M522425

(19)中華民國智慧財產局

(12)新型說明書公告本 **(11)證書號數：TW M522425 U**

(45)公告日： 中華民國 105 (2016) 年 05 月 21 日

(21)申請案號：104208943 (22)申請日： 中華民國 104 (2015) 年 06 月 05 日

(51)Int. Cl.： *G06Q10/08 (2012.01)*

(71)申請人：傑卓國際有限公司(中華民國) J&S INTERNATION (TW)
新竹縣竹北市六家五路 2 段 210 號 14 樓之 5

(72)新型創作人：陳煜仁 CHEN, YU REN (TW)；李皞白 LEE, HAO PAI (TW)；黃祥麟 HUANG, HSIANG LIN (TW)；陳育進 CHEN, YU CHIN (TW)

(74)代理人：許郁莉

申請專利範圍項數：10 項 圖式數：12 共 60 頁

(54)名稱

物聯網連接架構

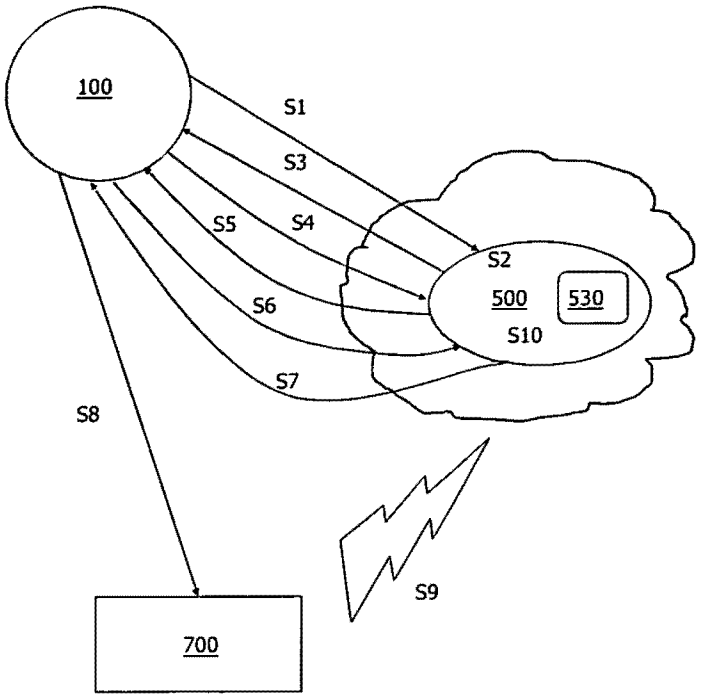
IOT CONNECTED ARCHITECTURE

(57)摘要

物聯網連接架構是由用戶端裝置、雲端裝置及數個代理裝置所組成；其中，用戶端裝置為一種具有無線通信功能且具有特定用戶識別碼的裝置；雲端裝置具有與用戶端通信之功能，藉由用戶端裝置的特定用戶識別碼確認用戶端裝置為物聯網中的其中之一個用戶端裝置；以及代理伺服裝置具有其網址及密碼，並能與雲端裝置通信。當雲端裝置確認用戶端裝置為物聯網的裝置後，使得用戶端裝置只能與代理伺服裝置通信，並再由代理伺服裝置與雲端裝置通信。

Internet of thing architecture consists of client device, cloud device, and the several proxy devices, in which the client device is a device which having a wireless communication function and has a specific user identification code, the cloud device is capable of communicating with client, with the specific client identification code to confirm the client device is one of the client device for the internet of thing, and the proxy device having its website and the password and is communicated with the cloud device. After the client device is the device of the internet of thing which is confirmed by the cloud device, the client device is merely communicated with the proxy device and the proxy device is then communicated with the cloud device.

指定代表圖：



第一圖

符號簡單說明：

S1~S10・・・通信方向

100・・・用戶端裝置

500・・・雲端裝置

530・・・記憶體模組

700・・・代理伺服裝置

104年 09月 21日 修正替換頁

公告本

新型摘要

※ 申請案號：104208943

※ 申請日：104、6、05　　※IPC 分類：G06Q 10/08 (2012.01)

【新型名稱】(中文/英文)

物聯網連接架構/ IOT connected Architecture

【中文】

物聯網連接架構是由用戶端裝置、雲端裝置及數個代理裝置所組成；其中，用戶端裝置為一種具有無線通信功能且具有特定用戶識別碼的裝置；雲端裝置具有與用戶端通信之功能，藉由用戶端裝置的特定用戶識別碼確認用戶端裝置為物聯網中的其中之一個用戶端裝置；以及代理伺服裝置具有其網址及密碼，並能與雲端裝置通信。當雲端裝置確認用戶端裝置為物聯網的裝置後，使得用戶端裝置只能與代理伺服裝置通信，並再由代理伺服裝置與雲端裝置通信。

【英文】

Internet of thing architecture consists of client device, cloud device, and the several proxy devices, in which the client device is a device which having a wireless communication function and has a specific user identification code, the cloud device is capable of communicating with client, with the specific client identification code to confirm the client device is one of the client device for the internet of thing, and the proxy device having its website and the password and

is communicated with the cloud device. After the client device is the device of the internet of thing which is confirmed by the cloud device, the client device is merely communicated with the proxy device and the proxy device is then communicated with the cloud device.

【代表圖】

【本案指定代表圖】：第（一）圖。

【本代表圖之符號簡單說明】：

通信方向	S1~S10
用戶端裝置	100
雲端裝置	500
記憶體模組	530
代理伺服裝置	700

104年 09月 21日 修正替換頁

新型專利說明書

（本說明書格式、順序，請勿任意更動）

【新型名稱】（中文/英文）

物聯網連接架構/ IOT connected Architecture

【技術領域】

【0001】 本創作是有關於一種雲端服務應用的系統，特別是有關於一種使用物聯網連接架構，以及使用此物聯網連接架構將產品的物流、倉儲及銷售狀況傳送到雲端裝置進處理的管理系統。

【先前技術】

【0002】 隨著科技之快速發展與經濟之結構巨變，傳統「企業對企業」之競爭形態已演變為「供應鏈對供應鏈」的競爭局面。提昇供應鏈資訊整合功能，以改善物流效率及降低物流成本，是現今企業創造競爭力的重要課題。隨著「無線射頻識別」(Radio Frequency Identification，RFID)技術的進步，RFID已逐漸被採用於供應鏈活動與流程改造。

【0003】 在物流管理的特性中，有助於提高產業競爭力的兩種特性因子分別為效率性與完整性。首先，就效率性而言，不只是在一定時間內把貨物送至客戶手中而已，還要加上在同時間內把不同的貨物送至不同的客戶手中的整合性配送方式。其次，就完整性而言，不只有提供貨物的實體完整性，還要提供貨物內容資訊。廠商為了提升這兩種特性，必須要取得貨物本身的即時資訊，而將RFID技術配合雲端監控系統，即可協助企業與其夥伴（經銷商），能夠在第一時間掌控物流，以便能夠即時的產生貨物的即時資訊。

【0004】 藉由RFID與雲端監控系統所提供的即時資訊，可提高顧客對於貨物的完整性的滿意度。貨物的完整性不單只有實體貨品的完整性，其貨物內容的資訊的提供，也是貨物完整性的考量方面。而且單針對貨物從生產工廠出產之後，到顧客的手中，在這個過程中，RFID讓物流中心對於貨物的監控情形，與即時提供貨品資訊可進一步作風險評估。

【0005】 在物流管理的特性中，效率和安全是其中最重要的二個環節，因此對於製造商和托運業者來說，如何有效追蹤及管理商品是最重要的問題之一。如果廠商想要提升這兩種特性，則必須要取得貨物本身的即時資訊，而透過 RFID 與雲端監控系統的技術便能夠產生即時的貨物完整資訊。

【0006】 此外，經由RFID與雲端監控系統的建制，使用業務端庫存量亦可快速回傳企業總部，使企業總部能夠在最短的時間內掌握第一手的商品銷售狀況跟市場需求。因此可以有效改善以往企業下訂採購的時程，例如:以往下訂採購的時程往往以月為單位，若估算錯誤則造成貨品囤積(多估）或者失去銷售獲利機會（少估）；而當企業總部能夠即時掌控銷售狀況跟市場需求時，可使企業快速反應，越短的下訂採購時間表示企業可依市場實際反應，及時增加或減少供貨，有效降低風險、增加獲利。

【0007】 能夠形成上述這些應用，是因為物聯網(Internet of Things；IOT)連接架構的建立。物聯網是藉由一個高度整合的雲端網路，將每個人與周遭的事物全部連接在一個網路內；例如:製造者、消費者、機器、生產原料、產品生產過程、物流管理、產品銷售狀況、消費習慣等，所有從產品生產到產品銷售，進而到根據這些產品銷售狀況的大數據(big data)，推斷或預估出消費者的消費習慣等，都可以通過產品上的感測元件(例如:RFID、

電子標籤)與軟體程式連接到物聯網平台。同樣的，物聯網在效率和安全是最重要的二個關鍵條件，然而，效率和安全卻是兩個互相牴觸的指標。因此，如何兼顧效率和安全是物流管理系統能否成功應用的關鍵。

【新型內容】

【0008】 為了將上述的需求實際運用在企業運營上，本創作之一主要目的在於提供一種物聯網的連通架構，包括:一用戶端裝置，為一具有無線通信功能的裝置，藉由特定用戶識別碼確認該用戶端裝置為物聯網中的其中之一個用戶端裝置；雲端裝置，具有與用戶端通信之功能，可以藉由且特定用戶識別碼來確認該用戶端裝置為物聯網中的其中之一個用戶端裝置；代理伺服裝置，具有網址及密碼，並能與雲端裝置通信；其中，於雲端裝置提供代理伺服裝置的網址及密碼予用戶端裝置後，用戶端裝置只能與代理伺服裝置通信，並再由代理伺服裝置與該雲端裝置通信，以便將用戶端裝置上的訊息傳至雲端裝置中；可以提高物聯網的安全性、效率性與降低商業運營的成本。

【0009】 本創作之另一主要目的在於提供一種使用本創作物聯網連通架構的物品物流管理系統，能夠提高物流管理的效率性與降低運營的成本。

【0010】 依據上述目的，本創作首先提供一種物聯網的連通架構，包括:用戶端裝置，為具有無線通信功能的裝置，且具有特定用戶識別碼；雲端裝置，具有與用戶端裝置通信之功能，藉由特定用戶識別碼確認用戶端裝置為物聯網中的其中之一個用戶端裝置；代理伺服裝置，具有網址及密

碼，並能與雲端裝置通信；其中，於雲端裝置提供代理伺服裝置的網址及密碼予物聯網中的用戶端裝置後，用戶端裝置只能與代理伺服裝置通信，並再由代理伺服裝置與雲端裝置通信，以便將用戶端裝置上的訊息傳至雲端裝置中。

【0011】 本創作接著提供一種物聯網的連通架構，包括:多個用戶端裝置，每一個用戶端裝置均為具有無線通信功能的裝置，且每一個用戶端裝置均具有特定的用戶識別碼；雲端裝置，具有與每一個用戶端裝置通信之功能，藉由每一個特定用戶識別碼確認每一個用戶端裝置均為物聯網中的其中之一個用戶端裝置；多個代理伺服裝置，每一個代理伺服裝置具有網址及密碼，並能與雲端裝置通信；其中，於雲端裝置提供每一個代理伺服裝置的網址及密碼予至少一個物聯網中的用戶端裝置並形成配對後，每一個用戶端裝置只能與配對的代理伺服裝置通信，並再由代理伺服裝置與雲端裝置通信，以便將每一個用戶端裝置上的訊息傳至雲端裝置中。

【圖式簡單說明】

【0012】

第一圖，係本創作的物聯網連接架構示意圖；

第二圖，係本創作的物聯網連接架構另一實施例的示意圖；

第三圖，係本創作的物聯網連接方法的流程圖；

第四圖，係創作的物聯網連接方法的另一實施例的示意圖；

第五圖，係本創作的物聯網產品的物流管理系統架構示意圖；

第六圖，係本創作的讀寫裝置結構示意圖；

第七 A 圖，係本創作的雲端裝置結構示意圖；

第七 B 圖，係本創作儲存在記憶體模組中的安全判斷資料示意圖；

第七 C 圖，係本創作儲存在記憶體模組內的倉儲資料示意圖；

第八圖，係本創作的物聯網產品物流管理系統第一實施例知示意圖；

第九圖，係本創作的物聯網產品物流管理系統第一實施例中的第二位置區域示意圖；

第十圖，係本創作的物聯網產品物流管理系統第二實施例的產品倉儲管理示意圖；

第十一圖，係本創作的物聯網產品物流管理系統第二實施例的產品銷售管理示意圖；

第十二圖，係本創作中的管理者訊息顯示的示意圖。

【實施方式】

【0013】 為使本創作之目的、技術特徵及優點，能更為相關技術領域人員所了解並得以實施本創作，在此配合所附圖式，於後續之說明書闡明本創作之技術特徵與實施方式，並列舉較佳實施例進一步說明，然以下實施例說明並非用以限定本創作，且以下文中所對照之圖式，係表達與本創作特徵有關之示意。

【0014】 首先，請參考第一圖，是本創作的物聯網連接架構示意圖。如第一圖所示，物聯網連接架構是由用戶端裝置(client device)100、雲端裝置(cloud device)500及至少一個代理裝置(broker device)700所組成；其中，用戶端裝置100為一種具有無線通信功能且具有特定用戶識別碼的裝置；雲端裝置500，具有與用戶端裝置100通信之功能，藉由用戶端裝置100的特定用戶識別碼確認用戶端裝置100為物聯網中的其中之一個用戶端裝置100；以

及代理伺服裝置700，具有其網址及密碼，並能與雲端裝置500通信。

【0015】 在本創作的物聯網連接架構中，用戶端裝置100是一種隨時變動的浮動IP (Internet Protocol)的無線通信功能的裝置(例如:個人電腦、筆記本電腦、智慧型手機、智慧型可攜式裝置、智慧型讀取裝置等)，並且每一個用戶端裝置100都具有獨特性的識別碼(例如:製造廠商於出廠時所設定的編碼；又例如: MAC Address等硬體資料)，以便用來產生用戶端裝置100的通用唯一識別碼（Universally Unique Identifier；縮寫為uuid），用以辨識或防止駭客侵入。此外，在本創作的物聯網連接架構中，雲端裝置500是一種固定式網域名稱系統(Domain Name System；縮寫為DNS)，其具有伺服器(sever)之功能並且具有與用戶端裝置100通信之功能，同時雲端裝置500至少是由接收/發射介面模組、資料處理模組及記憶體模組等裝置所組成；因此，雲端裝置500已經記錄著所有屬於本創作物聯網中的所有用戶端的uuid並已儲存在記憶體模組中，形成一資料庫。再者，代理伺服裝置700是一種隨時變動的浮動IP，其最主要的工作是將確認是為物聯網中的用戶端裝置100所傳送的編碼資料串在接收後，直接傳送出至雲端裝置500；特別要說明的是，代理伺服裝置700在收到用戶端裝置100所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去，在雲端裝置500收到代理伺服裝置700的資料串後，再經過解碼後，才會對用戶端裝置100所傳送的資料串進行處理。很明顯的，在本創作的物聯網連接架構中，在整個用戶端裝置100將資料串遞給雲端裝置500的過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率，可以大幅度的提高物聯網的安全性。

【0016】 而在本創作的物聯網連接架構的較佳實施例中，可以將多個用戶端裝置100分為多個群組，每一群組分別對應或配對至一個代理伺服裝置700，故在本創作的物聯網連接架構中，可以有多個代理伺服裝置700，如第2圖所示。當雲端裝置500判斷其中一個代理伺服裝置700遭受駭客攻擊後，可以選擇將被攻擊的代理伺服裝置700關閉，或再重新建立一個新的代理伺服裝置700的網址及密碼，可以更確保本創作物聯網的安全性。此外，在本創作的實施例中，代理伺服裝置700是選擇使用MQTT(Message Queuing Telemetry Transport) 的通信標準(protocol)來做資料串的傳送。由於MQTT是為了物聯網而設計的協定，特別是基於發佈/訂閱模式的羽量級消息傳輸協定，其為IBM的Andy Stanford-Clark博士及Arcom公司的Arlen Nipper 博士于1999年創作；最初是為大量計算能力有限且工作在低頻寬、不可靠的網路的遠端感測器和控制設備之間的通訊而設計的協定。因此，MQTT具有傳輸資料小且輕巧的優點，可以在頻寬及速度上都有極大優勢；也由於其所需要的網路頻寬是很低的，因而使得其所需要的硬體資源也是低的，故可以將物聯網系統或是使用此物聯網架構的各種商業運營系統(例如物流管理或是產品的生產履歷等) 之效率性提升；也因此可以有效地降低商業運營的成本。

【0017】 接著，詳細說明本創作的物聯網實際完成連接的過程及其方法。

【0018】 請繼續參考第一圖，首先，由用戶端裝置100向雲端裝置500進行登錄(如第1圖中的S1標示的通信方向)，例如: 用戶端裝置100通過https向雲端裝置500登錄，以便啟動物聯網系統。接著，當雲端裝置500收到用

戶端裝置100的請求後(如第一圖中的S2標示的通信方向)，雲端裝置500會先驗證用戶端裝置100所使用的MAC Address是否已經儲存在雲端裝置500的資料庫中；若確認用戶端裝置100所使用的MAC Address已經儲存在雲端裝置500的資料庫時，則產生一個客戶辯證碼(client uuid)；接著，雲端裝置500產生一對專屬客戶使用的金鑰；在本創作的較佳實施例中，此金鑰是使用RSM非對稱式金鑰(Asymmetric Key)；故可以產生出一對client_pub_key及client_pri_key；其中，RSM非對稱式金鑰具有解碼時間長，所以安全性高。此外，在另一較佳實施例中，雲端裝置500還可以選擇性的產生一個用戶端裝置100專屬的對稱式金鑰(Symmetric Key) client_share_key。故在本創作的較佳實施例中，可以選擇性的將RSM非對稱式金鑰及對稱式金鑰配合使用；由於，對稱式金鑰具有解碼時間短，相對地安全性較低，因此需要隨時變動client_share_key，以確保安全性；為此，雲端裝置500還會進一步產生/設定一個變動的時間(share_key_expiry date time)，藉由不定時的更改share_key_expiry date time來提升安全性；故當雲端裝置500偵測到隨時變動的client_share_key已經超過了share_key_expiry date time設定變動的時間後，即會自動產生新的client_share_key，以確保安全性。當雲端裝置500在確認一個用戶端裝置100的MAC Address資料與儲存在資料庫中相同時，則判斷此用戶端裝置100為本物聯網中的用戶端，之後，雲端裝置500會將所產生的uuid及金鑰等訊息回傳至用戶端裝置100(如第一圖中的S3標示的標通信方向)，這些回傳至用戶端裝置100的訊息包括:client_uuid、sever_pub_key (此sever_pub_key即是client_pub_key；因為所有用戶端裝置100都會使用同一個pub_key，所以又可稱為sever_pub_key)及client_pri_key。

【0019】 另外，若當雲端裝置500收到用戶端裝置100的請求後，雲端裝置500比對出用戶端裝置100所使用的MAC Address並不在雲端裝置500的資料庫中時，及判斷此用戶端裝置100所使用的MAC Address並非本物聯網中的用戶端裝置，則將此MAC Address訊息儲存在另一資料庫中，以便後續比對。特別要說明，S3通信方向的回傳機制，一般而言，是不會有錯誤的，但是還是有發生錯誤的機制；例如，等待Server反映時間過久導致此次連線失敗，則會再由用戶端裝置100重新執行一次，但是此時的雲端裝置500會判定此次的MAC address已經在資料庫中被記錄，因而還是會將此MAC address對應的uuid回傳，此時，雲端裝置500所產生並回傳給用戶端裝置100的一對金鑰會更新。因此，即便有假的裝置使用任何方法仿冒此用戶端裝置100的MAC address 也無法取得相同金鑰。換句話說，只會有一個確定的uuid能存活在系統中。

【0020】 接著，如第一圖中的S4標示的通信方向，當用戶端裝置100以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)通過https “要求” 取得client_share_key、share_key_expiry date time、MQTT_Broker IP及MQTT_Broker 帳號及密碼(username/passward)；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key、share_key_expiry date time、MQTT_Broker IP及MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100(如第一圖中的S5標示的通信方向)。

【0021】 此外，在本創作的一個較佳實施例中，MQTT_Broker的IP、

帳號及密碼可以選擇分兩次取得；例如，第一次(如第一圖中的S4標示的通信方向)，用戶端裝置100以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)通過https “要求” 取得client_share_key、share_key_expiry date time及MQTT_Broker IP；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key、share_key_expiry date time及MQTT_Broker IP等以client_pub_key編碼後回傳至用戶端裝置100(如第一圖中的S5標示的通信方向)。第二次(如第一圖中的S6標示的通信方向)，用戶端裝置100再以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)，通過https “要求” 取得MQTT_Broker 帳號及密碼；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100(如第一圖中的S7標示的通信方向)。特別要說明的，第一次及第二次所要取得的內容中，只要求將MQTT_Broker的IP、帳號及密碼分兩次取得，其他並不加以限制。

【0022】 很明顯地，在用戶端裝置100與雲端裝置500進行辨識與確認的過程中，所使用的https是屬於混合型密碼防駭、安全通訊協定(Secure Sockets Layer；SSL)或傳輸層安全協議(Transport Layer Security；TLS)，其本身屬於公認的安全協定，且雲端裝置500端所需要有的公認憑證，可以由用戶端裝置100藉由認證中心的數位簽章來確認訊息是否由雲端裝置500直接傳出；因此，當有駭客在訊息傳遞過程進行竄改、盜用或否認等行為時，

都可藉由這些安全認證來防止密碼遭竄改或盜用。

【0023】 接著，如第一圖中的S8標示的通信方向，當用戶端裝置100自雲端裝置500取得相關資料後，用戶端裝置100隨即會與代理伺服裝置700進行連接；但在進行與連接代理伺服裝置700前，必須確認所收到的訊息必須完整，此完整的訊息包括:1.Sever_pub_key；2.Client_pri_key；3.MQTT_Broker IP；4.MQTT_Broker username/passward；5.client_Share_key；6.Share_key_expiry date time。當用戶端裝置100在確認收到完整的訊息後，會使用client_share_key將client_uuid及用戶端裝置100所要傳給雲端的資料內容(data involved)進行編碼後，再上傳至代理伺服裝置700(即MQTT Broker)。

【0024】 在本創作的較佳實施例中，用戶端裝置100會進一步檢查Share_key_expiry date time的時效是否已經到期(例如:到期日為2015/0501)；如果已經過了Share_key_expiry date time的時效時(例如: 檢查期日的結果為2015/0502)，則用戶端裝置100會重新以編碼後的client_uuid(即client_uuid會根據sever_pub_key轉成亂碼)，通過https 要求取得新的share_key¬_expiry date time訊息；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將新的share_key_expiry date time以client_pub_key編碼後回傳至用戶端裝置100。此外，為增加安全性，share_key-_expiry date time所設定的時間可以是週期性的，也可以是隨機變數的，可以由雲端裝置500決定。

【0025】 當用戶端裝置100在確認已收到完整的訊息後，此時用戶端

裝置100已經知道代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼，故用戶端裝置100可以將編碼的client_uuid及資料串上傳至代理伺服裝置700(如第一圖中的S8標示的通信方向)；接著，代理伺服裝置700在收到用戶端裝置100所上傳的編碼client_uuid及資料串後，隨即將用戶端裝置100所上傳的訊息直接(也就是說，不做任何處理)傳送給雲端裝置500端；很明顯地，整個物聯網在用戶端裝置100將其訊息串遞給雲端裝置500的過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率。由於代理伺服裝置700只是將用戶端裝置100上傳的資料直接傳送給雲端裝置500，故可以降低代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼被破解的機率，可以更增加物聯網通信過程的安全性。

【0026】 接著，如第一圖中的S9標示的通信方向，雲端裝置500在接收到代理伺服裝置700所直接傳送的資料(即經過編碼後的client_uuid及資料串)後，隨即使用client_share_key進行解碼(Decode)，並且會驗證所收到的client_uuid及資料串是否完整及正確；如果正確時，則再儲存至記憶體模組中，等待使用者將這些收到的資料串進行特定的應用；若驗證所收到的client_uuid及資料串不完整或不正確時，則進行紀錄。要說明的是，要驗證出不正確的訊息的目的，是可以由物聯網系統藉著人工智慧作深度學習或人為增加、更改或修正的驗證機制，來防止或降低被駭成功的機率。在本實施例中，不正確的訊息包括，例如: (1)由網路爬蟲抓取新聞發現當下某些商品的偽品猖獗；又亦或是(2)程式一開始便設定的同一client_uuid，竟然在同一時間出現在兩個完全不同的地方，此時物聯網系統會通知公司稽查人

員或提出警告，而稽查人員可做出的處置方式至少有觀察或忽略等動作，達到事先預警及防駭的功效；又亦或是(3)裝置500本身持續受到某特定代理伺服裝置700傳送可疑資訊時，例如: 不明的client_uuid資訊時；當不正確的訊息持續出現時，則判斷代理伺服裝置700可能被駭客攻擊，則雲端裝置500可以選擇關閉此代理伺服裝置700(如第一圖中的S10標示的通信方向)。

【0027】 在本創作的實施例中，client_share_key編碼方式可以配合雜湊函數來防止竄改，其中雜湊函數可以選擇MD5、SHA-1或SHA-256等。同時，client_share_key也可以配合不同的解碼(decode)方式，例如:區塊密碼、串流密碼、ECB模式或是前述的混合方法等，除了可以更有效的提高破解難度外，還可以不損失解碼時間。

【0028】 請參考第二圖，是本創作的物聯網連接架構另一實施例的示意圖。如第二圖所示，物聯網連接架構是由複數個用戶端裝置100所組成、雲端裝置500及至少一個代理裝置700所組成；其中，每一個用戶端裝置100均為具有無線通信功能且具有特定用戶識別碼的裝置；雲端裝置500，具有與每一個用戶端裝置100通信之功能，藉由每一個用戶端裝置100各自獨有的特定用戶識別碼來確認用戶端裝置100為物聯網中的其中之一個用戶端裝置100；代理伺服裝置700，具有其網址及密碼，並能與雲端裝置500通信。由於第二圖的實施例與第一圖的實施例在基本連接的架構是相同的，而兩者之間的差異僅在於雲端裝置500提供每一個代理伺服裝置的網址、帳號及密碼予至少一個物聯網中的用戶端裝置100並形成配對後，這些被配對後的用戶端裝置100只能與配對的代理伺服裝置700通信，並再由代理伺服裝置700與雲端裝置500通信，以便將每一個用戶端裝置100上的資料串傳至雲端

裝置500中。故第二圖的物聯網實際完成連接的過程簡要說明如下。

【0029】 請繼續參考第二圖，首先，每一個用戶端裝置100各自過https向雲端裝置500進行登錄。接著，當雲端裝置500分別收到每一個用戶端裝置100的請求後，雲端裝置500會先驗證每一個用戶端裝置100所使用的MAC Address是否已經儲存在雲端裝置500的資料庫中；若確認每一個用戶端裝置100所使用的MAC Address都已經儲存在雲端裝置500的資料庫時，則分別產生每一個客戶各自的辯證碼(client uuid)；接著，雲端裝置500根據每一個用戶端裝置100產生一對專屬客戶使用的金鑰；當雲端裝置500判斷每一個用戶端裝置100均為本物聯網中的用戶端之後，雲端裝置500會將所產生的每一個uuid及金鑰等訊息回傳至相應的每一個用戶端裝置100中，這些回傳至每一個用戶端裝置100的訊息包括：client_uuid、sever_pub_key及client_pri_key。

【0030】 接著，每一個用戶端裝置100可以將其編碼後的client_uuid通過https “要求” 取得client_share_key、share_key_expiry date time、MQTT_Broker IP及MQTT_Broker 帳號及密碼(username/passward)；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據各自的sever_pri_key進行解碼，以確認每一個收到的client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key、share_key_expiry date time、MQTT_Broker IP及MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100。例如:將代理裝置(Broker-1)的IP、帳號及密碼回傳給Client-1~Client-5；將代理裝置(Broker-2)的IP、帳號及密碼回傳給Client-6~Client-15；將代理裝置(Broker-3)的IP、帳號及密碼回傳給

Client-16~Client-50；很明顯的，本物聯網已經將50個各別的用戶端裝置100分別配對由3個代理伺服裝置700來與雲端裝置500通信。接著，當每一個用戶端裝置100各自透過雲端裝置500取得相關資料後，用戶端裝置100隨即會與其所獲得的配對的代理伺服裝置700進行連接；同時，當每一個用戶端裝置100確認其由雲端裝置500所收到的訊息已包括:1.Sever_pub_key；2.Client_pri_key；3.MQTT_Broker IP；4.MQTT_Broker username/passward；5.Client_Share_key；6.Share_key_expiry date time後，會使用client_share_key將client_uuid及此用戶端裝置100所要傳給雲端的資料內容進行編碼後，再上傳至代理伺服裝置700(即MQTT Broker)。

【0031】 由於，當每一個用戶端裝置100在確認已收到完整的訊息後，此時用戶端裝置100已經知道其所配對的代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼，故用戶端裝置100可以將編碼client_uuid及訊息串上傳至配對的代理伺服裝置700；接著，每一個代理伺服裝置700在收到配對的用戶端裝置100所上傳的編碼client_uuid及訊息串後，隨即將用戶端裝置100所上傳的訊息直接(也就是說，不做任何處理)傳送給雲端裝置500端；很明顯地，整個物聯網在用戶端裝置100將其訊息串遞給雲端裝置500的過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率。由於每一個代理伺服裝置700只是將用戶端裝置100上傳的資料直接傳送給雲端裝置500，故可以降低代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼被破解的機率，可以更增加物聯網通信過程的安全性。接著，雲端裝置500在接收到每一個代理伺服裝置700所直接傳送的資料(即經過編碼後的client_uuid及資

料串)後，隨即使用每一個client_share_key進行解碼，並且會驗證所收到的client_uuid及資料串是否完整及正確；如果正確時，則再儲存至記憶體模組中，等待使用者將這些收到的資料串進行特定的應用；若驗證所收到的client_uuid及資料串不完整或不正確時，則進行紀錄；在本實施例中，不正確訊息的產生可能包括:每一個client 發佈信息頻率有一定的規律性，如若產生某client 以不正常或過多頻率來發佈的信息，則視為不正確的訊息；或代理伺服裝置700本身頻率發佈信息非經MQTT方式，而試圖連接雲端裝置500等；當不正確的訊息持續出現時，則判斷代理伺服裝置700可能被駭客攻擊；則雲端裝置500可以選擇關閉此代理伺服裝置700。

【0032】 綜合上述，本創作之物聯網連接架構的主要技術手段，是在雲端裝置500確認每一個用戶端裝置100均為本物聯網的用戶後，雲端裝置500會將代理伺服裝置700的MQTT_Broker IP、MQTT_Broker 帳號及密碼回傳給每一個用戶端裝置100，之後，每一個用戶端裝置100根據所收到的MQTT_Broker IP、MQTT_Broker 帳號及密碼與代理伺服裝置700連接，並且將每一個用戶端裝置100所要傳送的資料串編碼後，一起上傳至代理伺服裝置700，接著，代理伺服裝置700在不對用戶端裝置100傳送的資料串進行處理的狀況下，直接將用戶端裝置100傳送的資料串傳遞至雲端裝置500進行解碼及處理。很明顯的，本創作的物聯網連接架構分為兩個階段進行連接，並且在第一階段完成用戶端裝置100的辨識後，用戶端裝置100在第二階段中，只能與代理伺服裝置700連接；由於第一階段是在用戶端裝置100進行連接之前就已完成，故當用戶端裝置100正是傳遞資料串時，均只能與代理伺服裝置700連接及通信；因此，雲端裝置500並不會直接暴露出自己

的位址，故可以降低雲端裝置500被駭客攻擊的機率，可以有效的提高物聯網連接架構的安全性。

【0033】 再接著，詳細說明本創作的物聯網連接架構的連接方法及過程，透過本物聯網連接架構的連接方法及過程，可以更清楚的瞭解本創作使用代理伺服裝置700之創新點。

【0034】 請參考第三圖，是本創作的物聯網連接方法的流程圖。如第三圖所示，本創作的物聯網連接方法包括:

【0035】 步驟1: 由用戶端裝置100向雲端裝置500進行登錄，例如:用戶端裝置100通過https向雲端裝置500登錄，以便啟動物聯網系統。

【0036】 步驟2:當雲端裝置500收到用戶端裝置100的請求後，雲端裝置500會先驗證用戶端裝置100所使用的MAC Address是否已經儲存在雲端裝置500的資料庫中。

【0037】 步驟3: 當雲端裝置500確認用戶端裝置100所使用的MAC Address已經儲存在雲端裝置500的資料庫時，則判斷用戶端裝置100資料正確，其為本物聯網中的用戶端裝置100，則雲端裝置500會產生一個客戶辯證碼(client uuid)、一對專屬客戶使用的金鑰。在本實施例中，此金鑰是使用安全性高的RSM非對稱式金鑰(Asymmetric Key)；故可以產生出一對client_pub_key及client_pri_key；並且將其所產生的uuid及金鑰等訊息回傳用戶端裝置100，這些回傳用戶端裝置100的訊息包括: client_uuid、sever_pub_key (此sever_pub_key即是client_pub_key。此外，若當雲端裝置500收到用戶端裝置100的請求後，雲端裝置500比對出用戶端裝置100所使用的MAC Address並不在雲端裝置500的資料庫中時，及判斷此用戶端裝置100

所使用的MAC Address並非本物聯網中的用戶端裝置，則將此MAC Address訊息儲存在另一個資料庫中，以便後續比對。

【0038】 步驟4: 用戶端裝置100判斷雲端裝置500所產生的uuid及金鑰等訊息是否以正確收到；當用戶端裝置100確認已經正確地收到uuid及金鑰等訊息後，用戶端裝置100隨即會以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)通過https向雲端裝置500要求取得client_share_key、代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼(username/passward)。

【0039】 步驟5:當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key、代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100。

【0040】 步驟6: 當用戶端裝置100自雲端裝置500取得相關資料後，用戶端裝置100隨即會使用client_pri_key進行解碼，並確認所收到的訊息必須完整，此完整的訊息包括:1.Sever_pub_key ； 2.Client_pri_key ； 3.MQTT_Broker IP ； 4.MQTT_Broker username/passward ； 5.client_Share_key。當用戶端裝置100在確認收到完整的訊息後，即會與代理伺服裝置700進行連接；若用戶端裝置100判斷所收到的訊息不完整時，會回到步驟4，重新要求向雲端裝置500要求取得client_share_key、代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼(username/passward)。

【0041】 步驟7: 用戶端裝置100使用 MQTT_Broker IP及MQTT_Broker 帳號及密碼連接代理伺服裝置700；同時，也使用client_share_key將client_uuid及用戶端裝置100所要傳給雲端裝置500的資料內容(data involved)進行編碼後，再上傳至代理伺服裝置700。

【0042】 步驟8: 代理伺服裝置700在收到用戶端裝置100所上傳的編碼client_uuid及訊息串後，隨即將用戶端裝置100所上傳的訊息直接(也就是說，不做任何處理)傳送給雲端裝置500端。

【0043】 步驟9: 雲端裝置500在接收到代理伺服裝置700所直接傳送的資料後，隨即使用client_share_key進行解碼，並且會驗證所收到的client_uuid及資料串是否完整及正確。

【0044】 步驟10: 雲端裝置500判斷所收到的client_uuid及資料串完整及正確時，則將解碼後的用戶端資料串儲存至記憶體模組中，等待使用者將這些收到的資料串進行特定的應用；若驗證所收到的client_uuid及資料串不完整或不正確時，則進行紀錄；在本實施例中，不正確的訊息包括(1) 某ip 對應到的client_uuid不正確，則可能有盜用問題 (2) 若某 client_uuid 有配合上Geo Location 的資料上傳，可以藉由驗證GeoLocation 的合理性來驗證(是否某個client_uuid這一分鐘在亞洲，下一分鐘在北美)；當不正確的訊息持續出現時，則判斷代理伺服裝置700可能被駭客攻擊；則雲端裝置500可以選擇關閉此代理伺服裝置700。

【0045】 很明顯地，在整個物聯網架構的連接方法過程中，從步驟1至步驟6都是在每一個用戶端裝置100出廠前就與雲端裝置500完成連接，即每一個用戶端裝置100出廠後，就已經自雲端裝置500獲得完整的訊息包

括:1.Sever_pub_key；2.Client_pri_key；3.MQTT_Broker IP；4.MQTT_Broker username/passward；5.client_Share_key。當物聯網系統啟動後，每一個用戶端裝置100所要傳送給雲端裝置500處理的資料串，都會根據MQTT_Broker IP傳送至代理伺服裝置700，再由代理伺服裝置700直接將用戶端裝置100資料串傳送給雲端裝置500。故自步驟7至步驟10之間的訊息傳遞過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率。由於代理伺服裝置700只是將用戶端裝置100上傳的資料直接傳送給雲端裝置500，故可以降低代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼被破解的機率，可以更增加物聯網通信過程的安全性。

【0046】 接著，請參考第四圖，是本創作的物聯網連接方法另一實施例的流程圖。如第四圖所示，本創作的物聯網連接方法包括:

【0047】 步驟 1: 由用戶端裝置 100 向雲端裝置 500 進行登錄，例如:用戶端裝置 100 通過 https 向雲端裝置 500 登錄，以便啟動物聯網系統。

【0048】 步驟2:當雲端裝置500收到用戶端裝置100的請求後，雲端裝置500會先驗證用戶端裝置100所使用的MAC Address是否已經儲存在雲端裝置500的資料庫中。

【0049】 步驟3: 當雲端裝置500確認用戶端裝置100所使用的MAC Address已經儲存在雲端裝置500的資料庫時，則判斷用戶端裝置100資料正確，其為本物聯網中的用戶端裝置100，則雲端裝置500會產生一個客戶辯證碼(client uuid)、一對專屬客戶使用的金鑰。在本實施例中，此金鑰是使用安全性高的RSM非對稱式金鑰(Asymmetric Key)；故可以產生出一對

client_pub_key及client_pri_key；並且將其所產生的uuid及金鑰等訊息回傳用戶端裝置100，這些回傳用戶端裝置100的訊息包括：client_uuid、sever_pub_key (此sever_pub_key即是client_pub_key。此外，若當雲端裝置500收到用戶端裝置100的請求後，雲端裝置500比對出用戶端裝置100所使用的MAC Address並不在雲端裝置500的資料庫中時，及判斷此用戶端裝置100所使用的MAC Address並非本物聯網中的用戶端裝置，則將此MAC Address訊息儲存在另一資料庫中，以便後續比對。

【0050】 步驟4: 用戶端裝置100判斷雲端裝置500所產生的uuid及金鑰等訊息是否以正確收到；當用戶端裝置100確認已經正確地收到uuid及金鑰等訊息後，用戶端裝置100隨即會以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)通過https向雲端裝置500要求取得client_share_key、share_key_expiry date time、代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼(username/passward)。

【0051】 在本創作的較佳實施例中，此金鑰是使用RSM非對稱式金鑰(Asymmetric Key)；故可以產生出一對client_pub_key及client_pri_key；其中，RSM非對稱式金鑰具有解碼時間長，所以安全性高。此外，在另一較佳實施例中，雲端裝置500還可以選擇性的產生一個用戶端裝置100專屬的對稱式金鑰(Symmetric Key) client_share_key。故在本創作的較佳實施例中，可以選擇性的將RSM非對稱式金鑰及對稱式金鑰配合使用；由於，對稱式金鑰具有解碼時間短，相對地安全性較低，因此需要隨時變動client_share_key，以確保安全性；為此，雲端裝置500還會進一步產生一個隨時變動的share_key_expiry date time，藉由不定時的更改client_share_key

來提升安全性；故當雲端裝置500偵測到隨時變動的client_share_key已經超過了設定變動的時間後，即會自動產生新的client_share_key，以確保安全性。

【0052】 步驟5:當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key、share_key_expiry date time、代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100。

【0053】 步驟6: 當用戶端裝置100自雲端裝置500取得相關資料後，用戶端裝置100隨即會使用client_pri_key進行解碼，並確認所收到的訊息必須完整，此完整的訊息包括:1.Sever_pub_key ； 2.Client_pri_key ； 3.MQTT_Broker IP ； 4.MQTT_Broker username/passward ； 5.client_Share_key；6.share_key_expiry date time。當用戶端裝置100在確認收到完整的訊息後，即會與代理伺服裝置700進行連接；若用戶端裝置100判斷所收到的訊息不完整時，會回到步驟4，重新要求向雲端裝置500要求取得。

【0054】 步驟7: 用戶端裝置100使用 MQTT_Broker IP及MQTT_Broker 帳號及密碼連接代理伺服裝置700；同時，也使用client_share_key將client_uuid及用戶端裝置100所要傳給雲端裝置500的資料內容(data involved)進行編碼後，再上傳至代理伺服裝置700。

【0055】 步驟8: 用戶端裝置100檢查Share_key_expiry date time的時效是否已經到期；若檢查結果尚未到期後，則編碼後的client_uuid及資料串內容上傳至代理伺服裝置700；若檢查結果為過期狀態後，則會回到步驟4，

重新要求向雲端裝置500要求取得新的Share_key_expiry date time。例如:到期日為2015/0501時；如果檢查結果已經過了Share_key_expiry date time的時效時(例如: 檢查期日的結果為2015/0502)，則用戶端裝置100會重新以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)，通過https 要求取得新的share_key_expiry date time；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將新的share_key_expiry date time以client_pub_key編碼後回傳至用戶端裝置100。此外，為增加安全性，share_key_expiry date time所設定的時間可以是週期性的，也可以是隨機變數的，可以由雲端裝置500決定。

【0056】 步驟9: 代理伺服裝置700在收到用戶端裝置100所上傳的編碼client_uuid及訊息串後，隨即將用戶端裝置100所上傳的訊息直接(也就是說，不做任何處理)傳送給雲端裝置500端。

【0057】 步驟10: 雲端裝置500在接收到代理伺服裝置700所直接傳送的資料後，隨即使用client_share_key進行解碼，並且會驗證所收到的client_uuid及資料串是否完整及正確。

【0058】 步驟11: 雲端裝置500判斷所收到的client_uuid及資料串完整及正確時，則將解碼後的用戶端資料串儲存至記憶體模組中，等待使用者將這些收到的資料串進行特定的應用；若驗證所收到的client_uuid及資料串不完整或不正確時，則進行紀錄；在本實施例中，不正確的訊息包括(1) 某ip 對應到的client_uuid不正確，則可能有盜用問題 (2) 若某 client_uuid 有配合上Geo Location 的資料上傳，可以藉由驗證GeoLocation 的合理性來驗

證(是否某個client_uuid這一分鐘在亞洲，下一分鐘在北美)。當不正確的訊息持續出現時，則判斷代理伺服裝置700可能被駭客攻擊；則雲端裝置500可以選擇關閉此代理伺服裝置700。

【0059】 很明顯地，在整個物聯網架構的連接方法過程中，從步驟1至步驟6都是在每一個用戶端裝置100出廠前就與雲端裝置500完成連接，即每一個用戶端裝置100出廠後，就已經自雲端裝置500獲得完整的訊息包括:1.Sever_pub_key；2.Client_pri_key；3.MQTT_Broker IP；4.MQTT_Broker username/passward；5.client_Share_key；6.share_key_expiry date time。當物聯網系統啟動後，每一個用戶端裝置100所要傳送給雲端裝置500處理的資料串，都會根據MQTT_Broker IP傳送至代理伺服裝置700，再由代理伺服裝置700直接將用戶端裝置100資料串傳送給雲端裝置500。故自步驟7至步驟10之間的訊息傳遞過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率。由於代理伺服裝置700只是將用戶端裝置100上傳的資料直接傳送給雲端裝置500，故可以降低代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼被破解的機率，可以更增加物聯網通信過程的安全性。

【0060】 接著，本創作還可以在第三圖的步驟4中，將用戶端裝置100向雲端裝置500取得代理伺服裝置700的MQTT_Broker IP、MQTT_Broker 帳號及MQTT_Broker密碼的過程，分為兩次來執行；例如: 第一次是用戶端裝置100以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)通過https要求取得client_share_key及MQTT_Broker IP；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認

client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將client_share_key及MQTT_Broker IP等以client_pub_key編碼後回傳至用戶端裝置100；第二次是用戶端裝置100再以編碼後的client_uuid (即client_uuid會根據sever_pub_key轉成亂碼)，通過https要求取得MQTT_Broker 帳號及密碼；而當雲端裝置500收到轉成亂碼的client_uuid後，即會根據sever_pri_key進行解碼，以確認client_uuid是否正確；待雲端裝置500確認client_uuid正確後，雲端裝置500將MQTT_Broker 帳號及密碼等以client_pub_key編碼後回傳至用戶端裝置100。特別要說明的，第一次及第二次所要取得的內容中，只要求將MQTT_Broker的IP、帳號及密碼分兩次取得，其他並不加以限制。

【0061】 接著，詳細說明本創作的物聯網架構應用在產品的物流管理系統上的實施方式。

【0062】 首先，請參考第五圖，是本創作的物聯網產品物流管理系統架構示意圖。如第五圖所示，本創作的一種產品的物流管理系統，包括: 多個產品10、配置於每一個產品上的電子標籤12、至少一個用戶端裝置100(例如:個人電腦、筆記本電腦、智慧型手機、智慧型可攜式裝置、智慧型讀取裝置等)，且每一個用戶端裝置100可以讀取及傳送電子標籤12內部的訊息及藉由一個代理伺服裝置700傳送電子標籤12內部訊息至雲端裝置500及一個與雲端裝置500連接的顯示模組600所組成，物流管理系統之間使用無線網路形成通信鏈路；其中，每一個用戶端裝置100均為一種具有浮動IP的無線通信裝置，且每一個用戶端裝置100均具有一特定的用戶識別碼；雲端裝置500，是一種固定式網域名稱系統(DNS)，其具有伺服器(sever)之功能並且

具有與每一個用戶端裝置100通信之功能，藉由每一個用戶端裝置100的特定用戶識別碼確認每一個用戶端裝置100均為物聯網中的其中之一個用戶端裝置；代理伺服裝置700(即MQTT Broker)，是一種隨時變動的浮動IP，具有一網址及密碼，其最主要的工作是將確認是為物聯網中的用戶端裝置100所傳送的編碼資料串在接收後，直接傳送出至雲端裝置500，並能與雲端裝置500通信；其中，於雲端裝置500提供代理伺服裝置700的網址及密碼予物聯網中的每一個用戶端裝置100後，這些用戶端裝置100只能與代理伺服裝置700通信，並再由代理伺服裝置700與雲端裝置500通信，以便將每一個用戶端裝置100所要傳送的產品10訊息傳至雲端裝置500中，並於雲端裝置500處理後，將處理後的結果於一個顯示模組600上顯示出來。

【0063】 接著，請參考第六圖，是本創作的用戶端裝置(例如:個人電腦、筆記本電腦、智慧型手機、智慧型可攜式裝置、智慧型讀取裝置等)結構示意圖；如第六圖所示，用戶端裝置100包括控制器110、多個天線120、多個輸出入接口130及一個無線傳輸模組140所組成；再接著，請參考第七A圖，是本創作的雲端裝置結構示意圖；如第七A圖所示，雲端裝置500是由一個接收/發射介面模組510、資料處理模組520與記憶體模組530所組成，其中，在記憶體模組530中已建立了安全判斷資料庫，包括編號、用戶識別碼(例如:MAC Address)、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等資料，故資料處理模組520會執行比對及驗證，例如，至少比對每一個用戶端裝置100所使用的用戶識別碼(例如:MAC Address)是否已經儲存在雲端裝置500的記憶體模組530資料庫中；此外，雲端裝置500還可以通過接收/發射介面模組510與每一個用戶端裝置100、代理伺服裝置700及顯示模

組600通信。

【0064】 當物流管理系統運作時，每一個用戶端裝置100已經以無線傳輸模組140通過https向雲端裝置500進行登錄，並且已經確認每一個用戶端裝置100均為物聯網中的用戶端裝置，同時，每一個用戶端裝置100也已經確認收到完整的訊息，包括:1.Sever_pub_key；2.Client_pri_key；3.MQTT_Broker IP；4.MQTT_Broker username/passward；5.client_Share_key；6.Share_key_expiry date time；其登錄及驗證過程，如前述實施例所述。而在本物流管理系統實施例中的用戶端裝置100為一種讀寫裝置，其可以藉由天線120發出電訊號至產品10上的電子標籤12，並觸發電子標籤12將儲存於內部的訊息傳送出來，再由讀寫裝置的天線120接收電子標籤12傳送的訊息，經過輸出入接口130再傳遞至控制器110處理，並在使用client_share_key將client_uuid及電子標籤12訊息資料進行編碼後，由無線傳輸模組140將編碼後的訊息傳送到代理伺服裝置700；而代理伺服裝置700在收到用戶端裝置所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去；在雲端裝置500的接收/發射介面模組510收到代理伺服裝置700的資料串後，會再經過資料處理模組520解碼，此時，可以將電子標籤12內部的訊息儲存至記憶體模組530所設定的儲存空間，例如，儲存至特定公司所設定的儲存空間；或者可以同步將電子標籤12內部的訊息傳送到顯示模組600上顯示出資訊；也或者待資料處理模組520將多筆電子標籤12內部的訊息經過特定處理後，再傳送到顯示模組600上顯示出設定的資訊狀況；其中，資料處理模組520在進行安全辨識處理時，還可以將接收/發射介面模組510收到的每一個讀寫裝置的編號、用戶識別碼、所在倉庫的

名稱或編號以及其所在位置的座標(包括經緯度)等資料與儲存在記憶體模組530中的資料進行比對，如第七B圖所示，是本創作儲存在記憶體模組530中的安全判斷資料示意圖；若驗證所收到的client_uuid及資料串不完整或不正確時，則進行紀錄。

【0065】 在本實施例中，不正確訊息的產生可能包括:每一個用戶端裝置100發佈信息頻率有一定的規律性，如若產生某用戶端裝置100 以不正常或過多頻率來發佈的信息；或某用戶端裝置100 的ip 對應到的client_uuid不正確，則可能有盜用問題；或是，若某 client_uuid 有配合上Geo Location的資料上傳，可以藉由驗證GeoLocation 的合理性來驗證(是否某個client_uuid這一分鐘在亞洲，下一分鐘在北美)；或代理伺服裝置700本身頻率發佈信息非經MQTT方式，而試圖連接雲端裝置500等；則視為不正確的訊息。當不正確的訊息持續出現時，則判斷代理伺服裝置700可能被駭客攻擊；則雲端裝置500可以選擇關閉此代理伺服裝置700。此外，將雲端裝置500處理後的訊息傳送到顯示模組600的方式，可以示無線傳輸(WiFi, Bluetooth)或是有線傳輸。很明顯的，在本創作的物聯網連接架構中，在整個用戶端裝置100將資料串遞給雲端裝置500的過程中，雲端裝置500並不會直接暴露出自己的位址，故可以降低雲端裝置500被駭客攻擊的機率，可以大幅度的提高物聯網的安全性。

【0066】 要強調的是，經由前述的詳細說明，在本創作之後的產品物流管理系統實施例說明過程中，其每一個用戶端裝置100已經通過無線傳輸模組140向雲端裝置500進行登錄，並且已經確認每一個用戶端裝置100均為物聯網中的用戶端裝置，同時，每一個用戶端裝置100也已經確認收到完整

的訊息，包括代理伺服裝置700的MQTT_Broker IP及MQTT_Broker 帳號及密碼等，不再詳細贅述之。

【0067】 接著，請參考第八圖，係本創作的物聯網產品物流管理系統第一實施例示意圖。如第八圖所示，本創作的產品物流管理系統包括第一位置區域1，例如產品存放的倉庫；而產品10可以是任何貨物，例如，運動鞋、皮包、衣服等消費性產品。第一位置區域1內存放多個產品10，且每一產品10上均配置有一個電子標籤12，這些電子標籤12可以選擇在產品10存放於第一位置區域1後，再逐一貼上；同時，此電子標籤12中至少儲存有產品10的品名及識別編碼(ID code)；第一位置區域1具有一個出入口，且此出入口上配置有至少一個可以做為用戶端裝置100 的第一讀寫裝置31/32/33(例如: 三個第一讀寫裝置的安全辨識碼分別為A001 、A002及A003)，每一個第一讀寫裝置31/32/33均有一個安全辨識碼、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等訊息；而在出入口上配置多個第一讀寫裝置的目的，是當單位時間內產品通過出入口的數量增加時，可以有效的提高產品訊息讀寫的速度及正確率，而降低產品訊息讀寫的失誤率。

【0068】 當存放於第一位置區域1的產品10需要運送至銷售據點時，每一個產品10都一定要經過配置在出入口上的至少一個第一讀寫裝置31/32/33，而每一個第一讀寫裝置31/32/33上的第一天線120會發射出訊號，使得每一個通過第一讀寫裝置31/32/33的電子標籤12在接收到第一天線120會發射出的訊號後，即會觸發電子標籤12將儲存於內部的產品訊息傳送出來，再由第一讀寫裝置31/32/33的第一天線120接收電子標籤12傳送的訊

息，經過輸出入接口130傳遞至控制器110處理後，並在使用client_share_key將client_uuid及電子標籤12訊息資料進行編碼後，由無線傳輸模組140將編碼後的訊息傳送到代理伺服裝置700；而代理伺服裝置700在收到用戶端裝置所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去；在雲端裝置500的接收/發射介面模組510收到代理伺服裝置700的資料串後，會再經過資料處理模組520解碼，此時，可以將電子標籤12內部的訊息儲存至記憶體模組530所設定的儲存空間，例如，儲存至特定公司所設定的儲存空間；或者可以同步將電子標籤12內部的訊息傳送到顯示模組600上顯示出資訊；也或者待資料處理模組520將多筆電子標籤12內部的訊息經過特定處理後，再傳送到顯示模組600上顯示出設定的資訊狀況，使得雲端裝置500可以掌握有哪些產品及數量已經移出第一位置區域1；因而，可以進一步與存放在記憶體模組530內的倉儲資料進行比對，已確認兩者數量是否相同。

【0069】 接著，上述被移出的產品10需要被運送到另一區域進行販售時，可能需要透過運輸裝置將這些產品送到設定的區域進行倉儲；例如，要將放在上海自由貿易區中的一萬雙運動鞋運送至北京王府井大街的銷售點倉儲。為了確保所要運送的運動鞋如期如數的送到設定的區域進行倉儲，因此，進入運輸裝置的入口時，就必須確認是那些運動鞋進入運輸裝置(例如:一個貨櫃)，同時還必須確保整個運送過程中，放在運輸裝置中的產品是沒有被缺少的。

【0070】 為了解決上述需求，本創作的產品物流管理系統第一實施例接著進行如下的程序。運輸裝置上的貨櫃(或稱為第二位置區域2)配置一個

出入口，出入口上配置至少一個可以做為用戶端裝置100 的第二讀寫裝置41/42/43(例如：三個第二讀寫裝置的安全辨識碼分別為P004、P005及P006)，而每一個第二讀寫裝置41/42/43上的第二天線220會發射出訊號，使得每一個通過第二讀寫裝置41/42/43的電子標籤12在接收到第二天線220會發射出的訊號後，即會觸發電子標籤12將儲存於內部的產品訊息傳送出來，再由第二讀寫裝置41/42/43的第二天線220接收電子標籤12傳送的訊息，經過輸出入接口130傳遞至控制器210處理後，並在使用client_share_key將client_uuid及電子標籤12訊息資料進行編碼後，由無線傳輸模組240將編碼後的訊息傳送到代理伺服裝置700；而代理伺服裝置700在收到用戶端裝置所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去；在雲端裝置500的接收/發射介面模組510收到代理伺服裝置700的資料串後，會再經過資料處理模組520解碼，此時，可以將電子標籤12內部的訊息儲存至記憶體模組530所設定的儲存空間，例如，儲存至特定公司所設定的儲存空間；或者可以同步將電子標籤12內部的訊息傳送到顯示模組600上顯示出資訊；也或者待資料處理模組520將多筆電子標籤12內部的訊息經過特定處理後，再傳送到顯示模組600上顯示出設定的資訊狀況；使得雲端裝置500可以知道送進第二位置區域2的產品數量以及每一產品的品名及識別編碼，可以進一步與記憶體模組530內的倉儲資料進行比對，使得雲端裝置500可以掌握有哪些產品及數量已經進入至第二位置區域2存放；此外，本實施例在對第二讀寫裝置41/42/43所傳送訊息的安全確認方式與前述相同，不再另行說明；其中的差異處在於安全辨識碼，以本實施例而言，P004中的P代表是配置在運輸貨櫃上的讀寫裝置，故其可以選擇傳送或是不傳送

座標(包括經/緯度)訊息。

【0071】 再接著，請參考第九圖，係本創作的物聯網產品物流管理系統第一實施例中的第二位置區域示意圖。在第二位置區域2中，進一步配置有至少一個可以做為用戶端裝置100 的第三讀寫裝置51/52/53(例如: 三個第三讀寫裝置的安全辨識碼分別為G007、G008及G009)，其中，每一個第三讀寫裝置51/52/53是至少一個第三天線320、第三控制模組310、定位裝置150及一第三無線傳輸模組340所組成。這些第三讀寫裝置51/52/53用以對放置在第二位置區域2中的產品10進行掃描或監控，以確保存放在第二位置區域2的產品數量都安全的放置在第二位置區域2中；很明顯的，在本實施例中，此第二位置區域2為一種運送產品的運輸貨櫃，已使整個產品10在運送過程中，這些第三讀寫裝置51/52/53都會持續地經由第三天線320發出訊息至產品10上的電子標籤12後，即會觸發電子標籤12將儲存於內部的產品訊息發射出來，再由第三讀寫裝置51/52/53的第三天線320接收電子標籤12發射的訊息，經過輸出入接口130傳遞至控制器110處理後，並在使用client_share_key將client_uuid及電子標籤12訊息資料進行編碼後，由無線傳輸模組140將編碼後的訊息傳送到代理伺服裝置700；而代理伺服裝置700在收到用戶端裝置所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去；在雲端裝置500的接收/發射介面模組510收到代理伺服裝置700的資料串後，會再經過資料處理模組520解碼，此時，可以將電子標籤12內部的訊息儲存至記憶體模組530所設定的儲存空間，例如，儲存至特定公司所設定的儲存空間；或者可以同步將電子標籤12內部的訊息傳送到顯示模組600上顯示出資訊；也或者待資料處理模組520將多筆電子標

籤12內部的訊息經過特定處理後，再傳送到顯示模組600上顯示出設定的資訊狀況；使得雲端裝置500可以藉由GPS座標訊息來判斷出產品目前運送至何處。

【0072】 此外，要強調的是，上述實施例所述的電子標籤可以包括NFC、RFID、ID stamp或ID貼紙等其中一種；其中，如果放置在第二位置區域2(或稱為貨櫃2)中的產品10上的電子標籤12是RFID時，則配置在第二位置區域(貨櫃)2中的第三讀寫裝置51/52/53可以固定在一位置上；而若當放置在第二位置區域(貨櫃)2中的產品10上的電子標籤12是NFC、ID stamp或ID貼紙時，則配置在第二位置區域2中的第三讀寫裝置51/52/53就必須要能在第二位置區域(貨櫃)2中移動，以確定能掃描到每一個產品10。再者，系統上的電子標籤12與第一天線120、第二天線220及第三天線320的頻率是相互匹配。

【0073】 另外，還要強調的是，雲端裝置500是一種固定式網域名稱系統(DNS)，其具有伺服器(sever)之功能並且具有與用戶端裝置100通信之功能，是由一個接收/發射介面模組510、資料處理模組520與記憶體模組530所組成，並且可以通過接收/發射介面模組510與顯示模組600連接；資料處理模組520已經將配置在第一位置區域1的第一出入口上的至少一個第一讀寫裝置31/32/33 (例如配置3個第一讀寫裝置)的安全辨識碼、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等訊息紀錄並儲存在記憶體模組530的記憶體中；同樣的，資料處理模組520也已經將配置在第二位置區域2的第二出入口上的至少一個第二讀寫裝置41/42/43的安全辨識碼(例如配置3個第二讀寫裝置)、所在倉庫的名稱或編號以及其所在位置的座標(包

括經緯度)等訊息紀錄並儲存在記憶體模組530的的記憶體中；而配置在第二位置區域2中的至少一個第三讀寫裝置51/52/53，其安全辨識碼、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等訊息，也會被紀錄並儲存在記憶體模組530的記憶體中，如第七B圖及第七C圖所示，其中，第七C圖係本創作儲存在記憶體模組內的倉儲資料示意圖。當資料處理模組520判斷所收到的client_uuid及資料串正確時，就可以將這些訊息儲存至記憶體模組530所設定的特定儲存空間；當判斷所收到的client_uuid及資料串不正確時或是錯誤時，表示所收到的讀寫裝置並非物流管理系統所傳送，可能有駭客訊息要入侵或客戶端資料異常，故雲端裝置500的資料處理模組520就會依據判別結果來決定是忽略此訊息又或者可以選擇關閉此一代理伺服裝置700或者發出警告通知，不進行後續的處理。

【0074】 此外，在第一位置區域1中的產品10訊息可以在產品10進入第一位置區域1之前就已經記錄在雲端裝置500在資料處理模組520或記憶體模組530中；其也可以選擇在將複數個產品10都經過第一位置區域1的第一讀寫裝置31/32/33後，將通過第一位置區域1的產品10數量以及每一產品的品名及識別編碼都記錄後，再建立產品在第一位置區域1中的產品數量以及每一產品的品名及識別編碼資料，並也記錄在雲端裝置500在資料處理模組520或記憶體模組530中，如第七C圖所示；此時，雲端裝置500在資料處理模組520執行儲存至記憶體模組530的過程中，還會增加一個資料儲存的時間記錄，以做為後續比對的資料之一。而選擇以前述何種方式記錄第一位置區域1中的產品數量以及每一產品的品名及識別編碼資料，本創作並不加以限制。

【0075】 很明顯的，當第一位置區域1中的產品數量以及每一產品的品名及識別編碼等資料已經建立在雲端裝置500的記憶體模組530後，即會通過雲端裝置500內的資料處理模組520進行處理及比對；當資料處理模組520經過安全判斷及訊息處理後，即會知道通過第一位置區域1的產品數量以及每一產品的品名及識別編碼，可以進一步與記憶體模組530內的倉儲資料(如第七C圖所示)進行比對，使得雲端裝置500可以掌握有哪些產品及數量已經移出第一位置區域1。此時，雲端裝置500可以通過接收/發射介面模組510與顯示器就600連接，用以將原儲存在第一位置區域1的產品數量、產品的品名以及記錄的時間都顯示出來；或是顯示出在何時已經有哪些產品及數量已經移出第一位置區域1，及還有多少產品及數量還存放在第一位置區域1中；可以使得管理者能夠掌握第一位置區域1中的產品數量及產品的品名；當然，管理者也可以透過雲端裝置500查詢的方式，知道存放在第一位置區域1的產品品名及其識別編碼。

【0076】 最後，經過本創作的產品物流管理系統第一實施例的運作後，管理者可以在與雲端裝置500連接的顯示模組600上看到目前在倉庫中還存放著多少產品、目前有多少產品正在運送途中、目前已運送至何處及預定何時會到達目的地(王府井大街)等訊息；同時，管理者也可以通過雲端裝置500對管理系統中的產品查詢其產品的品名及識別編碼。同樣的，在本創作的另一較佳實施例中，配置在第二位置區域2中的第一讀寫裝置31/32/33也可以如第三讀寫裝置51/52/53就必須要能在第一位置區域1中移動，以確定能掃描到每一個產品10。

【0077】 在本創作的物品管理系統可以進一步與物品倉儲及銷售管

理系統整合成為一個完整的系統，其詳細的運作過程說明如下。

【0078】 請參考第十圖，是本創作物聯網產品物流管理系統第二實施例的物品倉儲管理示意圖。首先，當多個貼有電子標籤12的產品10已經放置於第一倉儲區域1(或稱為第一位置區域1)，例如在第一實施例中，已將產品(一萬雙運動鞋)運送到王府井大街的第一倉儲區域1中存放，並且放置於第一倉儲區域1中的產品數量、產品品名及識別編碼也已經儲存在雲端裝置的記憶裝置中；很明顯的，第一倉儲區域1具有一個出入口，且此出入口上配置有至少一個第一讀寫裝置，每一個第一讀寫裝置均有一個編號31/32/33(例如：三個第一讀寫裝置的安全辨識碼分別為A001、A002及A003)、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等訊息，並且也都已經紀錄或儲存在雲端裝置的記憶裝置中。接著，當管理者要將放置於第一倉儲區域1中的產品分別送到不同的銷售據點時，即可以由本創作的物品倉儲及銷售管理系統來達成。

【0079】 當管理者要將放置於第一倉儲區域1中的產品(一萬雙運動鞋)分別送五千雙運動鞋到第一銷售據點、三千雙運動鞋到第二銷售據點及一千雙運動鞋到第三銷售據點；此時，當產品編號1至編號5000的運動鞋要運送到第一銷售據點時，這些編號1至編號5000的運動鞋會通過第一倉儲區域1的出入口，而出入口上配置有至少一個第一讀寫裝置，其中，每一個第一讀寫裝置31/32/33上的第一天線120會發射出訊號，使得每一個通過第一讀寫裝置31/32/33的電子標籤12在接收到第一天線120會發射出的訊號後，即會觸發電子標籤12將儲存於內部的產品訊息發射出來，再由第一讀寫裝置31/32/33的第一天線120接收電子標籤12發射的訊息，經過輸出入接口130

傳遞至控制器110處理後，並在使用client_share_key將client_uuid及電子標籤12訊息資料進行編碼後，由無線傳輸模組140將編碼後的訊息傳送到代理伺服裝置700；而代理伺服裝置700在收到用戶端裝置所傳送的資料串後，不做任何處理，而是直接將接收到的資料串直接傳送出去；在雲端裝置500的接收/發射介面模組510收到代理伺服裝置700的資料串後，會再經過資料處理模組520解碼，此時，可以將電子標籤12內部的訊息儲存至記憶體模組530所設定的儲存空間，例如，儲存至特定公司所設定的儲存空間；其中，第一讀寫裝置31/32/33所傳送的訊息包括其編號、所在倉庫的名稱或編號、其所在位置的座標(包括經緯度)、電子標籤中的產品品名及識別編碼；當編號1至編號5000的運動鞋都經過第一倉儲區域1的第一讀寫裝置31/32/33後，很明顯的，雲端裝置500的資料處理模組520處理後，即會知道編號1至編號5000的運動鞋已經移出第一倉儲區域1，而雲端裝置500內的資料處理模組520就會將編號1至編號5000的運動鞋移出第一倉儲區域1的時間記錄，例如:早上9點。而在雲端裝置500的資料處理模組520進行處理的過程中，資料處理模組520會先確認這些收到的訊息，是否為管理系統的第一讀寫裝置31/32/33所發出；例如，資料處理模組520至少會確認每一個送進來的第一讀寫裝置的編號、所在倉庫的名稱或編號以及其所在位置的座標(包括經緯度)等訊息，是否與儲存在記憶體模組530內的記錄訊息相同；當判斷所收到的訊息正確時，就可以將這些第一讀寫裝置31/32/33所傳送的訊息儲存至記憶體模組530所設定的特定儲存空間或者可以同步將電子標籤12內部的訊息傳送到顯示模組600上顯示出資訊；也或者待資料處理模組520將多筆電子標籤12內部的訊息經過特定處理後，再傳送到顯示模組600上顯示出設定

的資訊狀況；使得雲端裝置500；當判斷所收到的訊息不正確時，表示可能有駭客訊息要入侵，故資料處理模組就會忽略此訊息，不進行後續的處理又或者可以選擇關閉此代理伺服裝置700或者進一步發出警告至雲端裝置。

【0080】 同樣的，當編號5001至編號8000的運動鞋通過第一倉儲區域1的出入口上的至少一個第一讀寫裝置31/32/33後，通過相同的系統運作，雲端裝置500即會知道編號5001至編號8000的運動鞋已經移出第一倉儲區域1，而雲端裝置500內的資料處理模組520就會將編號5001至編號8000的運動鞋移出第一倉儲區域1的時間記錄，例如:早上10點。當編號8001至編號9000的運動鞋通過第一倉儲區域1的出入口上的至少一個第一讀寫裝置31/32/33後，通過相同的系統運作，雲端裝置500即會知道編號8001至編號9000的運動鞋已經移出第一倉儲區域1，而雲端裝置500內的資料處理模組520就會將編號8001至編號9000的運動鞋移出第一倉儲區域1的時間記錄，例如:早上11點。當第二實施例運作到此時，管理者可以在與雲端裝置500連接的顯示模組600上看到目前在倉庫中還存放著編號9001至編號10000的運動鞋；而編號1至編號5000的運動鞋、編號5001至編號8000的運動鞋及編號8001至編號9000的運動鞋則顯示在不同的時間已經移出第一倉儲區域1。

【0081】 接著，當編號1至編號5000的運動鞋已經運送到第一銷售據點後，即會通過配置在第一銷售據點中的讀寫裝置61(例如: 安全辨識碼為S010)，因此，透過系統前述相同的運作後，管理者可以在與雲端裝置500連接的顯示模組600上看到目前在倉庫中還存放著編號9001至編號10000的運動鞋；而編號1至編號5000的運動鞋在早上11點已經存放在第一銷售據點中，而管理者也可以通過雲端裝置500進行產品訊息的查詢，例如查詢編號

1至編號5000運動鞋的尺寸訊息。同樣的，當編號5001至編號8000的運動鞋已經運送到第二銷售據點後，即會通過配置在第二銷售據點中的讀寫裝置62(例如: 安全辨識碼為S011)，因此，透過系統前述相同的運作後，管理者可以在與雲端裝置500連接的顯示模組600上看到目前在倉庫中還存放著編號9001至編號10000的運動鞋、編號1至編號5000的運動鞋在早上11點已經存放在第一銷售據點、以及編號5001至編號8000的運動鞋在早上11點30分已經存放在第二銷售據點中，而管理者也可以通過雲端裝置500進行產品訊息的查詢，例如查詢編號5001至編號8000運動鞋的尺寸訊息。再接著，當編號8001至編號9000的運動鞋已經運送到第三銷售據點後，即會通過配置在第三銷售據點中的讀寫裝置63(例如: 安全辨識碼為S012)，因此，透過系統前述相同的運作後，管理者可以在與雲端裝置500連接的顯示模組600上看到目前在倉庫中還存放著編號9001至編號10000的運動鞋，編號1至編號5000的運動鞋在早上11點已經存放在第一銷售據點、編號5001至編號8000的運動鞋在早上11點30分已經存放在第二銷售據點、以及編號8001至編號9000的運動鞋在早上12點已經存放在第三銷售據點中，而管理者也可以通過雲端裝置500進行產品訊息的查詢，例如查詢編號8001至編號9000運動鞋的尺寸訊息。

【0082】 最後，說明本第二實施例的銷售運作，請參考第十一圖，是本創作的物聯網產品物流管理系統第二實施例的銷售管理示意圖。如第十一圖所示，當客戶已經確定所要購買的產品(例如:運動鞋編號第999)後，服務人員會攜帶產品10至櫃台進行結帳。此時，銷售人員會將產品10上的電子標籤12拿至配置在櫃台上的讀寫裝置71(例如:編號為CS0100)，其中，配

置在櫃台上的讀寫裝置71除了與一般讀寫裝置有相同的結構外，還進一步有一消磁模組170；當確定客戶已經完成付款後，即由櫃台通知讀寫裝置71發出編號第999的運動鞋已經售出的訊息，由於配置在櫃台上的讀寫裝置71的編號、所在銷售點的名稱或編號及其所在位置的座標(包括經緯度)等訊息已經儲存在雲端裝置中，故當配置在櫃台上的讀寫裝置71將已完成產品銷售的訊息送出後，經過雲端裝置500的資料處理模組520處理後，就會通過接收/發射介面模組510在顯示模組600上顯示出原先存放在第一銷售點的編號第999的運動鞋已經售出的訊息。因此，透過系統前述相同的運作後，管理者可以在與雲端裝置500連接的顯示模組600上看到存放在第一銷售點的編號第999的運動鞋已經售出的訊息。同樣的，當存放在第二銷售點的讀寫裝置(未顯示於圖中)送出編號第5999的運動鞋已經售出的訊息及存放在第三銷售點的讀寫裝置(未顯示於圖中)送出編號第8999的運動鞋已經售出的訊息後，經過雲端裝置500的資料處理模組520處理後，就會通過接收/發射介面模組510在顯示模組600上顯示第一銷售點的編號第999的運動鞋已經售出的訊息、第二銷售點的編號第5999的運動鞋已經售出的訊息以及第三銷售點的編號第8999的運動鞋已經售出的訊息；其最後顯示在顯示模組600上，其銷售訊息的顯示結果，如第十二圖所示，係本創作中的管理者訊息顯示的示意圖。

【0083】 此外，當配置在產品10上的電子標籤是使用RFID時，則此RFID可以回收再使用；當然這些配置在產品上的電子標籤12也可以使用其他型式，例如: 包括NFC、ID stamp或ID貼紙等。而本第二實施例的電子標籤12與系統中的每一支天線120/220/320的頻率是相互匹配的。

【0084】 根據上述的第一實施例與第二實施例的詳細說明後，本創作可以將其進一步組合後，即會形成本創作完整的物品倉儲、物流及銷售管理系統，故不再詳細說明。

【0085】 雖然本創作以前述之較佳實施例揭露如上，然其並非用以限定本創作，任何熟習本領域技藝者，在不脫離本創作之精神和範圍內，當可作些許之更動與潤飾，因此本創作之專利保護範圍須視本說明書所附之申請專利範圍所界定者為準。

【符號說明】

【0086】

通信方向 S1~S10

第一位置區域(第一倉儲區域) 1

產品 10

電子標籤 12

第二位置區域(貨櫃) _2

第一讀寫裝置 31/32/33

第二讀寫裝置 41/42/43

第三讀寫裝置 51/52/53

讀寫裝置 61/62/63/71

用戶端裝置 100

控制器 110/210

第三控制模組 310

第一天線 120

第二天線 220

第三天線 320

輸出入接口 130

無線傳輸模組 140/240

第三無線傳輸模組 340

定位裝置 150

消磁模組 170

雲端裝置 500

接收/發射介面模組 510

資料處理模組 520

記憶體模組 530

顯示模組 600

代理伺服裝置 700

申請專利範圍

1. 一種物聯網的連接架構，包括:

一用戶端裝置，為一具有無線通信功能的裝置，且具有一特定用戶識別碼；

一雲端裝置，具有與該用戶端裝置通信之功能，藉由該特定用戶識別碼確認該用戶端裝置為該物聯網中的其中之一該用戶端裝置；

一代理伺服裝置，具有一網址及一密碼，並能與該雲端裝置通信；

其中，於該雲端裝置提供該代理伺服裝置的該網址及該密碼予該物聯網中的該用戶端裝置後，該用戶端裝置只能與該代理伺服裝置通信，並再由該代理伺服裝置與該雲端裝置通信，以便將該用戶端裝置上的訊息傳至該雲端裝置中。

2. 一種物聯網的連接架構，包括:

多個用戶端裝置，每一該用戶端裝置均為一具有無線通信功能的裝置，且每一該用戶端裝置均具有一特定的用戶識別碼；

一雲端裝置，具有與該些用戶端裝置通信之功能，藉由該些特定用戶識別碼確認該些用戶端裝置均為該物聯網中的其中之一該用戶端裝置；

多個代理伺服裝置，每一該代理伺服裝置具有一網址及一密碼，並能與該雲端裝置通信；

其中，於該雲端裝置提供每一該代理伺服裝置的該網址及該密碼予至少一個該物聯網中的該用戶端裝置並形成配對後，該些用戶端裝置只能與配對的該代理伺服裝置通信，並再由該代理伺服裝置與該雲端裝置通信，以便將每一該用戶端裝置上的每一該訊息傳至該雲端裝置中。

3. 如申請專利範圍 1 或 2 所述的物聯網的連接架構，其中，該雲端裝置提供該代理伺服裝置的該網址及該密碼予該物聯網中的該用戶端裝置時，是可以選擇分次取得。

4. 如申請專利範圍 1 或 2 所述的物聯網的連接架構，其中，該用戶端裝置與該雲端裝置之間是使用的 https 的安全協定。

5. 如申請專利範圍 1 或 2 所述的物聯網的連接架構，其中，該代理伺服裝置為 MQTT(Message Queuing Telemetry Transport) 通信標準傳送資料。

6. 如申請專利範圍 1 或 2 所述的物聯網的連接架構，其中，當該雲端裝置確認該用戶端裝置為該物聯網中的其中之一該用戶端裝置後，該雲端裝置傳遞一個客戶辯證碼(client uuid)及一對專屬客戶使用的金鑰(client_pub_key 及 client_pri_key)至該用戶端裝置。

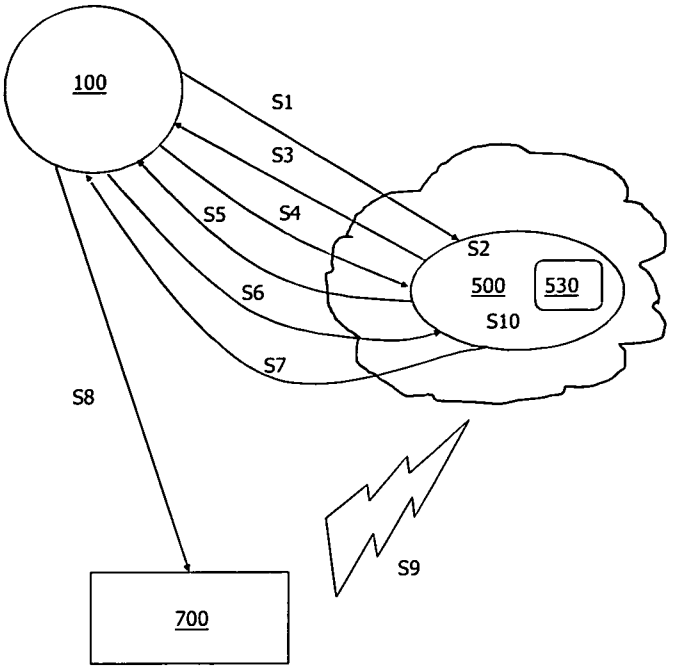
7. 如申請專利範圍 6 所述的物聯網的連接架構，其中，該對金鑰為 RSM 非對稱式金鑰(Asymmetric Key)。

8. 如申請專利範圍 6 所述的物聯網的連接架構，其中，該對金鑰為對稱式金鑰(Symmetric Key)。

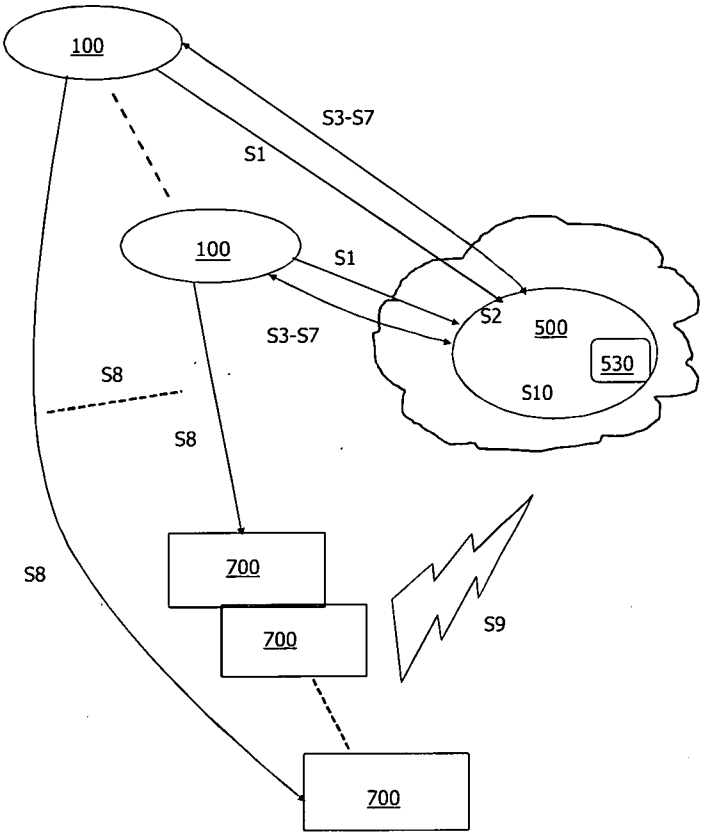
9. 如申請專利範圍 8 所述的物聯網的連接架構，其中，於該對金鑰為對稱式金鑰時，該雲端裝置進一步設定一個變動的時間(Share_key_expiry date time)並將其傳遞至該用戶端裝置。

10. 如申請專利範圍 9 所述的物聯網的連接架構，其中，該設定的變動的時間(Share_key_expiry date time)是週期性或是隨機變數。

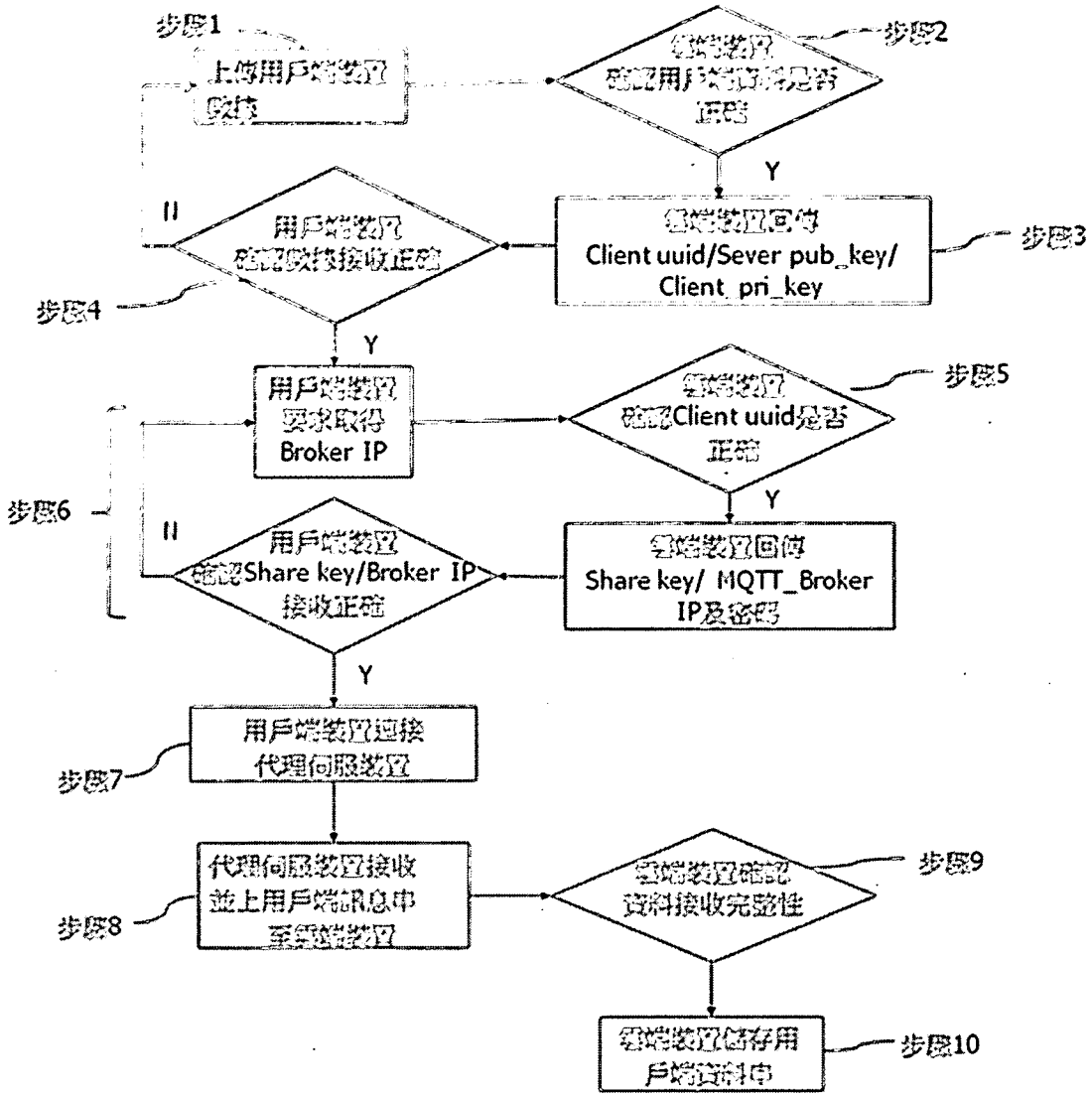
圖式



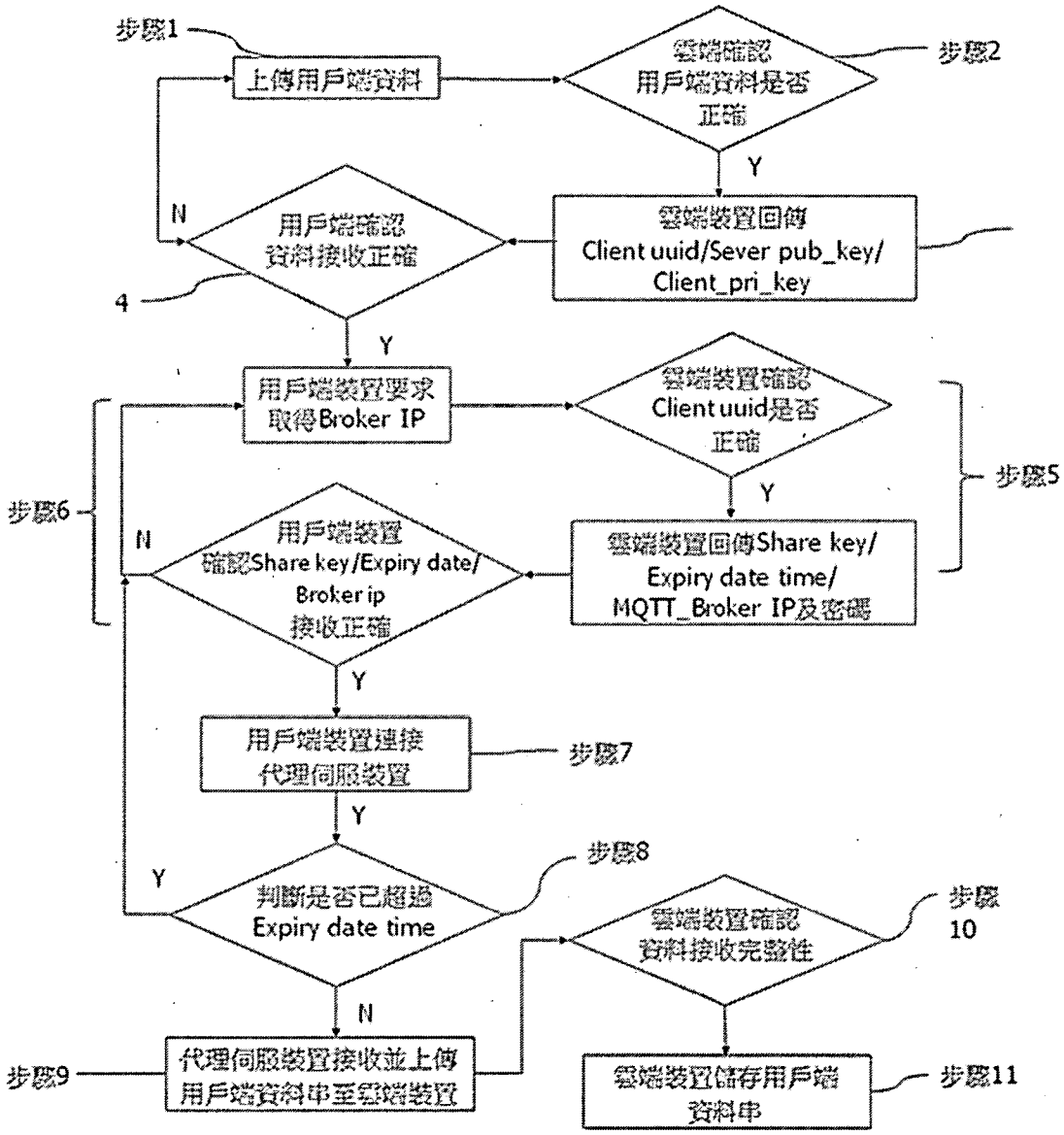
第一圖



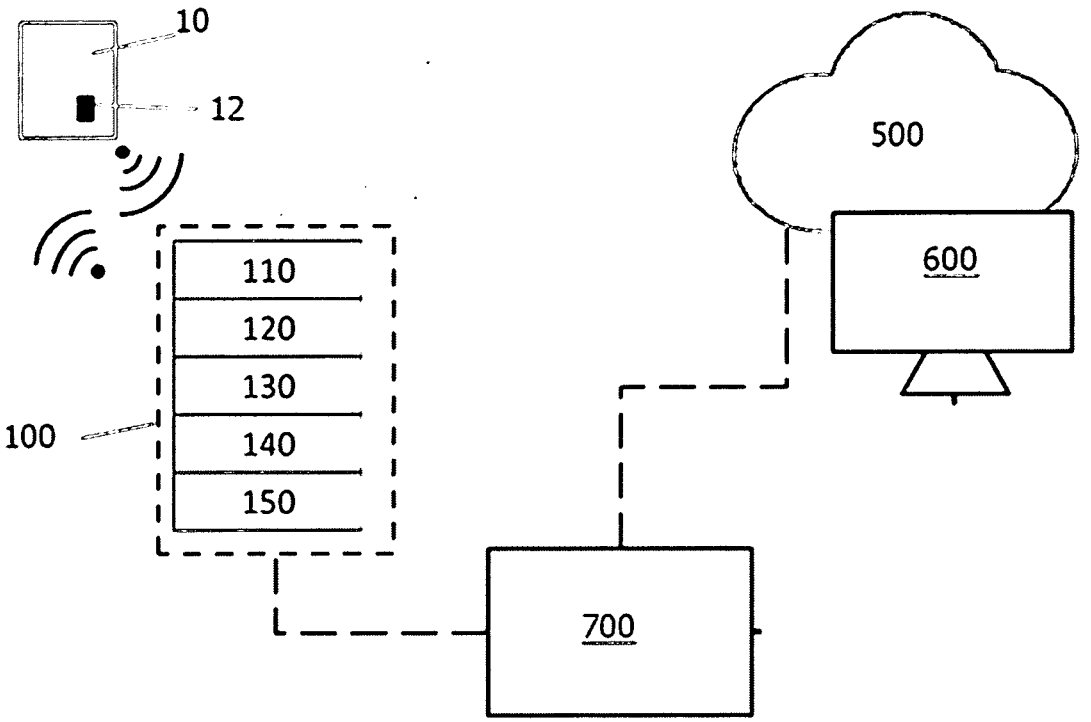
第二圖


步驟1
步驟2
Y
步驟3
Client uuid/Sever pub_key/
Client_pri_key
步驟4
Y
用戶端裝置
要求取得
Broker IP
步驟5
Y
步驟6
Share key/ MQTT_Broker
IP及密碼
Y
用戶端裝置連接
代理伺服裝置
步驟7
步驟8
步驟9
步驟10

第三圖

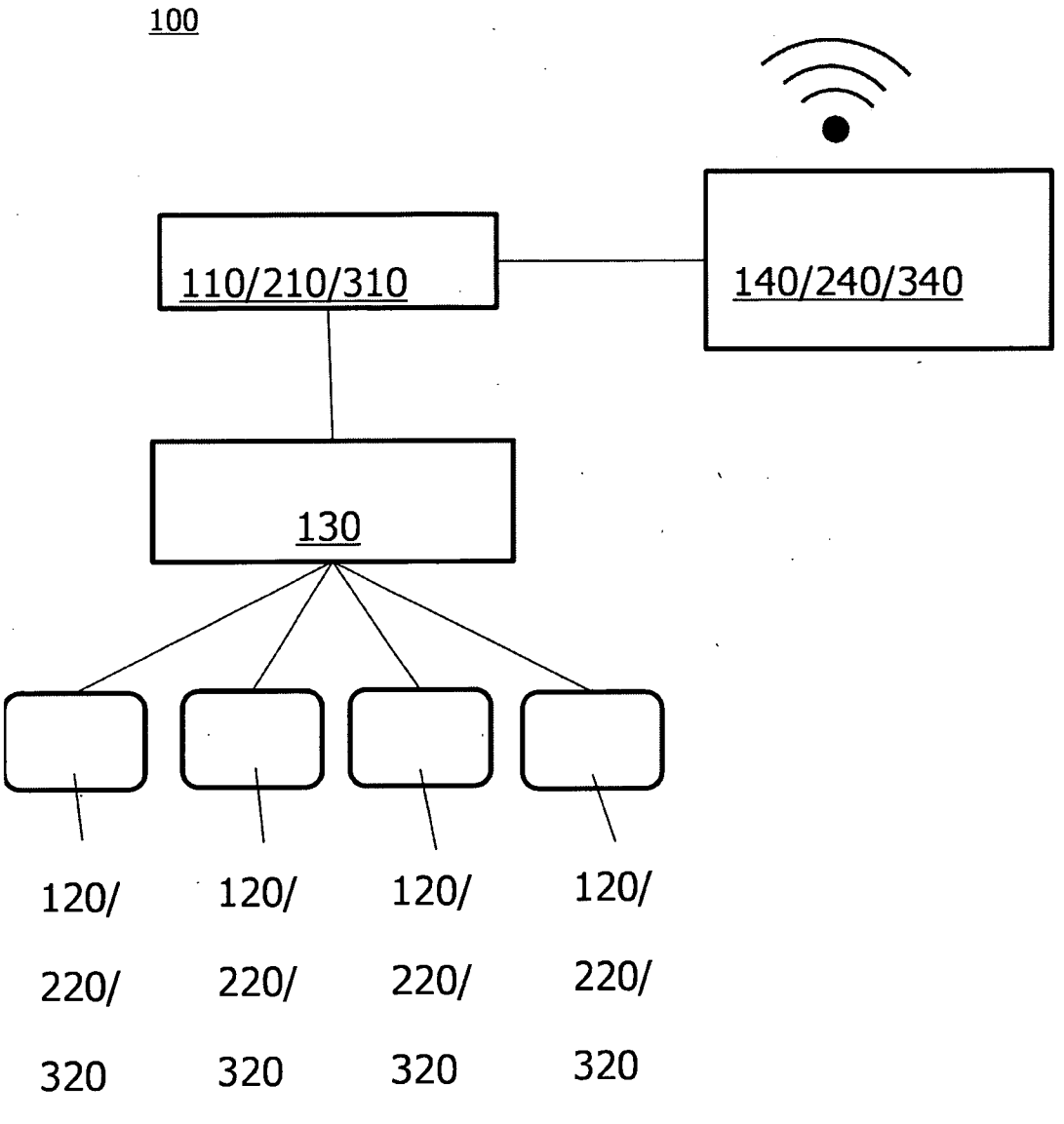

步驟1
上傳用戶端資料
雲端確認
用戶端資料是否
正確
步驟2
Y
N
用戶端確認
資料接收正確
雲端裝置回傳
Client uuid/Sever pub_key/
Client_pri_key
4
Y
用戶端裝置要求
取得Broker IP
雲端裝置確認
Client uuid是否
正確
步驟5
Y
步驟6
N
用戶端裝置
確認Share key/Expiry date/
Broker ip
接收正確
雲端裝置回傳Share key/
Expiry date time/
MQTT_Broker IP及密碼
Y
用戶端裝置連接
代理伺服裝置
步驟7
Y
步驟8
Y
判斷是否已超過
Expiry date time
雲端裝置確認
資料接收完整性
步驟
10
N
步驟9
代理伺服裝置接收並上傳
用戶端資料串至雲端裝置
雲端裝置儲存用戶端
資料串
步驟11

第四圖

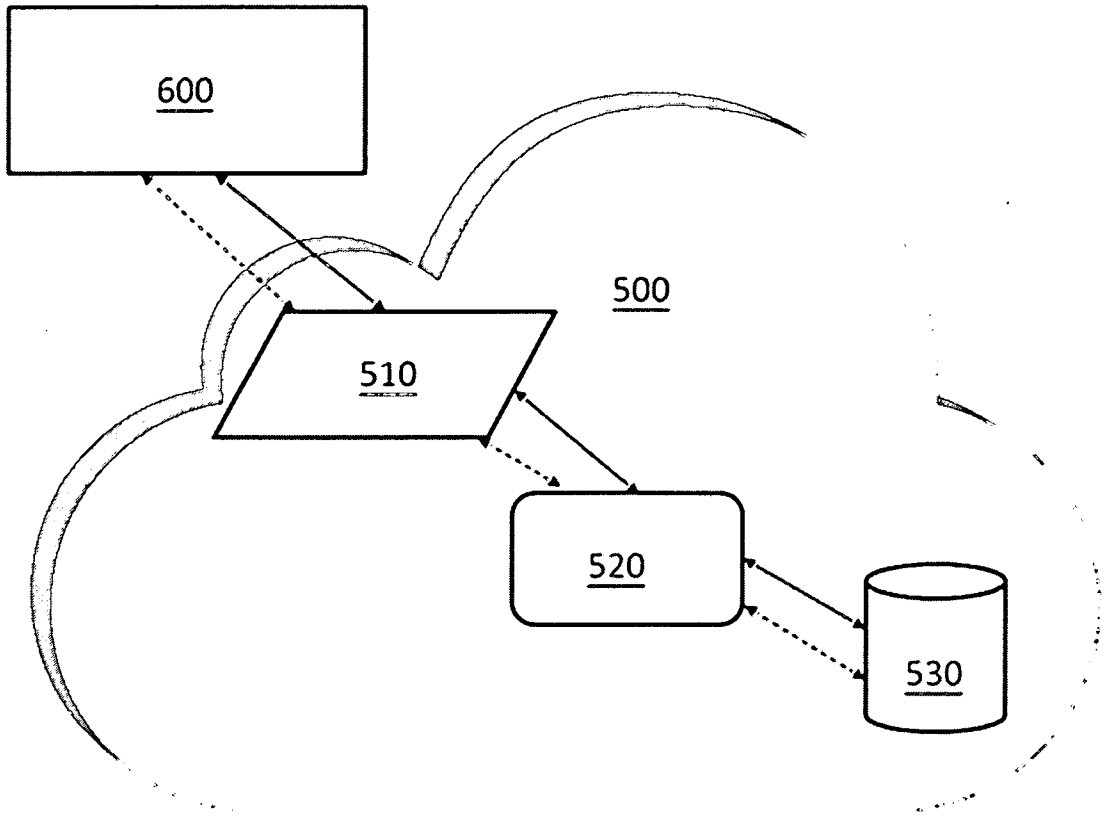


第五圖

104年 09月 21日 修正替換頁



第六圖



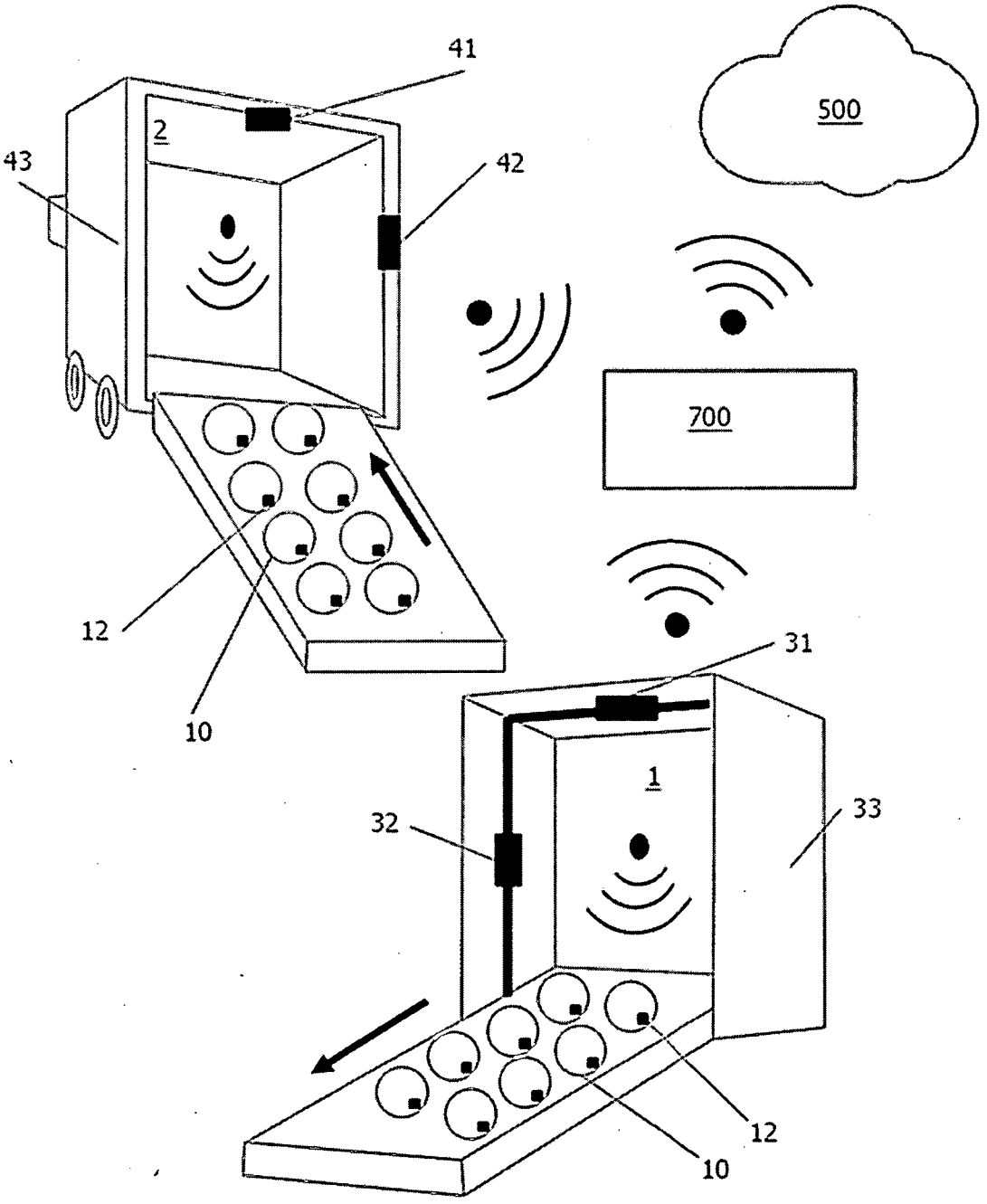
第七A圖

編號	安全辨識碼	倉庫/銷售點名稱	座標(包括經/緯度)
31	A001	上海市浦東新區順通路	30.864534/121.851318
32	A002	上海市浦東新區順通路	30.864534/121.851318
33	A003	上海市浦東新區順通路	30.864534/121.851318
41	P004		
42	P005		
43	P006		
51	G007		GPS
52	G008		GPS
53	G009		GPS
61	S010	北京華爾道夫酒店	39.916166/116.414106
62	S011	JVC百貨	39.913876/116.410869
63	S012	東方新天地	39.909889/116.413154
71	CS0100	華爾道夫酒店	39.916166/116.414106

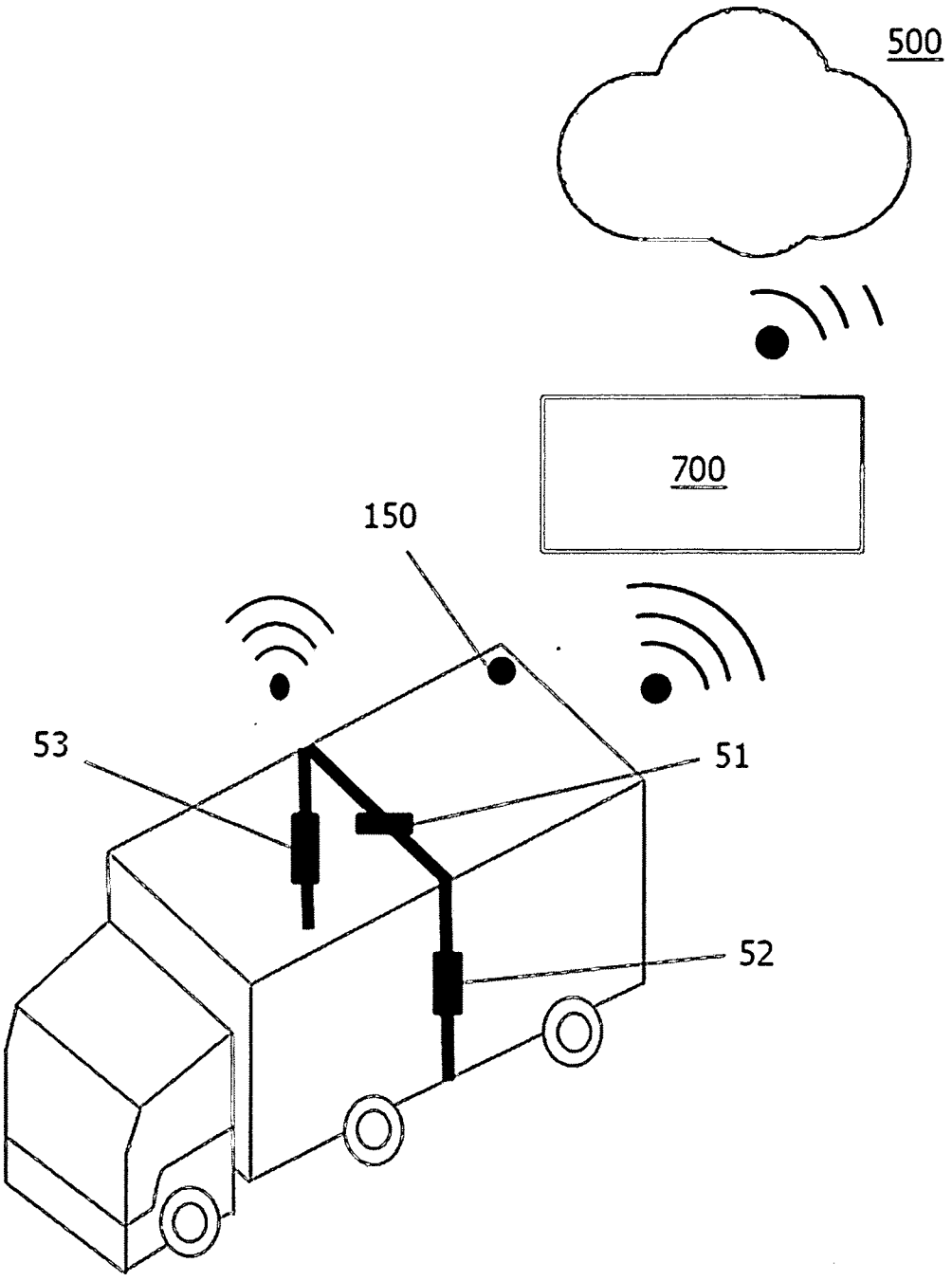
第七B圖

倉庫/銷售點名稱	品名	品名識別編碼	數量
上海市浦東新區順通路	女款常規跑鞋	581432220	4000
上海市松江步行街店	女款常規跑鞋	581432220	200
上海市浦東區順通路店	女款常規跑鞋	581432220	300
上海市洋浦區中原路店	女款常規跑鞋	581432220	300
上海市閔行區蚬橋店	女款常規跑鞋	581432220	200
北京市王府井大街	女款常規跑鞋	581432220	5000
北京市華爾道夫酒店	女款常規跑鞋	581432220	2000
北京市JVC百貨	女款常規跑鞋	581432220	5000
北京市東方新天地	女款常規跑鞋	581432220	3000

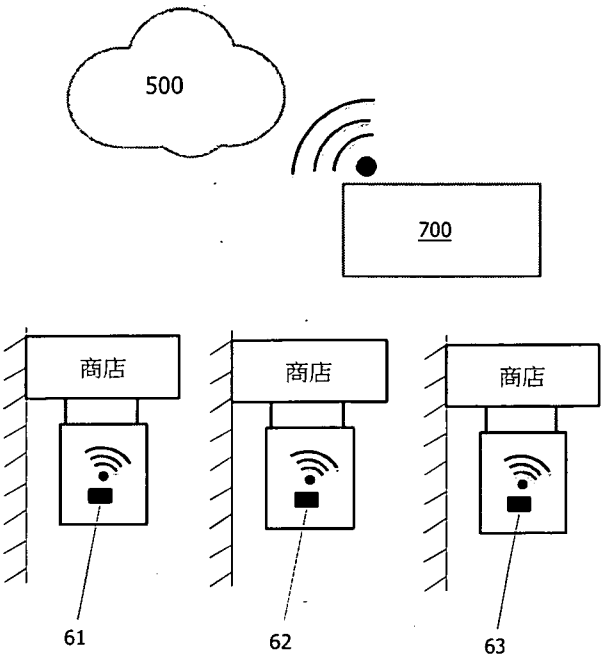
第七C圖



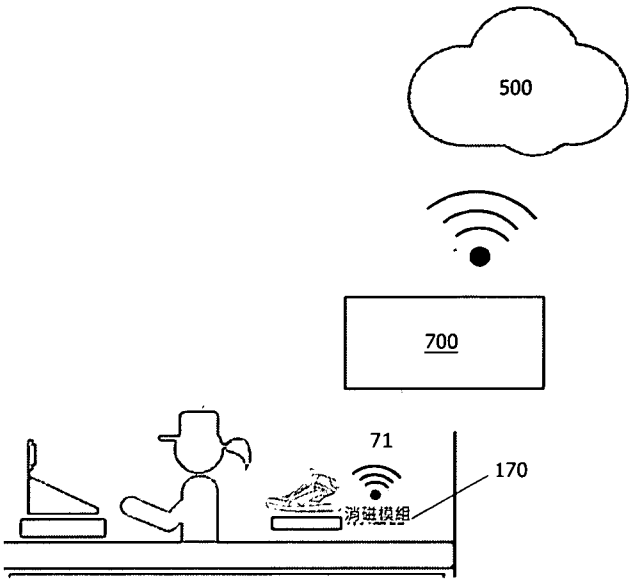
第八圖



第九圖

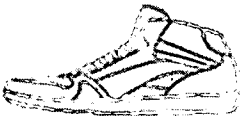


第十圖



第十一圖

104年 09月 21日 修正替換頁

產品外觀		
已售出數量 2001	已出廠數量 2500	庫存數量 499
女款常規慢跑鞋	581432220	

樣式選擇	女款鞋	已售數量	
		501	
地點選擇	上海市	出廠數量	
		1000	
分售店	到貨數量	已售數量	庫存數量
上海市浦東新區順通路	200	99	101
上海市松江步行街店	121	66	55
上海市浦東區順通路店	155	65	90
上海市浦東區張江店	150	70	80
上海市浦東區張江2店	125	101	24
上海市洋浦區中原路店	121	40	81
上海市閔行區端橋店	68	20	48
上海市樂購商場	60	40	20

第十二圖