Achieving Communication-Efficient Privacy-Preserving Query for Fog-Enhanced IoT
Nafiseh Izadi Yekta (Master Student) and Rongxing Lu*
Contact Email: rlu1@unb.ca
Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB)

ABSTRACT

Internet of things (IoT) has attracted significant attention in recent years, and various IoT devices including industrial and utility components and other items embedded with electronics, sensors, and network connectivity have already provided rich services to the end users. Nevertheless, IoT still faces many security and privacy challenges. In this paper, we propose a new efficient privacy-preserving query scheme, called XRQuery, for fog computing-enhanced IoT. The proposed XRQuery scheme is characterized by employing a new communication-efficient private information retrieval technique, which can preserve the privacy for both the end user and the service provider in IoT query service. Detailed security analysis shows the XRQuery scheme really preserves the privacy. In addition, extensive performance evaluation also indicates XRQuery can vastly reduce the communication overheads between the fog device and the end user in fog computing-enhanced IoT.

1. System Initialization

- **IoT devices**: a set of IoT devices \( D = \{D_1, D_2, \ldots, D_n\} \) are deployed at an area of interest.
- **Fog device**: is deployed at the network edge, which receives the data reported from IoT devices
- **Service provider**: is a server deployed at a cloud platform.
- **End user**: is an IoT service requester in our model.

2. End User Query

- End user’s query (Enc(1), Enc[])
  - Enc[] = {Enc[0], Enc[1], \ldots, Enc[m]} where m is equal to \( \log(n) \)
  - Encrypts the value 1 as Enc(1)

**Algorithm 1: QUERY GENERATION**

**Input**: \( (SK, bits[], d) \) for querying device \( D_a \)

1. for \( j = 0 \) to bits.length do
2. \[ Enc[j] = s^d(r_j \cdot q + bits[j]) \mod p \]
3. return Enc[]

3. Fog Device Response

- **Algorithm 2: XNOR GENERATION**
  **Input**: Enclist, Enc(i), and array[j]
  **Output**: XNOR[i]

1. for \( j = 0 \) to array.length do
2. \[ XNOR[i] = \begin{cases} 
           Enc(1) + Enc(1) + Enclist[j] \times array[j](q - 1) \times Enclist[j] + \\
           (Enc(1) + Enc(1)[q - 1])(1 - array[j])(q - 1) \mod p 
        \end{cases} \]
3. return XNOR[]

4. End User Result Checking

- XRQuery is inspired by XNOR gates in logical circuits to achieve privacy preservation for both service provider and user in an IoT query service.
- XRQuery is super efficient in term of communication cost i.e., achieving \( O(\log(n)) \) between the end user and the fog device.
- The extensive performance evaluations show it is very efficient in terms of computational cost.

Conclusion

Future Work

For future work, I want to investigate other areas of private information retrieval to assess the possibility of using the same technique to improve the state of the art of those areas.