物聯網通訊與安全

第3章 物聯網安全性
IoT Security

蘇維宗 (Wei-Tsung Su)
suwt@au.edu.tw
564D

歷史版本

版本	說明	日期	負責人
v1.0	初版	2019/02/18	蘇維宗

設計與實作訊息佇列遙測之物對物安全傳輸協定

Design and Implementation of MQTT Thing-to-Thing Security Protocol

口試學生: 陳韋丞
指導教授: 蘇維宗　博士

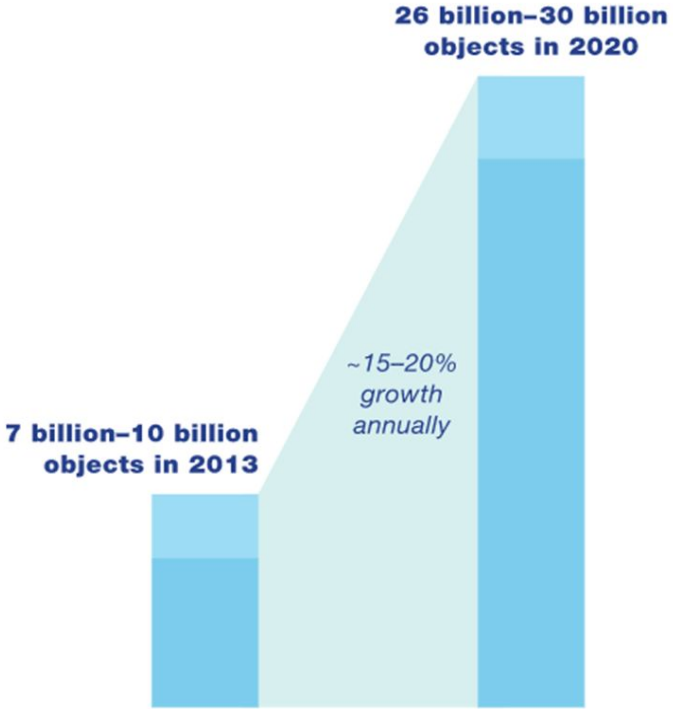
大綱

- **緒論**
- 相關研究
- 設計與實作MQTT-TTS
- 效能分析
- 結論與未來展望

物聯網

近年來，因為資訊與網路技術普及，使得物聯網的熱潮再度興起。

諸如智慧城市、智慧穿戴、工業4.0等應用都需要運用物聯網技術來達到其目的。

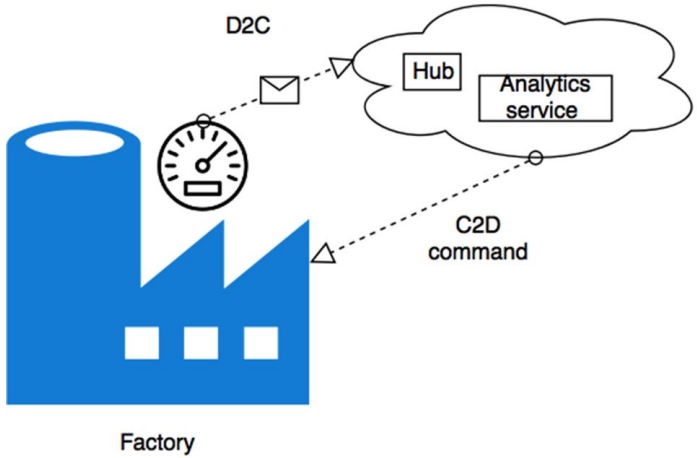


來源 : Mckinsey物聯網發展報告

物聯網帶來革命性的改變

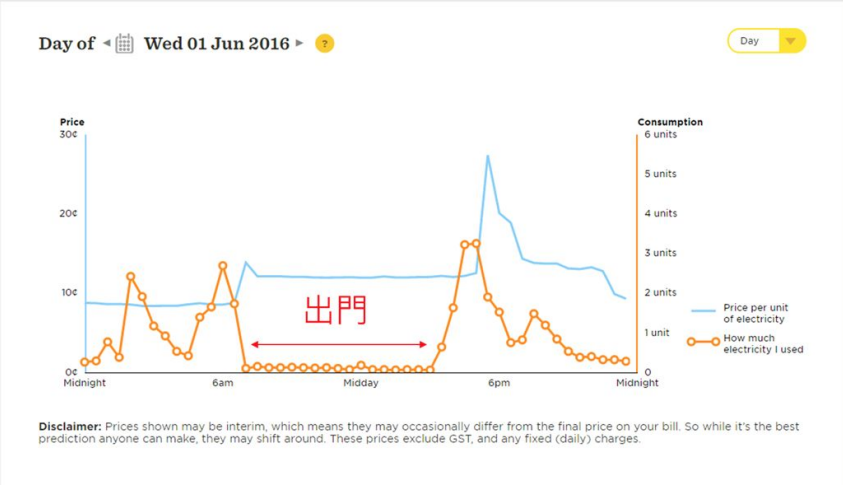
物聯網確實可以對許多應用帶來革命性的改變，因為聯網能力將資料上傳至雲端。

- Device to Cloud
- Cloud to Device
- 強大計算能力
- 大量的儲存體
- 遠端遙測



物聯網的利與弊

透過物聯網的技術可以改善我們生活，在安全機制未完善下也可能損害到我們的生活。



物聯網安全的挑戰

資料分享與安全兩難

常用的RSA、AES都不便於在物聯網環境分享資料

物聯網裝置的數量龐大

傳統存取控制清單(Access Control List，ACL)的擴充性低

沒有適合的身份認證機制來認證裝置

物聯網裝置的資源有限

裝置能力參差不齊

物聯網通訊協定安全機制與其限制(1/2)

目前有許多種通訊協定能應用在物聯網環境上，但然而沒有一個統一標準與規範，其中包含HTTP、MQTT、CoAP、AMQP 、DDS。

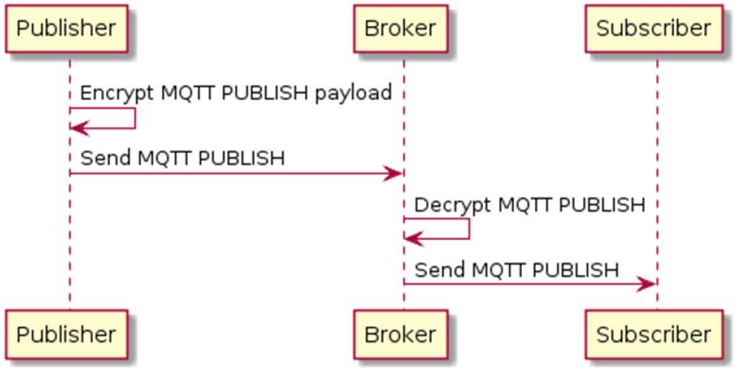
本論文選擇基於MQTT實作端點到端點的安全通訊協定的原因

- MQTT是眾多大廠物聯網雲端平台所支援的
- MQTT在開發者開發選擇中也是最熱門的選項之一

物聯網通訊協定安全機制與其限制(2/2)

MQTT目前提供了兩種安全機制用來保護傳輸的資料

- 傳輸層安全(Transport Layer Security，TLS)可以確保上傳至訊息代理人的資料受到保護。
- 權限控制清單(ACL)可以透過規則限制資料的發布與訂 閱。



研究貢獻

設計與實作MQTT Thing-to-Thing Security (MQTT-TTS)

- 採用物對物傳輸通道保護
- 彈性的資安機制選擇
- 支援密文屬性加密系統

模擬設計對於較弱IoT裝置可以透過委外運算來減少60~80%的運算時間並維持資料隱密性

大綱

- 緒論
- **相關研究**
- 設計與實作MQTT-TTS
- 效能分析
- 結論與未來展望

訊息佇列遙測傳輸協定(MQTT)

輕量級的通訊協定

訊息標頭大小只有 2 Bytes

透過發佈/訂閱模式來傳送訊息

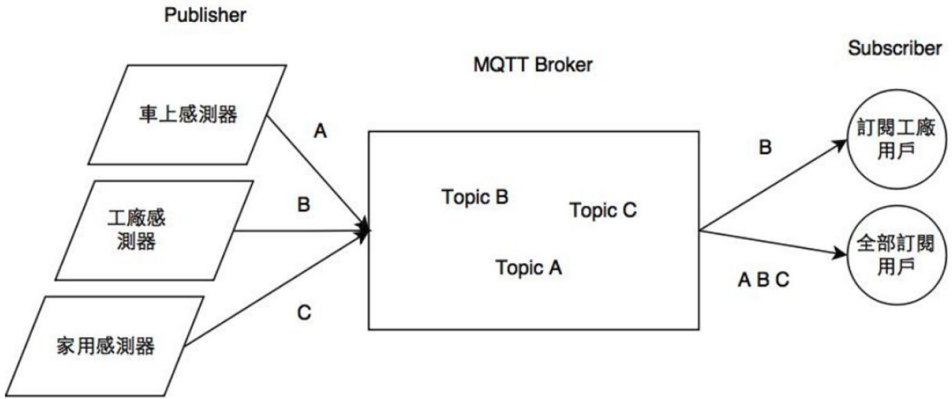
提供三種服務品質模式(Quality of Service，簡稱 QoS)

QoS代表發布者與代理人，或者代理人與訂 閱者之間的傳輸品質

具有最後遺囑機制

發佈/訂閱模式來傳送訊息(Pub/Sub)

Broker (訊息代理人): 將訊息配送到有訂閱相同主題的訂閱者
Publisher (資料發佈者): 將訊息送往訊息代理人
Subscriber (資料訂閱者): 向訊息代理人訂閱主題，並接收主題訊息



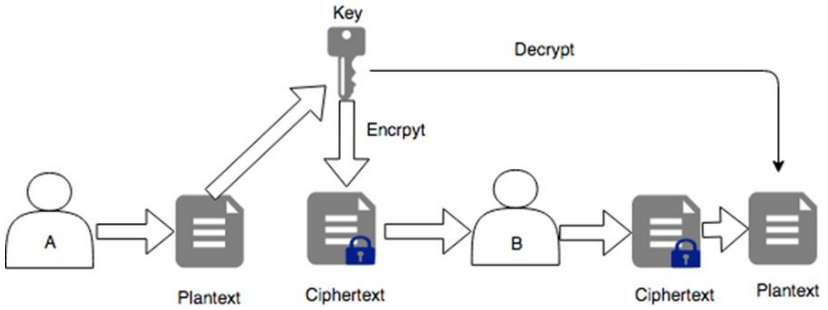
MQTT訊息標題格式

bit	7	6	5	4	3	2	1	0
byte 1	Message Type				DUP Flag	QoS Level		Ret
byte 2	Remaining Length							
Variable Header								
Payload								

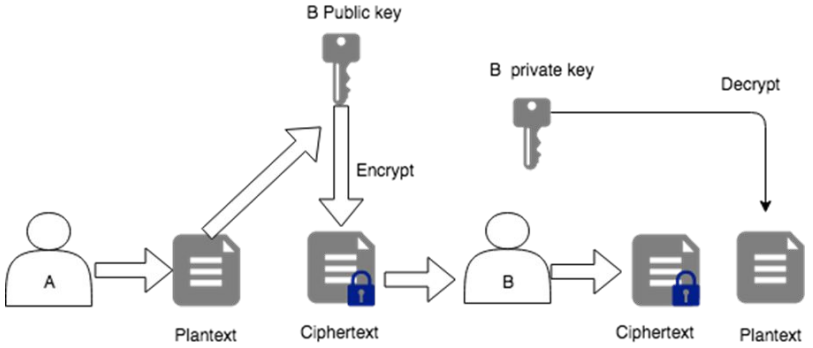
Question: 想想看如何透過這兩種加密演算法傳送資料給真理大學的所有資工系老師與學生 ？

傳統資料加密演算法

對稱式金鑰加密
(Symmetric-key algorithm)



非對稱式金鑰加密
(Asymmetric-key algorithm)



屬性加密(Attribute-Based Encryption，ABE)

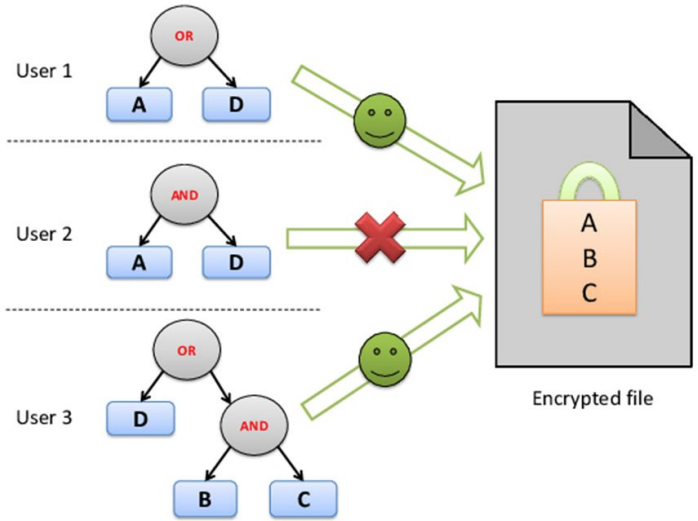
密鑰策略屬性加密(Key-Policy ABE，簡稱KP-ABE)

將存取政策放在金鑰

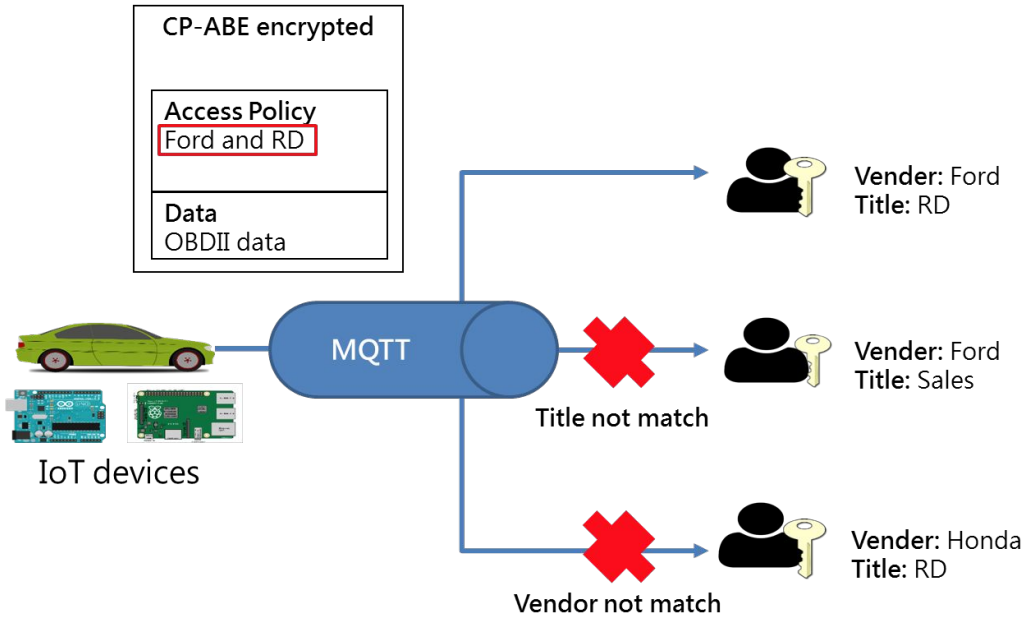
密文政策屬性加密(Ciphertext-Policy ABE，簡稱CP-ABE)

將存取政策放在秘文

密鑰策略屬性加密(KP-ABE)



密文政策屬性加密(CP-ABE)



CP-ABE四個基本的演算法

設置(Setup)

輸入一個安全參數，輸出一個公開金鑰 (簡稱PK)與一個主密鑰(簡稱MK)。

金鑰生成(MK,S)

輸入主密鑰MK 與使用者屬性S，然後輸出一個私密金鑰 (簡稱SK)

加密(PK,M,P)

輸入公開金鑰PK 與明文M 以及存取政策P，然後輸出密文CT

解密(PK,SK,CT)

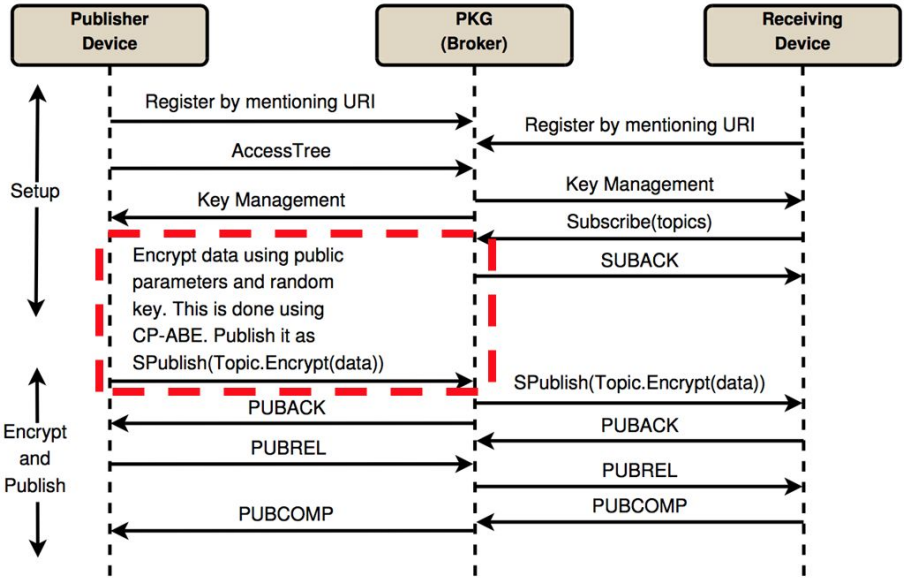
輸入公開金鑰PK 與密文CT 以及私密金鑰SK，當私密金鑰SK 裡的屬性S與密文CT 裡的存取策略P所描述之屬性相符合時才能 夠解密得出明文M。

相關論文

Meena Singh等人提出基於KP-ABE與CP-ABE演算法使得MQTT更為安全的SMQTT

將SMQTT內的Publish稱為SPublish，並用模擬方式來評估效能性。

Meena Singh等人將原始的MQTT Header所保留Message Type “0000”拿來使用。



相關論文(續)

Lochan Bisne等人使用動態S-BOX AES在應用層端加密資料最後在使用KP-ABE加密AES KEY，並運用MQTT傳輸協定傳送使得MQTT更安全並模擬效能實驗。

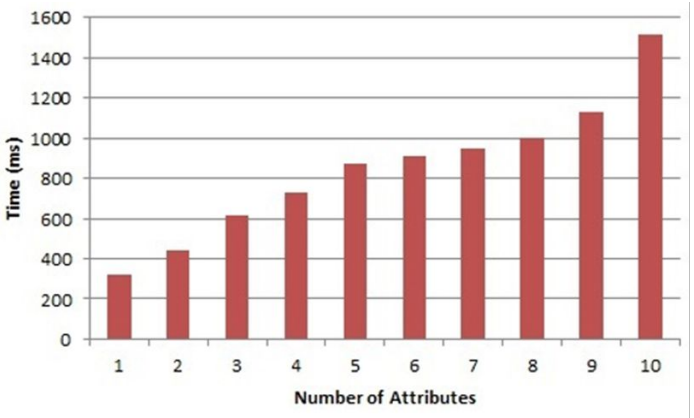


Fig. 4. Average Encryption Execution Time

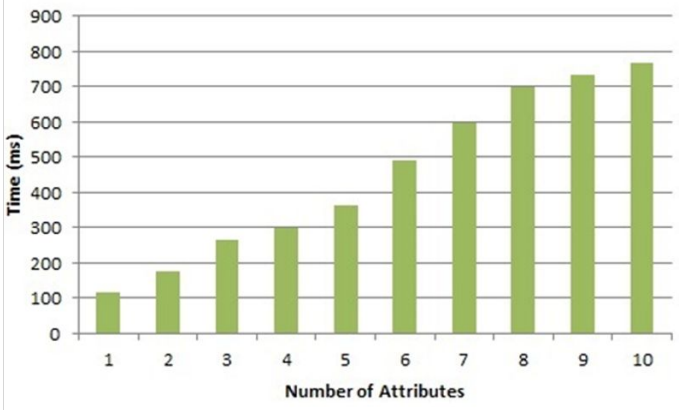
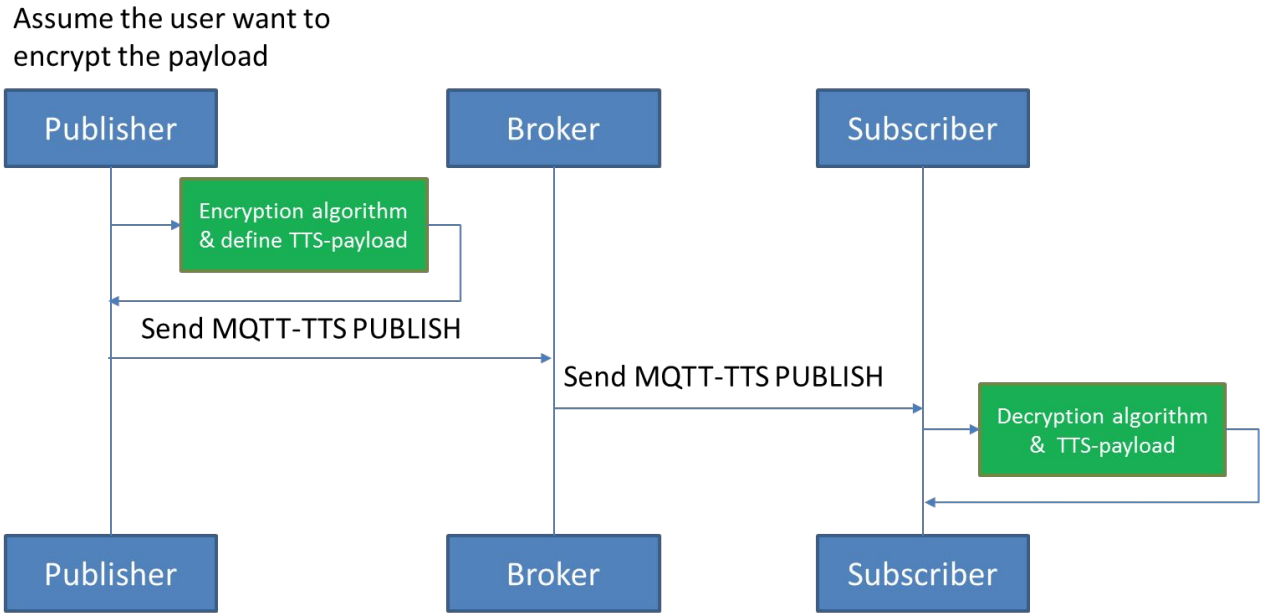


Fig. 5. Average Decryption Execution Time

大綱

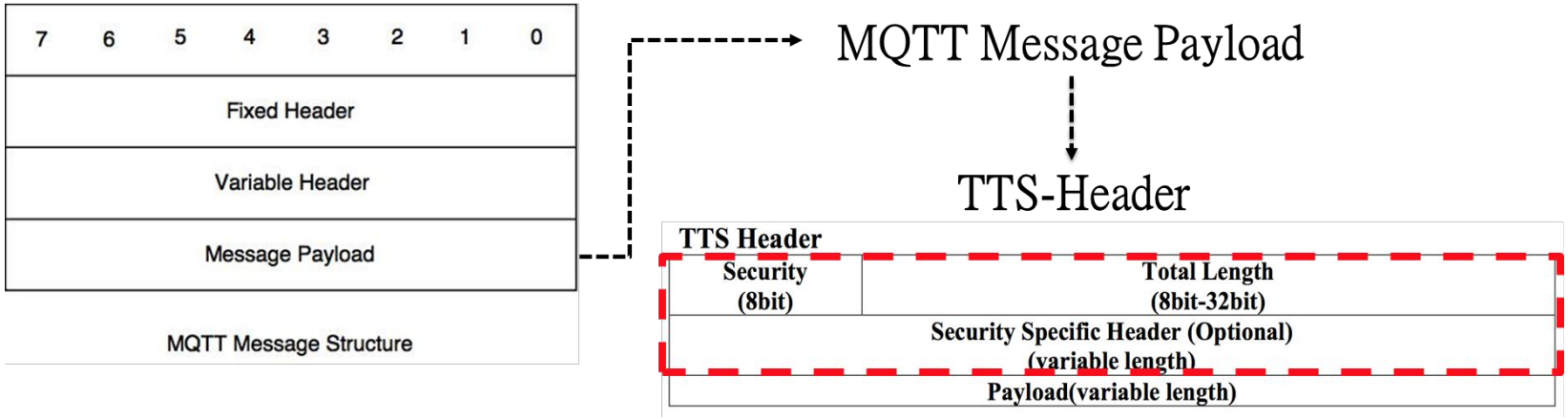
- 緒論
- 相關研究
- **設計與實作MQTT-TTS**
- 效能分析
- 結論與未來展望

MQTT-TTS循序圖


Assume the user want to encrypt the payload
Publisher
Broker
Subscriber
Encryption algorithm & define TTS-payload
Send MQTT-TTS PUBLISH
Send MQTT-TTS PUBLISH
Decryption algorithm & TTS-payload
Publisher
Broker
Subscriber

MQTT-TTS訊息格式(標頭格式)

- Security欄位是讓接收端知道傳送端採用的資訊安全機制
- Total Length欄位是用來檢測資料長度



MQTT-TTS訊息格式(Security)

Security為了讓MQTT-TTS能支援各式各樣的資訊安全機制，因此Security欄位長度設計為8 bits，最多可支援256種不同的方法。

例如

對稱式加密(DES, AES, …)
非對稱式加密(RSA, ESS, CP-ABE, …)
雜湊函數(MD5, SHA-2, SHA-3, …)

Bit(8)	加密演算法
00000000	DES 對稱式
00000001	3DES對稱式
00000010	AES 對稱式
00000011	ElGamal 非對稱式
00000100	RSA 非對稱式
00000101	ECC 非對稱式
00000110	CPABE 非對稱式
00000111	KPABE 非對稱式
00001000	HASH 雜湊
00001001	MD5雜湊
00001010	SHA-2雜湊
00001011	SHA-3雜湊
00001100	RIPEMD雜湊

MQTT-TTS訊息格式(Security-Specific Header)

不同資訊安全機制，可能需要提供額外的資訊

以AES為例，須提供加密模式、金鑰長度、IV類型。

AES Header

Mode-of-operation(4bit)	Crypto-key-length(8bit)	IV-Type(4bit)

Bit(4)	加密模式
0000	ECB
0001	CBC
0010	PCBC
0011	CFB
0100	OFB
0101	CTR
0110	GCM
0111	XTS

Bit(8)	加密金鑰長度
00000000	128
00000001	192
00000010	256

Bit(4)	IV-類型
0000	No-IV
0001	Fixed IV
0010	Counter IV
0011	Random IV
0100	Nonce-Generated IV

實作MQTT-TTS使用到的Open Source

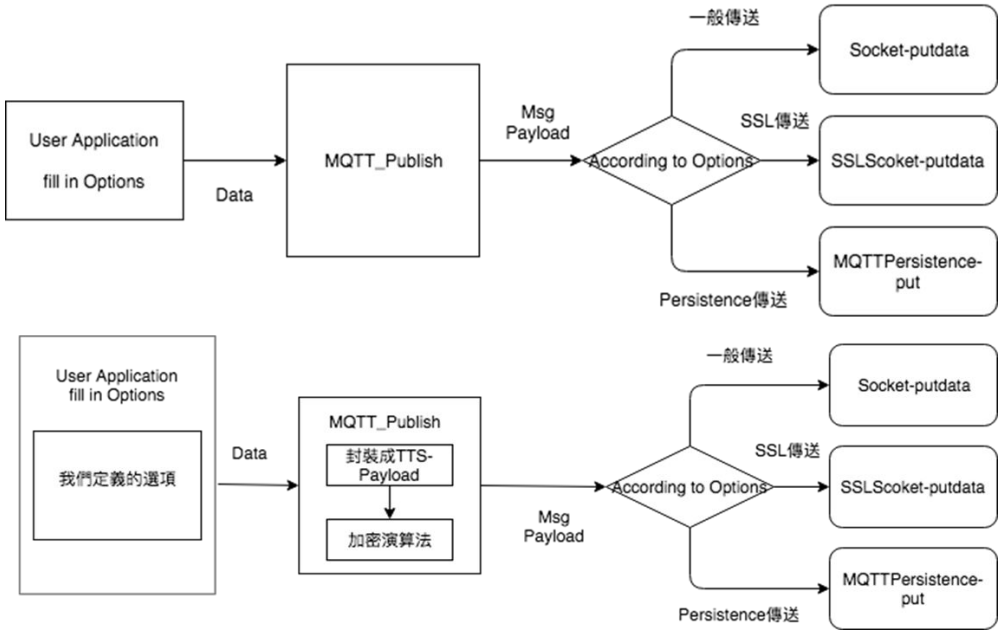
Eclipse MQTT-Paho (https://github.com/eclipse/paho.mqtt.c)

- Sync Pub/Sub
- Async Pub/Sub

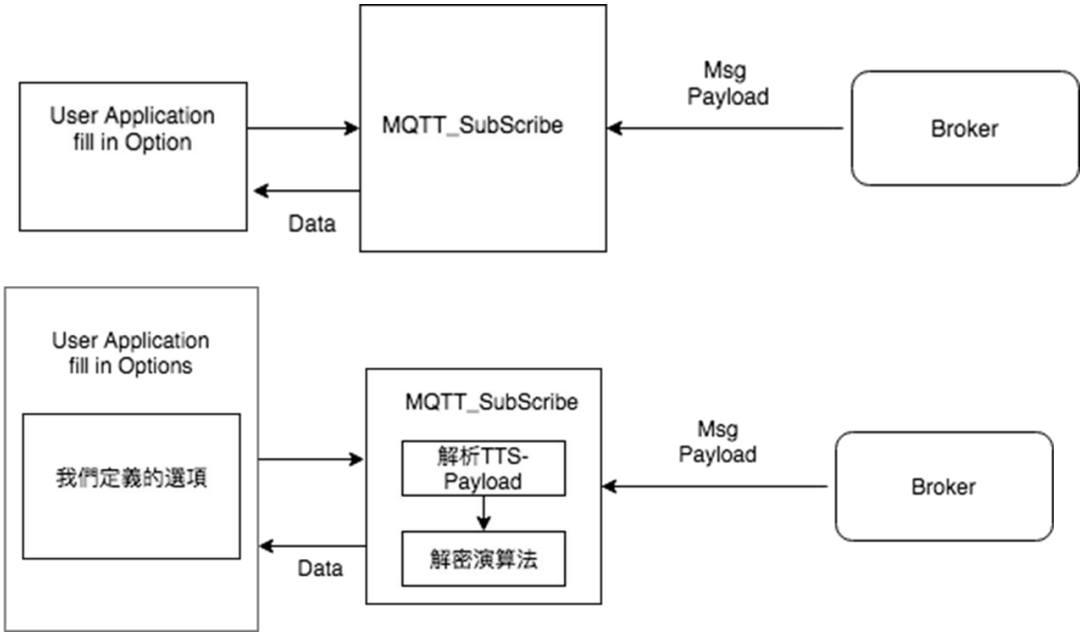
CP-ABE工具套件 (http://acsc.cs.utexas.edu/cpabe/)

- 基於Stanford所提供的Pairing-Based Cryptography Library
- Setup、Keygen、Enc、Dec

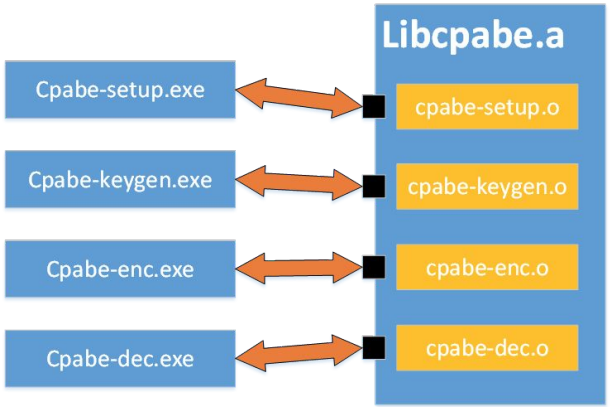
實作MQTT-TTS (資料發佈端)



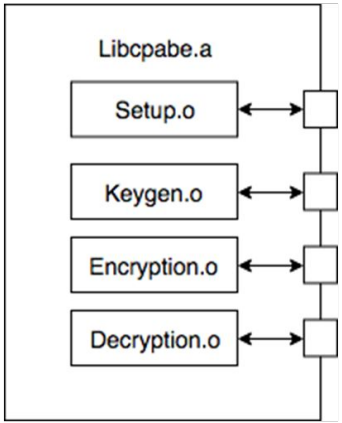
實作MQTT-TTS (資料訂閱端)



實作MQTT-TTS (CP-ABE函式庫)

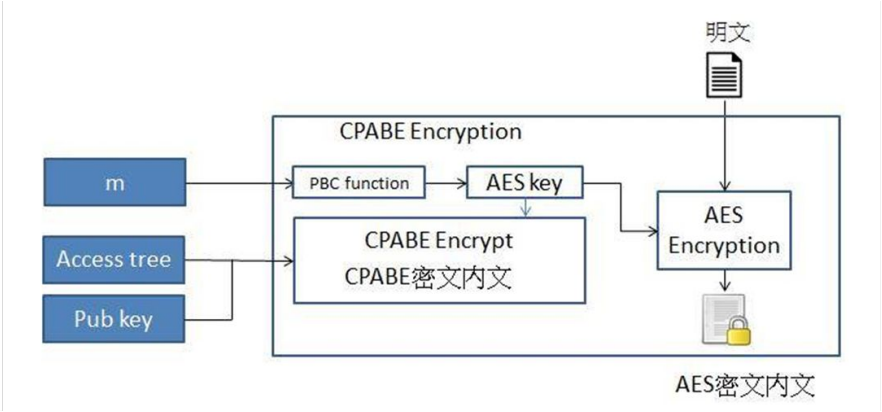


原始使用方法：執行檔，並且用CMD方式下指令與參數



更改後使用方法：讓其他程式透過API的窗口與這四個演算法連接

混合式CP-ABE密文格式



MQTT-TTS開放原始碼

基於開放原始碼授權，MQTT-TTS的原始碼也開源於GitHub

MQTT-TTS

https://github.com/beebit-sec/beebit-mqttc-sdk

CP-ABE SDK

https://github.com/beebit-sec/beebit-cpabe-sdk

大綱

- 緒論
- 相關研究
- 設計與實作MQTT-TTS
- **效能分析**
- 結論與未來展望

硬體規格

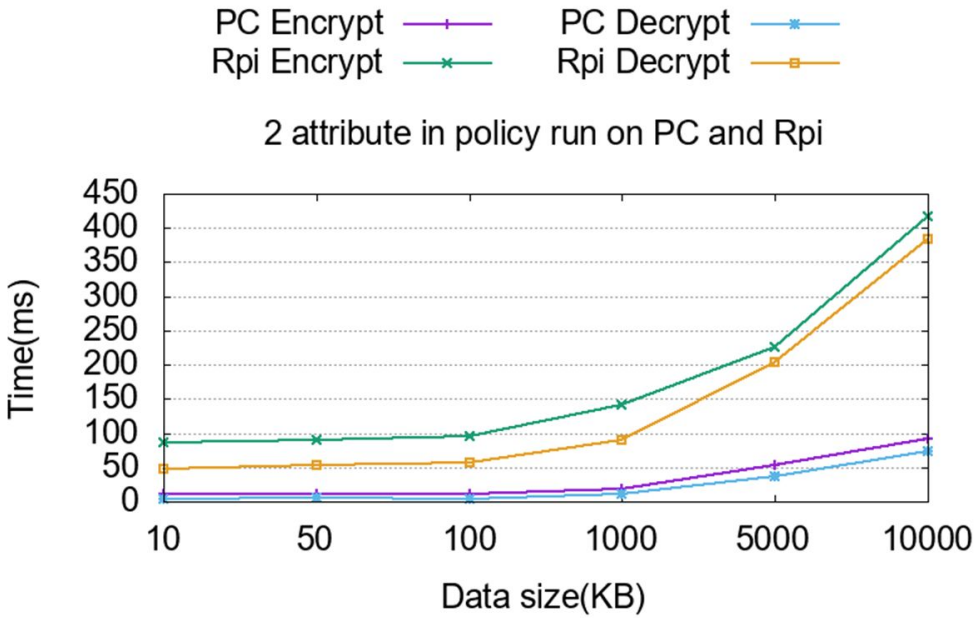
筆電 硬體規格

硬體設備	Intel® Core™ i5-3210M@3.10 GHz
記憶體	4 GB
作業系統	Windows 7, 32bit, ubuntu 16.04
MQTT	Eclipse Paho MQTT C v3

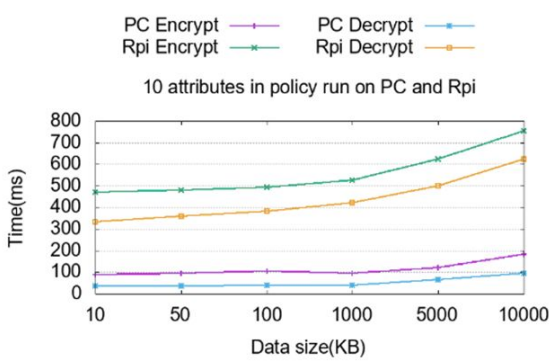
Rpi 3 硬體規格

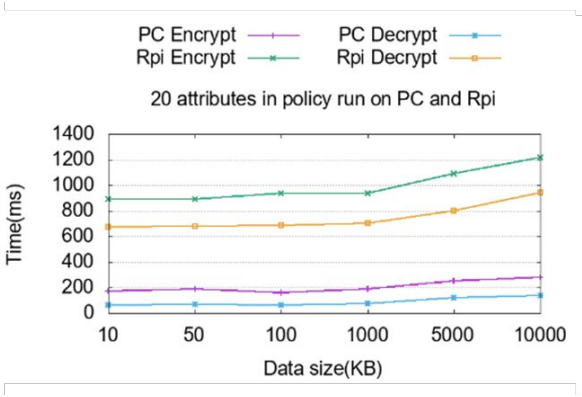
硬體設備	Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
記憶體	1 GB
作業系統	raspbian, 32bit
MQTT	Eclipse Paho MQTT C v3

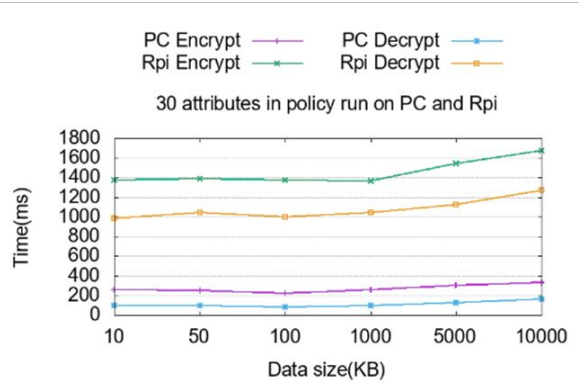
實驗一：資料大小與執行時間



實驗二:存取控制政策複雜度與執行時間

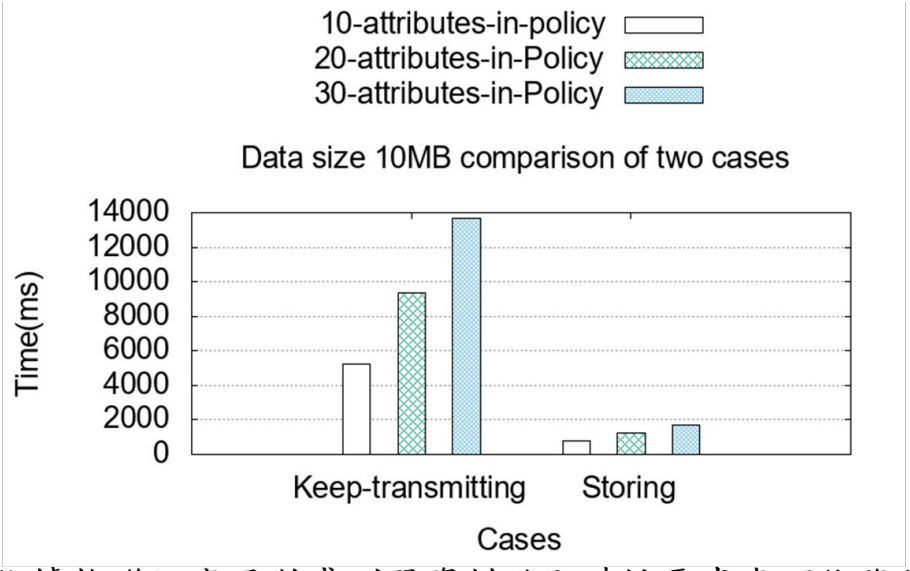






建議一 CP-ABE存取政策中使用適當屬性來進行加密，可以提高執行效率

實驗三:比較兩種傳送模式



建議二 依據物聯網應用對感測器資料的即時性需求盡可能降低傳送頻率

大綱

- 緒論
- 相關研究
- 設計與實作MQTT-TTS
- 效能分析
- **結論與未來展望**

結論與未來展望

結論

MQTT-TTS提供物對物安全通訊協定，避免資料在傳送途中被竊取

MQTT-TTS可根據裝置能力提供適合裝置運算能力的加密演算法

未來展望

如果能在演算法層級將 CP-ABE輕量化，可以讓更多運算資源有限的 IoT裝置使用

實作並加入更多種資訊安全機制

設計並實作委外運算的架構，使得較弱的 IoT裝置可以使用高複雜度加密 (如CP-ABE)

Q & A

Computer History Museum, Mt. View, CA