Front. Comput. Sci., 2022, 16(6): 166824
https://doi.org/10.1007/s11704-022-1256-9

LETTER

Low-cost client-side encryption and secure Internet of things (IoT) provisioning

Joseph MAMVONG (✉)[1], Gokop GOTENG[1], Yue GAO[2]

1 School of Electronic Engineering & Computer Science, Queen Mary University of London, London E1 4NS, UK
2 Department of Electrical and Electronic Engineering, University of Surrey, Guildford, Surrey GU2 7XH, UK

1 Introduction and main contributions

Internet of things (IoT) deployments hold the promise to revolutionize the technology landscape through the unprecedented connectivity of billions of devices, in many sectors including: transportation, businesses, healthcare, agriculture and homes to mention a few. In [1], cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The use of classical encryption schemes for appropriate client-side encryption before cloud storage is an additional challenge given the scarcity of power and computing resources available in constrained IoT.

As shown in the experimental setup in Online Resource 1, provisioning an IoT device onto a cloud platform entails the process of creating a unique identity on the cloud via requisite and secure authentication credentials, while client-side encryption is used to achieve encryption of data at the end of the device before it is sent onto cloud storage.

According to [2], while the deployment of IoT devices is estimated in billions, very little to no information is present on ease of device provisioning. According to [3], some of the challenging problems in the implementation of the IoT include: key management, device authentication, user access control, privacy preservation and identity management to mention but a few. Encryption-before-outsourcing is a widely recommended method to guarantee the confidentiality of user data [4] and the need for architecting IoT devices with client-side encryption capabilities in order to preserve the privacy of data generated and outsourced to cloud storage systems brings on additional burden on the devices, given the scarcity of resources. In order to protect the security of the outsourced data, an intuitive way is to encrypt the data before outsourcing it to the cloud [5].

This work investigates resource constrain on a sample IoT device, implemented a low-cost client-side encryption algorithm for data encryption as advocated in [5], and leverages a secure element to addresses the challenges of key management and device authentication as highlighted in [3], by securely provisioning the device on an IoT cloud services platform. The main contributions are as follows:

- Implementation and comparison a low-cost algorithm (Based on the AES) to lighweight 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 the Amazon Web Services (AWS) IoT core using AWS Command Line Interface (CLI).

2 Low-cost client-side encryption and secure IoT provisioning

With additional details provided in Online Resource 2, Algorithm 1 and Algorithm 2 summarize the low-cost client encryption and secure provisioning algorithms of the sample IoT device respectively.

Consequent upon the scarcity of computing resources on a typical IoT device, a Low-cost algorithm -based on the AES

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
```

Received May 13, 2021; accepted February 28, 2022

E-mail: j.n.mamvong@qmul.ac.uk

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

and detailed in [6] is utilized for experimenting a client-side encryption of 16bytes of data. Algorithm 1 presents an algorithmic sequence of execution of the reduced round algorithm. Favourable to the experimentation and analysis of resource constrain of IoT devices as detailed in the Online Resource 2, the reduced round algorithm is 35% cheaper than the standard AES algorithm in terms of the encryption completion time of a single block data and thus, a plausible candidate for client-side encryption of IoT device data before outsourcing to the cloud for storage or processing.

An Avalanche effect test was experimented on the low-cost algorithm, and the encryption completion time compared to that of lightweight CLEFIA, after which the Low-cost algorithm is implemented as a client-side encryption solution in provisioning the sample IoT device, as further detailed in the Online Resource 2. The AWS CLI tool was utilized for enabling programmatic access to the AWS IoT core cloud service and provisioning of the SAMG55 device and Zerynth studio for implementing and compiling the executable binaries of the reduced round algorithm for the sample client-side encryption of data. The cloud end of the experimental setup requires the creation of a cloud account with the AWS cloud platform, enabled with the AWS lambda and AWS IoT Core services.

3 Results, conclusion and future work

Our experimentation measured increase in the encryption completion time on the constrained IoT device in comparison to the PC, in determination of the level of constraint on a SAMG55 IoT device in determination of the level of constraint on the IoT device as shown in Fig. 2. The low-cost algorithm shows upto 50.3% reduction in the aforementioned encryption completion time and so, was utilized for experimenting low cost client-side encryption and the device provisioned to the cloud.

We implemented and compared the cost, in terms of encryption completion times, of lightweight CLEFIA and the efficient algorithm for power constrained IoT devices. A comparison of the least complex and the efficient algorithm for constrained IoT devices followed as shown in Fig. 1.

An analysis of resource constrain on an example IoT device (SAMG55) was presented by comparing a PC and SAMG55 microprocessor implementations of both the standard AES and the low-cost algorithm for client-side encryption of IoT device data. This comparison shows an increase of 657% in the encryption time using the IoT device in comparison to the PC, consequent upon the scarcity of computational resources available on typical IoT devices. The low-cost algorithm used for the client-side encryption is 35% less expensive in terms of the encryption completion time of a 16 bytes of data, compared to the standard AES and 0.97 times less expensive than lightweight CLEFIA, while passing the avalanche effect test with up to 93.75% which is well above a recommended 50% according to [7].

4 Conclusion

Security and ease of provisioning of IoT devices onto cloud infrastructure is instrumental to the deployment of IoT devices. With not much information available on the ease of secure provisioning of IoT devices couple with inherent challenge of these devices in encrypting data before transmission to the cloud due to their constrained nature, this work implements a low-cost client-side encryption algorithm

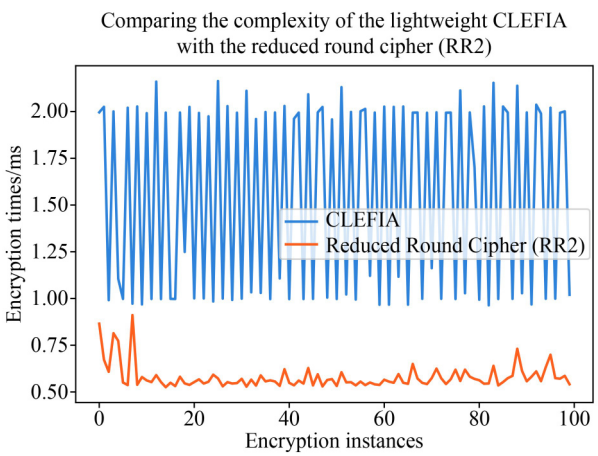

Fig. 1 Comparison of lightweight CLEFIA and the reduced round cipher (RR2)

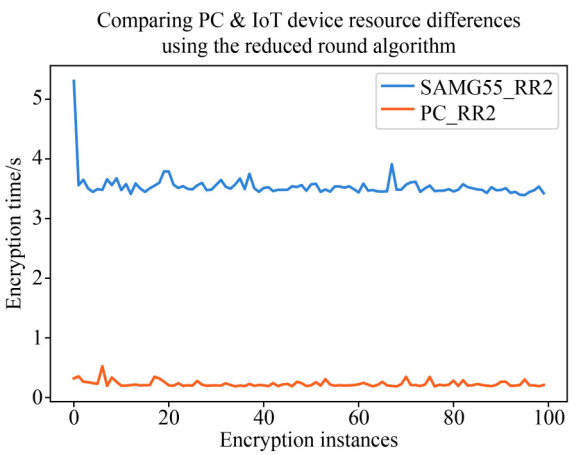

Fig. 2 A comparison of the PC and SAMG55 implementation of the reduced round algorithm

based on the AES to carry out data encryption at the IoT device's communication end using a SAMG55 microprocessor, following which the device is securely provisioned to a cloud platform as shown in Fig. 3. Related work and direction for future work is further detailed in Online Resources 1 and Online Resources 2.

Acknowledgements This research work was supported by Queen Mary University of London-Beijing University of Posts and Telecommunications (QMUL-BUPT) Joint Programme and the Tertiary Education Trust Fund (TETFUND) -via Plateau State University Bokkos-Nigeria.

Supporting information The supporting information is available online at journal.hep.cn and link.springer.com.

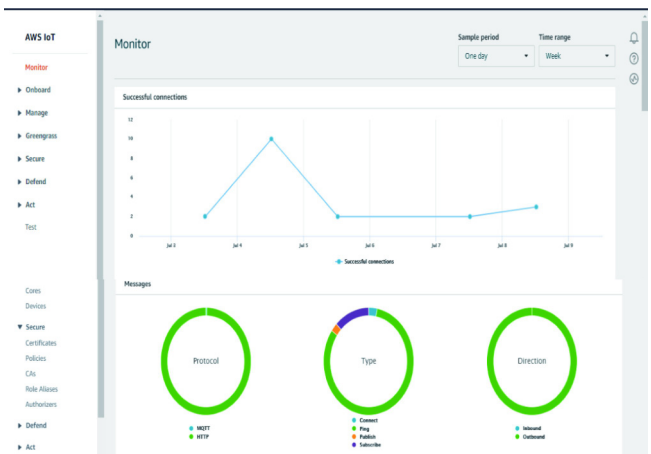

Fig. 3 Cloud-end view of provisioned IoT device and connection records

References

1. Aldossary S, Allen W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 2016, 7(4): 485–498
2. Ali O, Ishak M K, Wuttisittikulkij L, Maung T Z B. IoT devices and edge gateway provisioning, realtime analytics for simulated and virtually emulated devices. In: Proceedings of 2020 International Conference on Electronics, Information, and Communication (ICEIC). 2020, 1−5
3. Sahu A K, Sharma S, Tripathi S S, Singh K N. A study of authentication protocols in internet of things. In: Proceedings of 2019 International Conference on Information Technology (ICIT). 2019, 217−221
4. Deng H, Qin Z, Sha L, Yin H. A flexible privacy-preserving data sharing scheme in cloud-assisted IoT. IEEE Internet of Things Journal, 2020, 7(12): 11601–11611
5. Liu L, Wang H, Zhang Y. Secure IoT data outsourcing with aggregate statistics and fine-grained access control. IEEE Access, 2020, 8: 95057–95067
6. Mamvong J N, Goteng G L, Zhou B, Gao Y. Efficient security algorithm for power-constrained IoT devices. IEEE Internet of Things Journal, 2021, 8(7): 5498–5509
7. Jangra M, Singh B. Performance analysis of CLEFIA and present lightweight block ciphers. Journal of Discrete Mathematical Sciences and Cryptography, 2019, 22(8): 1489–1499