Low-cost Client-side Encryption and Secure Internet of Things (IoT) Provisioning

Joseph N. MAMVONG, Gokop L. GOTENG, Yue GAO

Frontiers of Computer Science, DOI: 10.1007/s11704-022-1256-9

Problems & Ideas

- **Problems of associated with client-side encryption and secure provisioning of constrained IoT devices include:**
  - Resource constraint with respect to the cost of using classical algorithms for encryption before outsourcing of IoT device data onto cloud storage systems
  - Availability of information on the process and ease of IoT provisioning.
- **Ideas:** An implementation of a low cost algorithm (based on the Advanced Encryption Standard) in tandem with IoT device constraint is utilized for client-side encryption of a sample IoT device and detailing the process of provisioning the sample IoT device onto an IoT cloud platform.

Algorithm 1: Client-Side-Encryption Execution Flow

```
Message, Key
initialization of the counter i = 0 and Nbr = 2
Expand key to length: (block size) *Nbr + block size
STATE = message XORed with Key (Key whitening)
Invoke the round function:
while i < Nbr : do
    STATE = SubByte(STATE)
    STATE = ShiftRows(STATE)
    if i < Nbr : then
        STATE = MixColumn(STATE)
    end
    Invoke addRoundKey(STATE, NextRoundkey)
end
STATE as resulting Ciphertext
```

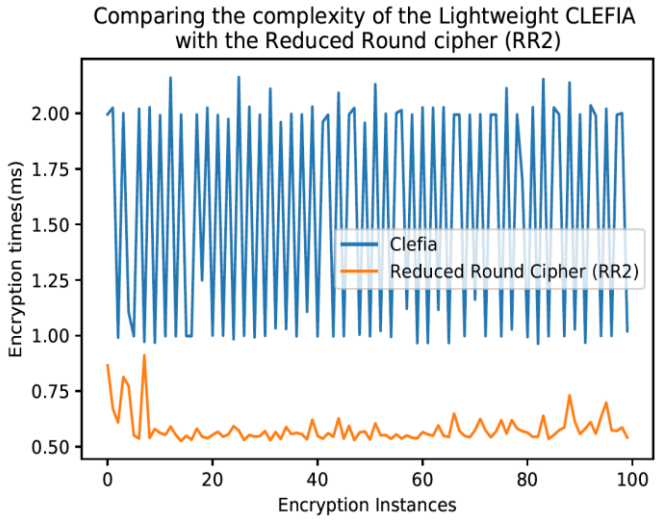
Algorithm 2: Device Provisioning Process Flow

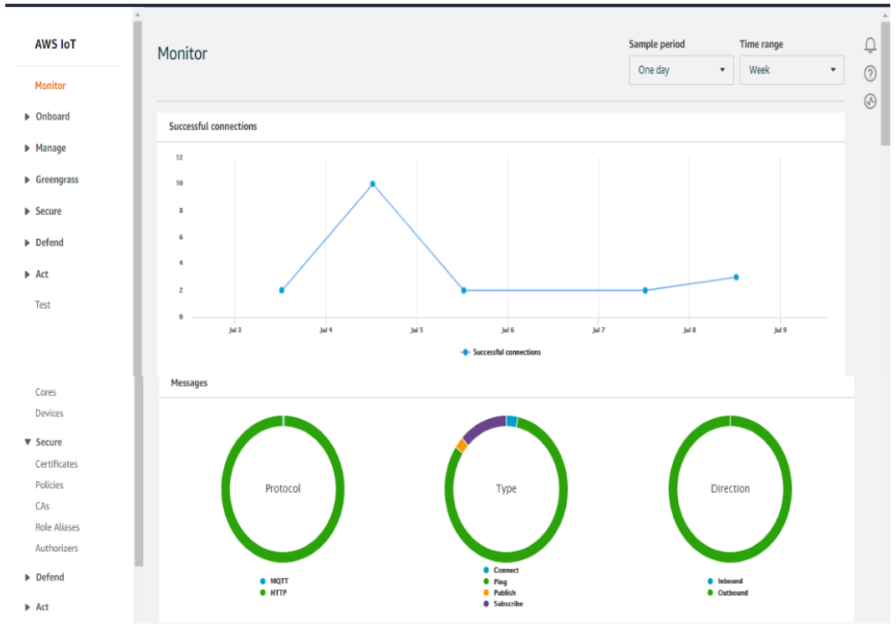
```
Initializing the IoT device and the ATECC608A secure element
Invoking device-cloud authentication leveraging the ATECC608A tamper-proof security keys
while Creation and registration of a Certificate Authority (CA) and the IoT device's security credentials do
    Create a Certificate Authority's root certificate
    ← Certificate
    Invoke the IoT device's certificate signing request to a certificate signer Certificate Authority
    sign the certificate signing request using the root certificate
    ← Certificate
    register the device's digital identity using the signed certificate.
    ← DeviceUniqueID
end
Connect the device to the IoT cloud by Via passing the network medium credentials to the WINC1500
```

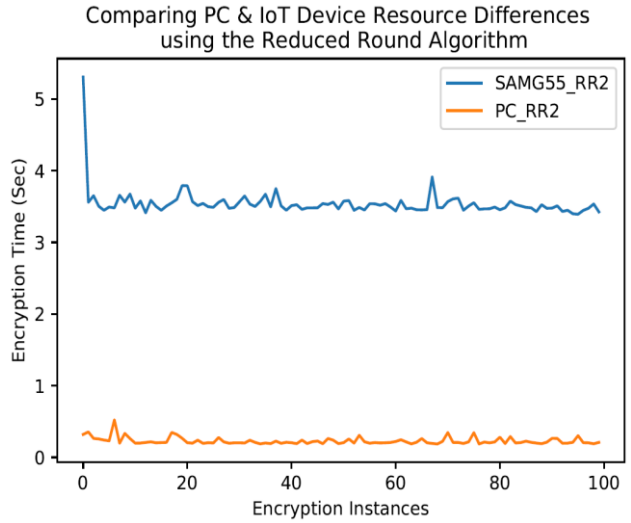
Client-side encryption and device provisioning algorithms. Left: The low-cost algorithm (based on the AES) Right: comparison of the PC and SAMG55 implementations of the reduced round algorithm.

Main Contributions

- **Contributions:**
  - **Implementation and comparison a Low-cost algorithm (Based on the AES) to lightweight CLEFIA, experimentation of the avalanche effect test on the low-cost algorithm and using it as client-side encryption solution in provisioning the SAMG55 microprocessor;**
  - **Experimentation and analysis of resource constrain in IoT devices, exemplified by comparing a PC and SAMG55 implementations of a Low-cost algorithm for client-side encryption to the standard AES128;**
  - **Secure provisioning of a sample IoT device (SAMg55 microprocessor) on AWS IoT core using the Amazon Web Services (AWS) Command Line Interface (CLI) programmatic access tools.**







Left: comparison of lightweight CLEFIA and the Low-cost cipher RR2; Middle: cloud-end view of the provisioned IoT device showing connection records; Right: comparison of the PC and SAMG55 implementations of the reduced round algorithm.