物聯網安全通訊標準與應用

陳志華[1,2]、林邦曄[3]、吳錦松[3]、蕭之彥[1]
[1]中華電信研究院智慧聯網研究所
[2]國立清華大學工業工程與工程管理學系
[3]中華電信研究院資通安全研究所
{chihua0826, bylin, chinsong, chihyenhsiao}@cht.com.tw

摘要

有鑑於介接各式各樣的物聯網終端設備和應用服務，並考量物聯網通訊的安全性，以提升傳輸資料的隱密性、完整性、不可否認性。本研究將參考國際物聯網標準作法，並提出一套三層式架構的物聯網系統，此系統包含有伺服器系統、閘道器、以及終端設備。其中，伺服器系統將可經由中介軟體服務設備與閘道器、終端設備通訊。閘道器和終端設備分別包含通訊模組、探索模組、連線管理模組、資訊安全模組、登錄模組、控制模組、通知模組、設定模組、以及資料模組，以廣泛應用在各種物聯網服務。本研究運用探索模組、連線管理模組、通訊模組，將可探索出網路內的其他終端設備，並與探索到的終端設備建立連線。此外，本研究設計控制模組、資料模組，將可依據共通的控制指令和應用資料內容，對各個終端設備進行控制和管理，並可取得每個終端設備的即時狀態和資訊。並且，本研究設計推播服務設備和通知模組，將可建立非連線導向的單向推播機制，主動將訊息發送至目的設備。最後，在資訊安全考量下，設計資訊安全設備和資訊安全模組，將可進行雙向授權和認證，以確認連線設備可被允許的存取控制列表，並且結合加解密技術保護資料傳輸。

關鍵詞：物聯網、閘道器、探索模組、資訊安全模組、雙向認證

The Standards and Applications of Secure Communications for Internet of Things

Chi-Hua Chen[1,2] Bon-Yeh Lin[1] Chin-Song Wu[1] Chih-Yen Hsiao [1]
[1]Telecommunication Laboratories, Chunghwa Telecom Co., Ltd.
[2]Department of Industrial Engineering and Engineering Management, National Tsing Hua University
{chihua0826, bylin, chinsong, chihyenhsiao}@cht.com.tw

Abstract

Due to the connections and communications of a variety of Internet of Things (IoT) devices, this study proposes a three-tier IoT system which includes servers, gateways, and

devices. The servers can communicate with gateways and devices through middleware server. The gateways and devices include communication module, discovery module, connection management module, security module, registry module, control module, notification module, configuration module and data module for a variety of IoT services and applications. In this study, the discovery module, connection management module and communication module can be used to discover the devices in the local area network and to connect with the discovered devices. Furthermore, common control signals and data schemes can be defined and implemented in the control module and data module to retrieve the real-time information and status of each device for device control and management. Moreover, this study designs a push service server and notification module to obtain a connectionless single-direction push mechanism for actively publishing messages to a target device. Finally, a security server and security modules are designed to perform mutual authorization and authentication according to access control lists and to combine with encryption and decryption techniques for the protection of data transmission.

Keywords: Internet of Things, Gateway, Discovery Module, Security Module, Mutual Authentication

壹、前言

近年來，隨著資通訊技術和行動感測技術的蓬勃發展，物聯網(Internet of Things, IoT)也隨之興起。感測設備可以即時感知環境資訊，並經由物和物(Machine to Machine, M2M)之間的互相通訊，讓各種應用設備能夠更智慧，得以自動化分析環境資訊後產生和執行相關的決策，如：掃地機器人、無人駕駛汽車等。其中，管理大師麥克波特(Michael Eugene Porter)則點出物聯網主要具有 4 個階段：(1) 監看、(2) 控制、(3) 最佳化、以及(4) 自主性，並且經由物聯網技術洞察使用者的行為和偏好，以及設備的使用狀態，進而設計出更具使用者經驗的新產品和預測性維修[7, 8]。

然而，雖然資通訊技術已經可以為設備間建立好網路基礎環境，但要做到 M2M 的技術，傳統的作法仍需由廠商之間互相協調和談委合作協議，再依合作廠商的資料模型和控制指令來建立通訊。而這個運作方式，一旦更換合作廠商則全部的資料模型和控制指令則會面臨修改的困境，將造成研發成本增加、產品上市時間的延宕等問題。因此，近年來開始有許多物聯網聯盟(如：AllSeen、開放連線基金會(Open Connectivity Foundation, OCF)、以及 oneM2M 等)開始針對 M2M 和 IoT 的通訊來制定共通的資料模型和控制指令，讓企業間可以更快串連各種不同廠商的設備，打造物聯網生態系統。

有鑑於此，本研究將參考國際物聯網聯盟標準的設計以提出一套三層式架構的物聯

網系統，包含有伺服器系統、閘道器、以及終端設備。並讓此系統能整合各個物聯網標準，以介接各個物聯網設備和生態系統，快速打造各種物聯應用服務。

此論文以下分為五個章節，在第二節中將探討物聯網標準和閘道器相關的研究背景。第三節說明物聯網系統的設計原理和實作。第四節提供物聯網系統的個案展示。最後一節則說明此論文之結論與未來研究方向。

貳、文獻探討

目前較熱門的物聯網標準主要有 AllJoyn、OCF、以及 oneM2M 三套，本節將分述這三套標準的運作方式。

2.1 AllJoyn

在 Qualcomm 公司的主導下，組織了 AllSeen 物聯網聯盟，開始制定 AllJoyn 協定，規範 AllSeen 聯盟的 M2M 控制指令和資料模型。AllJoyn 協定主要包含四個層次：AllJoyn 路由(Router)、AllJoyn 核心函式庫(Core Libs)、AllJoyn 框架(Frameworks)、以及 AllJoyn 應用層(Application Layer)，分述如下[1]。

2.1.1 AllJoyn 路由

AllJoyn 路由主要用來傳送資料予另一個 AllJoyn 設備，以及接收來自另一個 AllJoyn 設備的資料。

2.1.2 AllJoyn 核心函式庫

```
<node xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.allseenalliance.org/schemas/introspect.xsd">

   <interface name="org.alljoyn.Stream">
      <property name="Version" type="q" access="read"/>
      <method name="Open"/>
      <method name="Close"/>
   </interface>

   <interface name="org.alljoyn.Stream.Port">
      <property name="Version" type="q" access="read"/>
      <property name="Direction" type="y" access="read"/>
      <property name="Capabilities" type="a(sa{sv})" access="read"/>
```

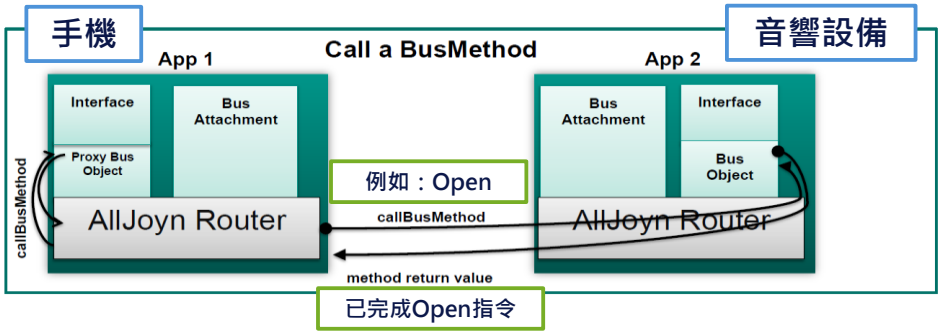
Type定義：
- s和v：字串
- q：數字
- a：陣列
- y：binary

圖一：AllJoyn 協定之 org.allseen.media.audio 介面[1]

AllJoyn 核心函式庫包含有探索和廣播函式庫(Discovery & Advertisement APIs)、連線函式庫(Connection APIs)、介面函式庫(Interface APIs)、以及安全函式庫(Security APIs)。各個 AllJoyn 設備可依其應用功能實作不同的介面函式庫(即資料模型)，如：音響介面(org.allseen.media.audio，如圖一所示)，並可以透過探索和廣播函式庫來搜尋網路內的 AllJoyn 設備或自身設備加入至網路時可廣播告知其他 AllJoyn 設備，再經由連線函式庫建立連線。此外，亦可結合安全函式庫建立安全的連線和通訊[1]。

2.1.3 AllJoyn 框架

包含有登錄、通知、控制、設定等基本功能，並且各個 AllJoyn 設備可依其應用功能實作不同控制指令，例如：燈泡(Lighting)、音響(Audio)等。當欲控制 AllJoyn 設備時，將可經由此共通的控制指令來操作和控制，例如：呼叫 Open 方法來開啟 AllJoyn 音響設備(如圖二所示)[1]。



圖二：控制 AllJoyn 音響設備[1]

2.1.4 AllJoyn 應用層

AllJoyn 應用層為開發者開發應用程式的層次，可呼叫底層的 AllJoyn 框架和 AllJoyn 核心函式庫以介接其他 AllJoyn 設備[1]。

然而，AllJoyn 協定雖然規範了共通的資格模型和控制指令，但此協定主要僅著重於物聯網架構三層中的感測層而已，無法連結至網路層和應用層。因此，此協定僅適用於區網內執行，無法連結至雲端伺服器。

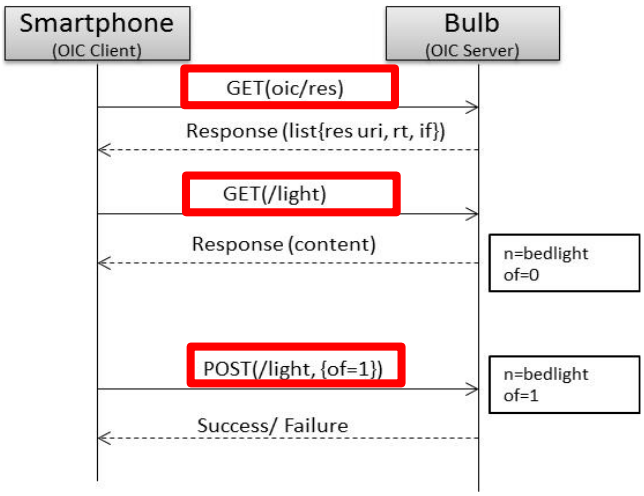
2.2 OCF

在 Intel 公司的主導下，組織了開放連線基金會之物聯網聯盟，開始制定 OCF 協定(前身為 OIC (Open Interconnect Consortium))，規範 OCF 聯盟的 M2M 控制指令和資料模型。

OCF 協定主要包含兩個層次：服務層(Service Layer)和基礎層(Base Layer)，分述如下[1]。

2.2.1 服務層

服務層包含有設備管理(Device Management)、識別子和定址(ID & Addressing)、資源模型(Resource Model)、以及 CRUDN 功能(Create, Retrieve, Update, Delete, and Notify)。各個 OCF 設備可依其應用功能實作不同的資源模型(即資料模型)和 CRUDN 功能(即控制指令)等。當欲控制 OCF 設備時，將可經由此共通的資料模型和控制指令來操作和控制，例如：呼叫 POST 方法，帶入資料模型參數(/light, {of=1})來開啟 OCF 燈泡設備(如圖三所示)[6]。



圖三：控制 OCF 燈泡設備[6]

2.2.2 基礎層

基礎層包含有探索功能(Discovery)、訊息功能(Messaging)、以及安全功能(Security)。各個 OCF 設備可透過探索功能來搜尋網路內的 OCF 設備或自身設備加入至網路時可廣播告知其他 OCF 設備，再經由訊息功能傳送訊息予其他 OCF 設備。此外，亦可結合安全功能建立安全的連線和通訊[6]。

然而，OCF 協定雖然規範了共通的資格模型和控制指令，但此協定與 AllJoyn 協定似乎，主要僅著重於物聯網架構三層中的感測層而已，無法連結至網路層和應用層。因此，此協定僅適用於區網內執行，無法連結至雲端伺服器。

2.3 oneM2M

在歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)和第三

代合作夥伴計劃(3rd Generation Partnership Project, 3GPP)等標準組織主導下，組織了oneM2M 物聯網聯盟，開始以 ETSI SmartM2M 標準為基礎制定 oneM2M 物聯網標準，規範 oneM2M 聯盟的 M2M 框架。其中，主要可以依物聯網架構三個層次(即感測層、網路層、以及應用層)分別制定和規範資料模型和控制指令，包含有三個角色：應用服務節點(Application Service Node, ASN)、中介節點(Middle Node, MN)、以及基礎設施節點(Infrastructure Node, IN)，分述如下[2]。

2.3.1 應用服務節點

應用服務節點包含有應用元件(Application Entity, AE)和通用服務元件(Common Service Entity, CSE)，為一般感測器、終端設備的角色。其中，通用服務元件主要將規範共通的資料模型和控制指令，並在此元件中提供通訊管理、資料管理與儲存、設備管理、探索服務、群組管理、定址、網路服務、註冊、安全管理、付費機制、以及訂閱與通知等功能。應用服務節點之應用元件主要依終端設備所要提供的功能實作此應用元件，例如：燈泡功能、音響功能等。再經由通用服務元件經由具象狀態傳輸(Representational State Transfer, REST)[3]、訊息序列遙測技術(Message Queuing Telemetry Transport, MQTT)[4]、受限應用程式協定(Constrained Application Protocol, CoAP)[5]、或 WebSocket 技術與中介節點或基礎設施節點進行介接。

2.3.2 中介節點

中介節點為閘道器的角色，包含有應用元件和通用服務元件。可於閘道器的應用元件實作資料彙整和分析功能，經由通用服務元件介接應用服務節點和基礎設施節點，可將應用服務節點的資料轉送到基礎設施節點，並可接收基礎設施節點傳送之控制指令，並將該控制指令轉送予應用服務節點。

2.3.3 基礎設施節點

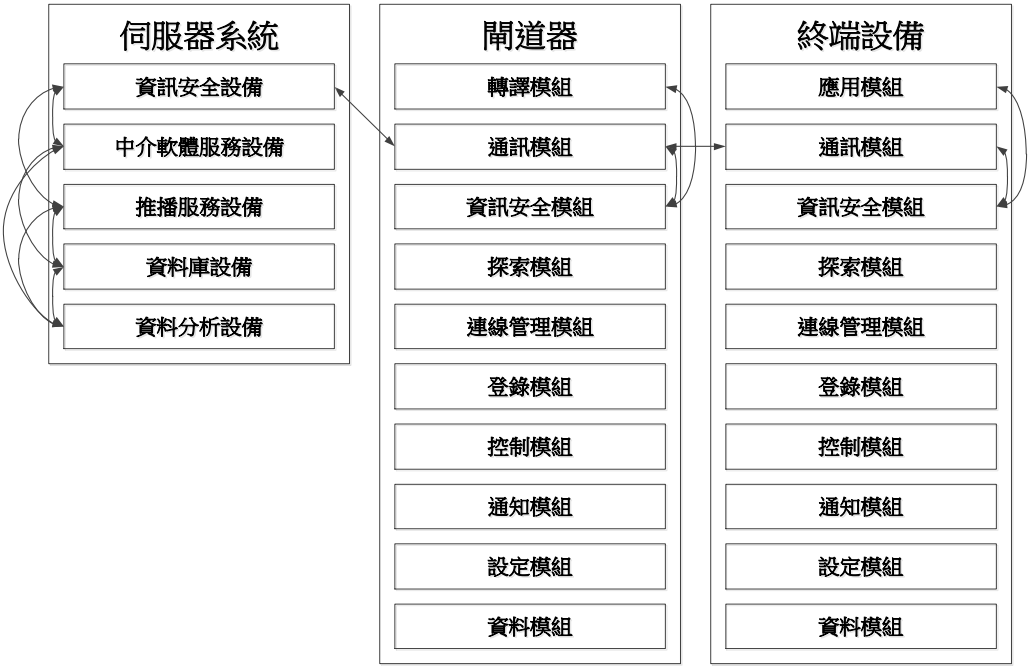
基礎設施節點為電信運營商或服務供應商的伺服器，包含應用元件和通用服務元件。基礎設施節點的應用元件主要可以收集資料和分析資料，並且可整合巨量資料技術，針對來自各種異質資料來源的物聯網大數據進行分析和預測，並依不同的情境產生控制指令和經由通用服務元件傳送控制指令予中介節點或應用服務節點，以達到管理大師麥克波特所述之監看、控制、最佳化、以及自主性。

oneM2M 標準雖然規範了物聯網架構三層，但 oneM2M 標準在運作上將需求較高的運算需求，無法適用於低階的設備。此外，現階段設備廠商仍主要採用 AllJoyn 和 OCF 甚於 oneM2M，故在物聯網發展上可參考 oneM2M 框架，並介接 AllJoyn 和 OCF 等物

聯網標準和其他非標準的設備，以擴增市場佔有率。

參、物聯網系統之設計與實作

本研究提出一套三層式架構的物聯網系統，此系統包含有(1) 伺服器系統、(2) 閘道器、以及(3) 終端設備(如圖四所示)，並以健康照護應用為例進行說明，各功能元件分述如下。



圖四：物聯網系統架構圖

3.1 伺服器系統

伺服器系包含(1) 中介軟體服務設備、(2) 推播服務設備、(3) 資料庫設備、(4) 資料分析設備、以及(5) 資訊安全設備。

- **中介軟體服務設備**

中介軟體服務設備包含通訊模組、處理模組、以及中介軟體模組。通訊模組可介接 Ethernet 網路介面，而中介軟體模組可提供網路服務、簡易物件存取協定(Simple Object Access Protocol, SOAP)、REST、WebSocket、CoAP 等中介軟體程式。在本研究中，服務提供者可先將應用服務部署到中介軟體服務設備，建立 REST 網路服務可供閘道器存取。當閘道器發出加密之 REST 網路服務要求給伺服器系統時，將先由資訊安全設備進

行解密，再經由中介軟體服務設備的通訊模組收到 REST 網路服務要求，可由處理模組分析其要求，並傳遞給 REST 中介軟體模組進行處理，再把處理後的結果經由通訊模組傳送予資訊安全設備，再由資訊安全設備進行加密後回傳予閘道器。

- **推播服務設備**

推播服務設備包含通訊模組、處理模組、推播模組、以及儲存模組。在本研究中，推播服務設備可採用 MQTT 技術進行實作。當閘道器發出連線、訂閱、發佈、離線的訊息要求給伺服器系統時，將先由資訊安全設備進行解密，再把解密後的訊息傳送予推播服務設備，推播服務設備再經由處理模組分析訊息要求內容。其中，每一個閘道器和終端設備皆具備一個唯一的識別碼，可以此識別碼作為主題，並訂閱此主題；完成訂閱後，推播服務設備欲推播訊息予閘道器或終端設備時，即可以發佈到該閘道器或該終端設備唯一識別碼的主題名稱上，將可經由通訊模組將此訊息傳遞給訂閱該主題的閘道器或連結閘道器的終端設備。此外，主題的設計上，也可以採用其他的命名方式，例如：「最新消息」之主題名稱，之後所有的閘道器和終端設備皆訂閱「最新消息」主題；當有消息要發佈給所有閘道器和終端設備時，可以發佈到「最新消息」主題上，將可把此訊息發佈到所有閘道器和終端設備。在訊息發佈和接受上也可以訂定不同的服務品質，可以分別只送一次、至少一次、最多一次等設計。

- **資料庫設備**

資料庫設備包含通訊模組、儲存模組、以及同步模組。在本研究中，物聯網資料庫設備可採用結構化查詢語言(Structural Query Language, SQL)(如：Microsoft SQL Server、MySQL 等)或 NoSQL (如：HBase、MongoDB 等)資料庫技術實作，並可於同步模組中設定不同物聯網資料庫設備的主從關係以進行資料同步。資料庫設備可經由通訊模組傳送和接收中介軟體服務設備、推播服務設備的資料，並可將收到的資料儲存到儲存模組中，以提供新增、修改、查詢、刪除等功能。

- **資料分析設備**

資料分析設備包含通訊模組、儲存模組、以及資料處理模組。在本研究中，資料處理模組可採用 R 語言和開放套件實作，建立統計資料處理模組、機器學習資料處理模組、深度學習資料處理模組、多目標決策資料處理模組。資料分析設備可經由通訊模組接收中介軟體服務設備的要求，並經由通訊模組建立與資料庫設備連線，並向資料庫設備取得資料。資料分析設備可將從資料庫設備取得的資料儲存於儲存模組中，並可由資料處理模組將資料從儲存模組中取出，並進行資料分析，再把分析完結果回傳予物聯網中介軟體服務設備。例如：統計資料處理模組可計算同一個血壓計物聯網終端設備，特定期間內的收縮壓值和舒張壓值之平均值、標準差、最大值、最小值等。

- **資訊安全設備**

資訊安全設備包含通訊模組、加解密模組、以及金鑰模組所組成。在研究中，加解密模組得採用 RSA (Rivest, Shamir, and Adleman)、進階加密標準(Advanced Encryption Standard, AES)、資料加密標準(Data Encryption Standard, DES)、三重資料加密演算法(Triple Data Encryption Standard, 3DES)等方法實施，金鑰模組可採用對稱式金鑰或非對稱式金鑰等方式實作。資訊安全設備可經由通訊模組與中介軟體服務設備、推播服務設備、閘道器、以及終端設備介接。資訊安全設備可經由加解密模組運用金鑰模組之金鑰進行資料加密或解密，再把處理後資料經由通訊模組轉送。例如：資訊安全設備、閘道器、終端設備可具備相同的金鑰，採用對稱式金鑰和 AES 加解密模組進行加解密。資訊安全設備亦可具備私密金鑰和公開金鑰，閘道器可採用資訊安全設備的公開金鑰和 RSA 演算法進行非對稱式金鑰的加解密，以確保資訊只有物聯網資訊安全設備能以其私密金鑰解密和讀取。

3.2 閘道器

閘道器係由(1) 通訊模組、(2) 轉譯模組、(3) 探索模組、(4) 連線管理模組、(5) 資訊安全模組、(6) 登錄模組、(7) 控制模組、(8) 通知模組、(9) 設定模組、以及(10) 資料模組所組成。在本研究中，終端設備可以是 Ethernet 網路閘道器或小基地台(Femto Cell 或 Small Cell)或 WiFi 存取熱點或 ZigBee 網路閘道器，並可同時連結 Ethernet、蜂巢網路(全球行動通訊系統(Global System for Mobile Communications, GSM)、通用封包無線服務(General Packet Radio Service, GPRS)、通用行動通訊系統(Universal Mobile Telecommunications System, UMTS)、長期演進技術(Long Term Evolution, LTE))、WiFi、藍牙(Bluetooth)、ZigBee 等，可將健康照護終端設備(如：血壓計、心率計、血糖計、體脂計、體重計等)即時資訊回傳至物聯網伺服器系統，並可由物聯網伺服器系統發出訊息控制健康照護終端設備。

- **通訊模組**

閘道器可具有 Ethernet 通訊模組、蜂巢網路通訊模組、WiFi 通訊模組、藍牙通訊模組、ZigBee 通訊模組、電力線通訊(Power Line Communication, PLC)通訊模組，可同時介接不同的網路介面，並可經由 Ethernet 通訊模組或蜂巢網路通訊模組與物聯網伺服器系統通訊，可經由 WiFi 通訊模組或藍牙通訊模組或 ZigBee 通訊模組或 PLC 通訊模組傳送和接收健康照護終端設備資料。

- **轉譯模組**

轉譯模組可傳送和接收不同通訊模組的資料，並將接收到的資料轉譯成另一個網路介面和協議所接受的資料模型再進行轉送。例如：經由 WiFi 通訊模組接收血壓計物聯

網終端設備加密的資訊(如：收縮壓值、舒張壓值、心率值等)時，將先傳送予資訊安全模組進行解密，再將解密後的資料由轉譯模組轉譯為物聯網中介軟體服務設備可支援的資料格式和傳輸協議(如：REST 等)，之後再把訊息傳送予資訊安全模組進行加密並經由 Ethernet 通訊模組或蜂巢網路通訊模組傳送予物聯網中介軟體服務設備。

- **探索模組**

探索模組運用資料模組可發送和接收特定資料內容的 TCP 或 UDP 單播或群播或廣播封包，經由封包傳遞探索網路內符合要求的物聯網終端設備。在本研究中，物聯網閘道器採用 UDP 廣播封包的方式，經由通訊模組發出探索封包給網路內所有的設備，並在探索封包中表述欲探索的標的物(如：血壓計)；當其他物聯網終端設備收到探索封包後，將解析封包內容和判斷自身設備是否為欲探索的標的物，如果接收到封包的物聯網終端設備是血壓計的話，將回覆訊息(如：IP 和設備識別碼)予物聯網閘道器的探索模組，如果接收到封包的物聯網終端設備不是血壓計的話，則不做任何回覆。可經由探索模組探索到網路內符合標的的終端設備。

- **連線管理模組**

連線管理模組對已探索到的物聯網終端設備發出要求建立連線，並監測連線品質，確保連線狀態，且可在斷線時，自動重新建立連線。在本研究中，可經由 WiFi 通訊模組以 WiFi 無線網路探索到血壓計終端設備，在探索模組中取得血壓計終端設備的 IP，再以該 IP 資訊建立 TCP 或 UDP 連線，並週期性發出封包測試該連線存活與否，如果連線中斷可由連線管理模組自動重新連線，並在連線失敗複數次後得停止重新連線。

- **資訊安全模組**

資訊安全模組包含有加解密裝置、以及金鑰裝置，可經由加解密裝置運用金鑰裝置之金鑰進行資料加密或解密，再把處理後資料經由通訊模組轉送。在本研究中，加解密裝置可採用 RSA、AES、DES、3DES 等方法實作，金鑰裝置可採用對稱式金鑰或非對稱式金鑰等方式實作。資訊安全模組可經由加解密裝置運用金鑰裝置之金鑰進行資料加密或解密，再把處理後資料經由通訊模組轉送。例如：資訊安全設備、閘道器資訊安全模組、終端設備資訊安全模組可具備相同的金鑰，採用對稱式金鑰和 AES 加解密模組進行加解密。資訊安全模組亦可具備私密金鑰和公開金鑰，閘道器資訊安全模組可採用私密金鑰和 RSA 演算法進行非對稱式金鑰的簽章，以確保資訊確實是由該閘道器資訊安全模組所簽署。

- **登錄模組**

登錄模組可在設備加入到網路時，可結合設定模組的資訊發送特定資料內容的 TCP 或 UDP 單播或群播或廣播封包，告知網路中其他設備新加入設備的相關資訊。在本研

究中，閘道器加入到網路時，可以向設定模組取得閘道器屬性資料(包含：含可支援的通訊模組、可支援的資料模組、廠牌、程式版本等)，並將此屬性資料以 UDP 封包廣播給網路內其他的終端設備。

- **控制模組**

控制模組可結合資料模組，依不同的應用和服務產生不同的控制訊號和資料模型內容，再經由通訊模組傳送控制訊號至其他終端設備，以達到控制需求。在本研究中，可由通訊模組接收到來自物聯網伺服器系統的 MQTT 訊息時，可經由轉譯模組解讀 MQTT 訊息的內容，再進行轉譯並運用控制模組依對應的資料模組將控制訊息轉為可控制終端設備的訊號(如：血壓計的訊號包含有開始量測、停止量測)和資料模型(如：血壓計的資料模型包含有收縮壓值、舒張壓值、心率值)。

- **通知模組**

通知模組可建立非連線導向的單向推播訊息傳遞通道，可主動發送訊息予其他終端設備，或可接收其他終端設備傳送的訊息。在本研究中，當閘道器相關屬性改變時，可運用通知模組經由通訊模組發出 UDP 廣播封包，告知網路內其他終端設備。例如：閘道器程式版本更改時，可經由通知模組進行通知。

- **設定模組**

設定模組可設定閘道器的相關屬性，包含可支援的通訊模組、可支援的資料模組等資訊。在本研究中，可於設定模組設定物聯網閘道器屬性資料(包含：含可支援的通訊模組、可支援的資料模組、廠牌、程式版本等)。

- **資料模組**

不同的資料模組可為不同的應用分別建立合適的資料模型內容，並且閘道器和終端設備可具備相同的資料模型內容以完成相同應用之不同的設備的介接。在本研究中，血壓計物聯網終端設備具備血壓計應用資料模組，該應用資料模組將儲存血壓計的資料格式內容，包含有收縮壓值、舒張壓值、心率值。

3.3 終端設備

終端設備係由(1) 通訊模組、(2) 應用功能模組、(3) 探索模組、(4) 連線管理模組、(5) 資訊安全模組、(6) 登錄模組、(7) 控制模組、(8) 通知模組、(9) 設定模組、以及(10) 資料模組所組成。在本研究中，終端設備是一種家庭應用終端設備(如：血壓計、心率計、血糖計、體脂計、體重計等)，可同時連結 WiFi、藍牙、ZigBee、PLC 等，可將健康照護終端即時資訊回傳至伺服器系統。

- **通訊模組**

終端設備可具有 WiFi 通訊模組、藍牙通訊模組、ZigBee 通訊模組、PLC 通訊模組，可同時介接不同的網路介面，並可經由 WiFi 通訊模組或藍牙通訊模組或 ZigBee 通訊模組或 PLC 通訊模組與物聯網閘道器通訊。

- **應用功能模組**

終端設備為一種健康照護終端設備(如：血壓計、心率計、血糖計、體脂計、體重計等)，例如：物聯網終端設備是一種血壓計物聯網終端設備，該設備包含有血壓計應用功能模組，可對血壓計應用功能模組進行血壓量測功能。

- **探索模組**

探索模組運用資料模組可發送和接收特定資料內容的 TCP 或 UDP 單播或群播或廣播封包，經由封包傳遞探索網路內符合要求的終端設備。在本研究中，終端設備探索模組可接收來自閘道器或其他終端設備的探索封包，並解析封包內容和判斷自身設備是否為欲探索的標的物，如果接收到封包的終端設備是標的物的話，將回覆訊息(如：IP 和設備識別碼)予閘道器或其他終端設備的探索模組，如果接收到封包的終端設備不是標的物的話，則不做任何回覆。可經由探索模組探索到網路內符合標的的終端設備。終端設備探索模組得與閘道器探索模組同樣功能，可探索網路內的其他終端設備。

- **連線管理模組**

連線管理模組對已探索到的其他終端設備發出要求建立連線，並監測連線品質，確保連線狀態，且可在斷線時，自動重新建立連線。在本研究中，可經由 WiFi 通訊模組以 WiFi 無線網路探索到血壓計終端設備，在探索模組中取得血壓計終端設備的 IP，再以該 IP 資訊建立 TCP 或 UDP 連線，並週期性發出封包測試該連線存活與否，如果連線中斷可由連線管理模組自動重新連線，並在連線失敗複數次後得停止重新連線。終端設備得逕行與其他終端設備進行連線，例如：血壓計與血壓計連線。

- **資訊安全模組**

資訊安全模組包含有加解密裝置、以及金鑰裝置，可經由加解密裝置運用金鑰裝置之金鑰進行資料加密或解密，再把處理後資料經由通訊模組轉送。在本研究中，加解密裝置可採用 RSA、AES、DES、3DES 等方法實作，金鑰裝置可採用對稱式金鑰或非對稱式金鑰等方式實作。資訊安全模組可經由加解密裝置運用金鑰裝置之金鑰進行資料加密或解密，再把處理後資料經由通訊模組轉送。例如：資訊安全設備、閘道器資訊安全模組、終端設備資訊安全模組可具備相同的金鑰，採用對稱式金鑰和 AES 加解密模組進行加解密。資訊安全模組亦可具備私密金鑰和公開金鑰，終端設備資訊安全模組可採

用私密金鑰和 RSA 演算法進行非對稱式金鑰的簽章，以確保資訊確實是由該終端設備資訊安全模組所簽署。

- **登錄模組**

登錄模組可在終端設備加入到網路時，可結合設定模組的資訊發送特定資料內容的 TCP 或 UDP 單播或群播或廣播封包，告知網路中閘道器或其他終端設備新加入終端設備的相關資訊。在本研究中，血壓計終端設備加入到網路時，可以向設定模組取得血壓計終端設備屬性資料(包含：含可支援的通訊模組、可支援的應用資料模組、廠牌、程式版本等)，並將此屬性資料以 UDP 封包廣播給網路內閘道器、其他終端設備。

- **控制模組**

控制模組可結合資料模組，依不同的應用和服務產生不同的控制訊號和資料模型內容，再經由通訊模組傳送控制訊號至其他終端設備，以達到控制需求。在本研究中，可運用控制模組依對應的資料模組建立可控制終端設備的訊號(如：血壓計的訊號包含有開始量測、停止量測)和資料模型(如：血壓計的資料模型包含有收縮壓值、舒張壓值、心率值)。

- **通知模組**

通知模組可建立非連線導向的單向推播訊息傳遞通道，可主動發送訊息予其他終端設備，或可接收其他終端設備傳送的訊息。在本研究中，當血壓計終端設備相關屬性改變時，可運用通知模組經由通訊模組發出 UDP 廣播封包，告知網路內閘道器和其他終端設備。例如：血壓計終端設備燈泡開始量測時，可經由通知模組進行通知。

- **設定模組**

設定模組可設定終端設備的相關屬性，包含可支援的通訊模組、可支援的資料模組等資訊。在本研究中，可於設定模組設定血壓計終端設備屬性資料(包含：含可支援的通訊模組、可支援的應用資料模組、廠牌、程式版本等)。

- **資料模組**

不同的資料模組可為不同的應用分別建立合適的資料模型內容，並且閘道器和終端設備可具備相同的資料模型內容以完成相同應用之不同的設備的介接。在本研究中，血壓計物聯網終端設備具備血壓計應用資料模組，該應用資料模組將儲存血壓計的資料格式內容，包含有收縮壓值、舒張壓值、心率值。

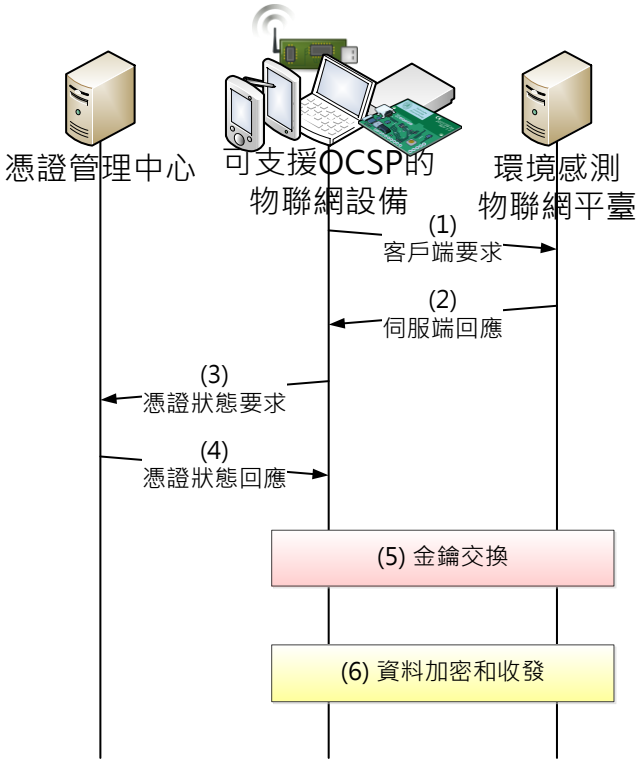
肆、安全通訊機制與應用

在本節中將先介紹雙向認證之安全通訊機制，再以健康照護為例說明安全通訊機制的操作方式。

4.1 雙向認證之安全通訊機制

本研究採用超文字傳輸安全協定(Hypertext Transfer Protocol Secure, HTTPS)，HTTPS 為一種在安全通訊協定(Secure Sockets Layer, SSL)或傳輸層安全協定(Transport Layer Security, TLS)基礎上運作的超文字傳輸協定(Hypertext Transfer Protocol, HTTP)，經由公開金鑰基礎建設(Public Key Infrastructure, PKI)建立安全的通訊機制，再透過底層的傳輸控制協定(Transmission Control Protocol, TCP)和網際網路協定(Internet Protocol, IP)進行傳輸。

有鑑於 TLS 安全等級較高，在物聯網系統主要將採用 TLS 技術建立安全傳輸機制，詳細運作流程(如圖五)說明如下。



圖五：HTTPS 運作流程圖

Step (1). 首先將先由可支援憑證狀態協定(Online Certificate Status Protocol, OCSP)的物聯網設備(此設備可為感測器、行動設備、使用者設備)發出「客戶端要求」的

訊息，在訊息中說明物聯網設備支援的傳輸協定版本、加解密演算法、以及一個客戶端隨機數作為後續建立會談金鑰(Session Key)使用。

Step (2). 環境感測物聯網平臺接收到物聯網設備的訊息後，將確認與物聯網設備採用的傳輸協定版本和加解密演算法，並產生一個伺服器端隨機數，再將環境感測物聯網平臺的伺服器端憑證和伺服器端隨機數以「伺服端回應」的訊息回覆給物聯網設備。

Step (3). 當物聯網設備接收到伺服器端憑證後，將向公開可信任的憑證管理中心(Certification Authority, CA)發出「憑證狀態要求」，向憑證管理中心查詢該伺服器端憑證的即時狀態。

Step (4). 憑證管理中心收到「憑證狀態要求」後，可確認物聯網設備所查詢的伺服器端憑證之狀態，並將此狀態資訊經由「憑證狀態回應」訊息回覆予物聯網設備。

Step (5). 當物聯網設備取得並確認伺服器端憑證的即時狀態為正常狀態後，物聯網設備將與環境感測物聯網平臺分別運用 Step (1)和 Step (2)的客戶端隨機數和伺服器端隨機數建立會談金鑰。

Step (6). 開始進行資料傳輸，並將該資料可以運用 Step (5)所產生的會談金鑰進行加解密，為物聯網設備將與環境感測物聯網平臺之間建立安全傳輸機制。

4.2 健康照護案例

在本案例中將說明健康照護物聯網系統的生理資料交換方法，其中主要包含(1) 生理資料授權方法和(2) 生理資料存取方法，分述如下。

4.2.1 生理資料授權方法

生理資料授權方法主要應用於病患可以授權給醫師瀏覽其生理資料，執行步驟描述如下：

Step (1). 病患使用其智慧型手機(以下稱為第一物聯網閘道器)運用資訊安全模組，運用第一物聯網閘道器的私鑰對訂閱時間 T1 及訂閱主題進行加密，該訂閱主題係第一物聯網閘道器的設備編號 I1，並產生第一加密資料 E1。

Step (2). 第一物聯網閘道器運用資訊安全模組，運用物聯網伺服器子系統的公鑰對第一加密資料 E1 進行加密，並產生第二加密資料 E2。

Step (3). 第一物聯網閘道器運用通訊模組和連線模組建立與物聯網伺服器子系統的連線，並傳送第二加密資料 E2。

Step (4). 物聯網伺服器子系統接收第二加密資料 E2。

Step (5). 物聯網伺服器子系統運用物聯網資訊安全設備，運用物聯網伺服器子系統的私鑰對第二加密資料 E2 進行解密，並得到第一加密資料 E1。

Step (6). 物聯網伺服器子系統運用物聯網資訊安全設備，運用第一物聯網閘道器的公鑰對第一加密資料 E1 解密，並得到訂閱時間 T1 及該訂閱主題。

Step (7). 物聯網伺服器子系統訂閱時間 T1 及該訂閱主題儲存至物聯網資料庫設備及物聯網推播服務設備，建立一訂閱主題資料。

Step (8). 醫師將訂閱主題輸入至其智慧型手機(以下稱為第二物聯網閘道器)，該訂閱主題係第一物聯網閘道器的設備編號 I1。

Step (9). 第二物聯網閘道器運用資訊安全模組，運用第二物聯網閘道器的私鑰對訂閱時間 T2、第二物聯網閘道器的設備編號 I2 及該訂閱主題進行加密，並產生第三加密資料 E3。

Step (10). 第二物聯網閘道器運用資訊安全模組，運用物聯網伺服器子系統的公鑰對第三加密資料 E3 進行加密，並產生第四加密資料 E4。

Step (11). 第一物聯網閘道器運用通訊模組和連線模組建立與物聯網伺服器子系統的連線，並傳送第四加密資料 E4。

Step (12). 物聯網伺服器子系統接收第四加密資料 E4。

Step (13). 物聯網伺服器子系統運用物聯網資訊安全設備，運用物聯網伺服器子系統的私鑰對第四加密資料 E4 進行解密，並得到第三加密資料 E3。

Step (14). 物聯網伺服器子系統運用物聯網資訊安全設備，運用第二物聯網閘道器的公鑰對第三加密資料 E3 解密，並得到訂閱時間 T2、第二物聯網閘道器的設備編號 I2 及訂閱主題。

Step (15). 物聯網伺服器子系統比對物聯網資料庫設備及物聯網推播服務設備中的訂閱主題集合，並將經由該物聯網推播服務設備將第二物聯網閘道器訂閱主題第一物聯網閘道器的設備編號 I1 的訊息推播給第一物聯網閘道器。

Step (16). 第一物聯網閘道器運用通訊模組和通知模組，接收物聯網伺服器子系統的第二物聯網閘道器訂閱主題第一物聯網閘道器的設備編號 I1 之訊息。

Step (17). 第一物聯網閘道器通知病患，確認是否授權生理資料瀏覽權限給第二物聯網閘道器。

Step (18). 物聯網伺服器子系統運用物聯網資訊安全設備，運用物聯網伺服器子系統的私鑰對訂閱時間 T2、該訂閱主題、及授權結果進行加密，並產生第五加密資料 E5。

Step (19). 物聯網伺服器子系統運用物聯網資訊安全設備，運用第二物聯網閘道器的公鑰對第五加密資料 E5 進行加密，並產生第六加密資料 E6。

Step (20). 物聯網伺服器子系統運用該物聯網推播服務設備將第六加密資料 E6 推播給第二物聯網閘道器。

Step (21). 第二物聯網閘道器運用通訊模組和通知模組，接收第六加密資料 E6。

Step (22). 第二物聯網閘道器運用資訊安全模組，運用第二物聯網閘道器的私鑰對第六加密資料 E6 進行加密，並得到第五加密資料 E5。

Step (23). 第二物聯網閘道器運用資訊安全模組，運用物聯網伺服器子系統的公鑰對第五加密資料 E5 進行加密，並得到訂閱時間 T2、該訂閱主題、及授權結果。

4.2.2 生理資料存取方法

生理資料存取方法主要應用於病患可以量測其生理資料，並由得到授權的醫師瀏覽其生理資料，執行步驟描述如下：

Step (1). 病患使用其智慧型手機(以下稱為第一物聯網閘道器)運用探索模組探索未探索到的血壓計物聯網終端設備(以下稱為第一物聯網終端設備)。

Step (2). 第一物聯網閘道器運用連線管理模組建立探索到的第一物聯網終端設備之連線。

Step (3). 病患使用第一物聯網終端設備進行量測，並由第一物聯網終端設備產生生理資料 D1。

Step (4). 第一物聯網終端設備運用資訊安全模組，運用一雜湊演算法對生理資料 D1、量測時間 T3、及第一物聯網終端設備的設備編號 I3 進行計算，並產生第一雜湊值 M1。

Step (5). 第一物聯網終端設備運用資訊安全模組，運用第一物聯網終端設備的私鑰對量測到的生理資料 D1、量測時間 T3、第一物聯網終端設備的設備編號 I3、及第一雜湊值 M1 進行加密，並產生第七加密資料 E7。

Step (6). 第一物聯網終端設備運用資訊安全模組，運用第一物聯網閘道器的公鑰對第七加密資料 E7 進行加密，並產生第八加密資料 E8。

Step (7). 第一物聯網終端設備運用通訊模組，把第八加密資料 E8 傳送給第一物聯網閘道器。

Step (8). 第一物聯網閘道器運用通訊模組，接收第八加密資料 E8。

Step (9). 第一物聯網閘道器運用資訊安全模組，運用第一物聯網閘道器的私鑰對第八加密資料 E8 進行解密，並得到第七加密資料 E7。

Step (10). 第一物聯網閘道器運用資訊安全模組，運用第一物聯網終端設備的公鑰對第七加密資料 E7 進行解密，並得到量測到的生理資料 D1、量測時間 T3、第一物聯網終端設備的設備編號 I3、及第一雜湊值 M1。

Step (11). 第一物聯網閘道器運用資訊安全模組，運用該雜湊演算法對生理資料 D1、量測時間 T3、及第一物聯網終端設備的設備編號 I3 進行計算，並產生第二雜湊值 M2。

Step (12). 第一物聯網閘道器運用資訊安全模組比對第一雜湊值 M1 和第二雜湊值 M2。

Step (13). 判斷第一雜湊值 M1 和第二雜湊值 M2 是否一致。

Step (14). 當第一雜湊值 M1 和第二雜湊值 M2 一致，第一物聯網閘道器運用資訊安全模組，運用該雜湊演算法對生理資料 D1、量測時間 T3、及第一物聯網閘道器的

設備編號 I1 進行計算，並產生第三雜湊值 M3。

Step (15). 第一物聯網閘道器運用資訊安全模組，運用第一物聯網閘道器的私鑰對量測到的生理資料 D1、量測時間 T3、第一物聯網閘道器的設備編號 I1、及第三雜湊值 M3 進行加密，並產生第九加密資料 E9。

Step (16). 第一物聯網閘道器運用資訊安全模組，運用物聯網伺服器子系統的公鑰對第九加密資料 E9 進行加密，並產生第十加密資料 E10。

Step (17). 第一物聯網閘道器運用通訊模組，把第十加密資料 E10 傳送給物聯網伺服器子系統。

Step (18). 物聯網伺服器子系統運用通訊模組，接收第十加密資料 E10。

Step (19). 物聯網伺服器子系統運用物聯網資訊安全設備，運用物聯網伺服器子系統的私鑰對第十加密資料 E10 進行解密，並得到第九加密資料 E9。

Step (20). 物聯網伺服器子系統運用物聯網資訊安全設備，運用第一物聯網閘道器的公鑰對第九加密資料 E9 進行解密，並得到量測到的生理資料 D1、量測時間 T3、第一物聯網閘道器的設備編號 I1、及第三雜湊值 M3。

Step (21). 物聯網伺服器子系統運用物聯網資訊安全設備，運用該雜湊演算法對生理資料 D1、量測時間 T3、及第一物聯網閘道器的設備編號 I1 進行計算，並產生第四雜湊值 M4。

Step (22). 物聯網伺服器子系統運用物聯網資訊安全設備比對第三雜湊值 M3 和第四雜湊值 M4。

Step (23). 判斷第三雜湊值 M3 和第四雜湊值 M4 是否一致。

Step (24). 當第三雜湊值 M3 和第四雜湊值 M4 一致，物聯網伺服器子系統將生理資料 D1、量測時間 T3、及第一物聯網閘道器的設備編號 I1 儲存到物聯網資料庫設備。

Step (25). 物聯網伺服器子系統將查詢物聯網資料庫設備和物聯網推播服務設備，確認目前有訂閱第一物聯網閘道器的設備編號 I1 並得到授權的醫師智慧型手機(以下稱為第二物聯網閘道器)。

Step (26). 物聯網伺服器子系統運用物聯網資訊安全設備，運用該雜湊演算法對生理資料 D1、量測時間 T3、及物聯網伺服器子系統的設備編號 I4 進行計算，並產生第五雜湊值 M5。

Step (27). 物聯網伺服器子系統運用物聯網資訊安全設備，運用物聯網伺服器子系統的私鑰對量測到的生理資料 D1、量測時間 T3、物聯網伺服器子系統的設備編號 I4、及第五雜湊值 M5 進行加密，並產生第十一加密資料 E11。

Step (28). 物聯網伺服器子系統運用物聯網資訊安全設備，運用第二物聯網閘道器的公鑰對第十一加密資料 E11 進行加密，並產生第十二加密資料 E12。

Step (29). 物聯網伺服器子系統運用通訊模組，把第十二加密資料 E12 傳送給第二物聯網閘道器。

Step (30). 第二物聯網閘道器運用通訊模組，接收第十二加密資料 E12。

Step (31). 第二物聯網閘道器運用資訊安全模組，運用第二物聯網閘道器的私鑰對第十二加密資料 E12 進行解密，並得到第十一加密資料 E11。

Step (32). 第二物聯網閘道器運用資訊安全模組，運用物聯網伺服器子系統的公鑰對第十一加密資料 E11 進行解密，並得到量測到的生理資料 D1、量測時間 T3、物聯網伺服器子系統的設備編號 I4、及第五雜湊值 M5。

Step (33). 第二物聯網閘道器運用資訊安全模組，運用該雜湊演算法對生理資料 D1、量測時間 T3、及物聯網伺服器子系統的設備編號 I4 進行計算，並產生第六雜湊值 M6。

Step (34). 第二物聯網閘道器運用資訊安全模組比對第五雜湊值 M5 和第六雜湊值 M6。

Step (35). 判斷第五雜湊值 M5 和第六雜湊值 M6 是否一致。

Step (36). 當第五雜湊值 M5 和第六雜湊值 M6 一致，第二物聯網閘道器呈現生理資料 D1。

伍、結論

有鑑於傳統 M2M 介接的作法需由廠商之間互相協調和談委合作協議，再依合作廠商的資料模型和控制指令來建立通訊；並且在更換合作廠商時，需修改全部的資料模型和控制指令，造成研發成本增加、產品上市時間的延宕等問題。近年來開始有許多物聯網聯盟(如：AllSeen、OCF、以及 oneM2M 等)開始制定共通的資料模型和控制指令，但 AllSeen 和 OCF 主要僅著重於感測層，無法連結至網路層和應用層，故本研究將參考各種物聯網聯盟標準，設計和實作一套能介接各種物聯網聯盟標準的系統和閘道器。本研究提出一套三層式架構的物聯網系統，此系統包含有伺服器系統、閘道器、以及終端設備。其中，伺服器系統將可經由中介軟體服務設備與閘道器、終端設備通訊。閘道器和終端設備分別包含通訊模組、探索模組、連線管理模組、資訊安全模組、登錄模組、控制模組、通知模組、設定模組、以及資料模組，以廣泛應用在各種物聯網服務。可經由轉譯模組介接各種不同的物聯網聯盟標準，並可將資料介接至伺服器系統進行巨量資料分析和機器學習，以達到監看、控制、最佳化、自主性等服務。

在未來研究中，將可考慮在此物聯網系統中開發各式各樣的應用服務，並透過介接不同的物聯網設備收集異質資料來源，分析和產生更有價值的商業智慧應用服務。

參考文獻

[1]. AllSeen Alliance, “Compliance & Certification Program for AllJoyn Certified - Program Management Document,” version 4.0, 2015.

[2]. oneM2M, “TS 0001: Functional Architecture,” v1.13.1, 2016.
[3]. oneM2M, “TS 0009: HTTP Protocol Binding,” v1.5.1, 2016.
[4]. oneM2M, “TS 0010: MQTT Protocol Binding,” v1.5.1, 2016.
[5]. oneM2M, “TS 0008: CoAP Protocol Binding,” v1.3.2, 2016.
[6]. Open Interconnect Consortium, “OIC Core Specification,” v1.0.0, 2015.
[7]. M.E. Porter and J.E. Heppelmann, “How smart, connected products are transforming competition,” *Harvard Business Review*, vol. 92, no. 11, pp. 64-88, 2014.
[8]. M.E. Porter and J.E. Heppelmann, “How smart, connected products are transforming companies,” *Harvard Business Review*, vol. 93, no. 10, pp. 97-114, 2015.

[作者簡介]

陳志華畢業於國立交通大學資訊管理與財務金融學系資訊管理博士班，現職為中華電信研究院智慧聯網研究所研究員，目前從事智慧運輸服務研發。

林邦曄畢業於國立交通大學資訊管理研究所博士班，現職為中華電信研究院資通安全研究所研究員，目前從事憑證管理服務研發。

吳錦松畢業於國立中央大學資訊工程學系博士班，現職為中華電信研究院資通安全研究所研究員，目前從事加解密技術研發。

蕭之彥畢業於國立交通大學資訊管理與財務金融學系資訊管理碩士班，現職為中華電信研究院智慧聯網研究所副研究員，目前從事物聯網服務平台研發。