ⊆ Range(A),

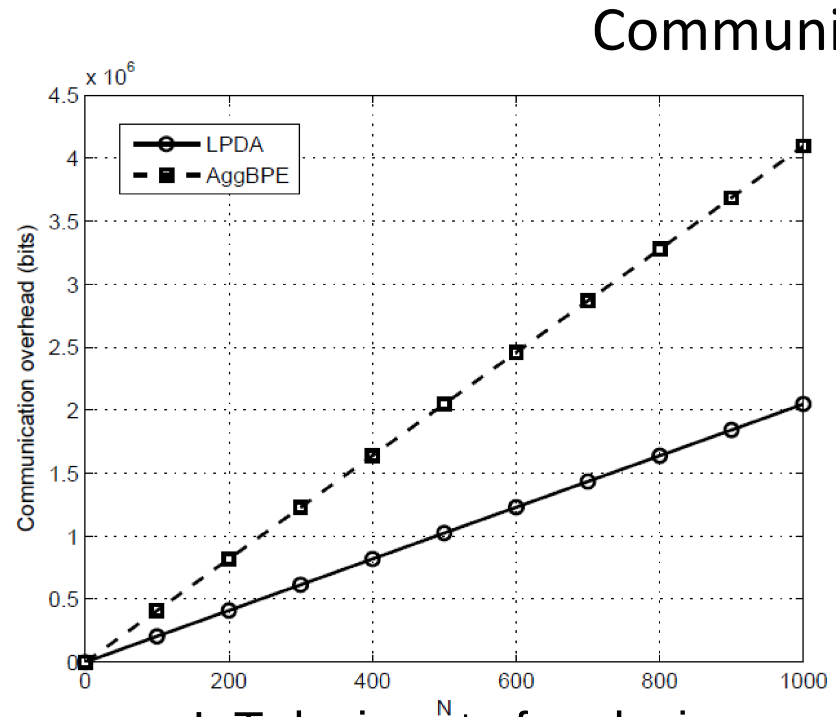
Pr[A(DS1) ∈ S] ≤ exp(ε) · Pr[A(DS2) ∈ S] holds.

Performance Evaluation

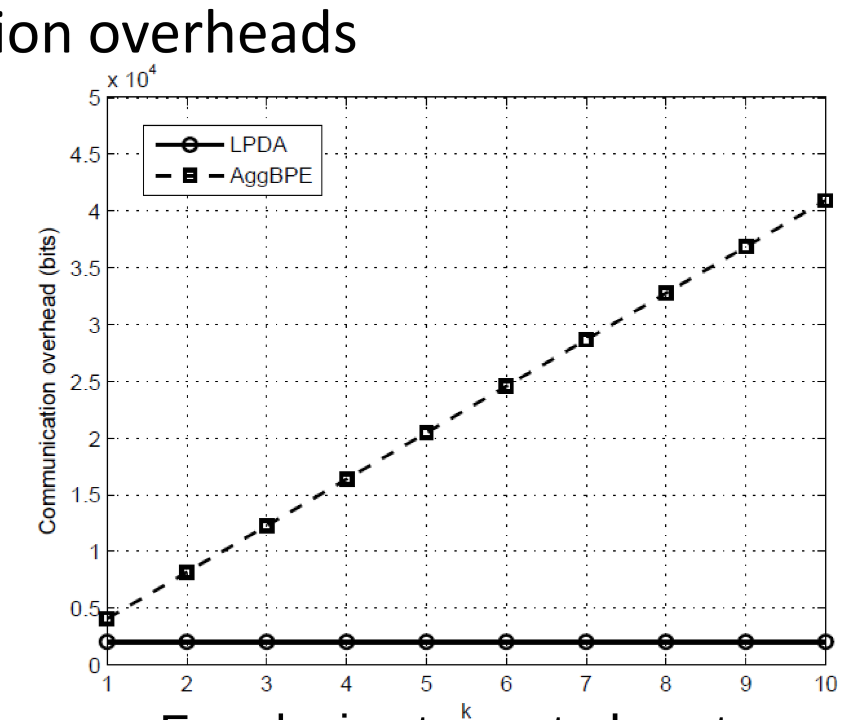
Computational costs

Entities	Computational costs	
	without malfunctioning device and no differential privacy enhancement	enhanced with differential privacy
Each IoT device	0.328 ms	
Fog device	0.470 ms	0.578 ms
Control center	0.062 ms	0.156 ms

Communication overheads



IoT devices to fog device



Fog device to control center

Parameter Settings

Parameter	Value
k_0, k_1, l	$k_0 = 512$, $k_1 = 50$, $l = 160$
p, q	$\lvert p\rvert = \lvert q\rvert = k_0 = 512$
$n = pq$	$\lvert n\rvert = 2k_0 = 1024$, $\lvert n^2\rvert = 4k_0 = 2048$
q_i	$\lvert q_i\rvert = k_1 = 50$
N, k	$N = 1000$, $k = 10$: 1000 IoT devices in 10 subsets
N_j	$N_j = 100$: the size of each subset $\mathcal{D}_j$ is 100
α_0	$\lvert\alpha_0\rvert = 30$: the size of the parameter α_0
X	$X = 2^8$: the message space is $[0, 2^8]$
ε	$\varepsilon = 1$: the privacy parameter set in differential privacy
$\mathbf{x}_{j1}$	$\mathbf{x}_{j1} \in Geom(\exp(-\frac{\varepsilon}{X}))$: the 1st noise added in $\mathcal{D}_j$'s aggregation, i.e., $\sum_{D_i \in \mathcal{D}_j} x_i + \mathbf{x}_{j1}$
$\mathbf{x}_{j2}$	$\mathbf{x}_{j2} \in Geom(\exp(-\frac{\varepsilon}{X^2}))$: the 2nd noise added in $\mathcal{D}_j$'s aggregation, i.e., $\sum_{D_i \in \mathcal{D}_j} x_i^2 + \mathbf{x}_{j2}$

Conclusion

- we have proposed a lightweight privacy-preserving data aggregation scheme, called LPDA, for fog computing-enhanced IoT. With the fog device deployed at the network edge, LPDA can not only early filter false data injected by external attackers, but also support fault-tolerance and efficiently aggregate hybrid IoT devices' data into one.

Future Work

- In future work, we will evaluate our proposed scheme in some realistic IoT scenarios, consider stronger adversarial model, and design new solutions under new model.

For more details: →

R. Lu, K. Heung, A. Lashkari, and A. Ghorbani, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT", IEEE Access, in press.