I829406

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I829406 B**

(45)公告日： 中華民國 113 (2024) 年 01 月 11 日

(21)申請案號：111141349 (22)申請日： 中華民國 111 (2022) 年 10 月 31 日

(51)Int. Cl.： ***H04L9/06 (2006.01)*** ***H04L9/08 (2006.01)***

(30)優先權：2022/10/04 美國 17/959,322

(71)申請人：麟數據科技股份有限公司 (中華民國) LNDATA, INC. (TW)
臺北市大安區和平東路 1 段 75 巷 3 號 2 樓

(72)發明人：鄭名傑 CHENG, MING-CHIEH (TW)

(74)代理人：王立成；余宗學

(56)參考文獻：

TW 202215251A CN 103987035A

US 7246097B2

審查人員：黎芷婷

申請專利範圍項數：20 項 圖式數：9 共 36 頁

(54)名稱

資料交換方法、電腦可讀取媒體、電腦程式產品及資料交換系統

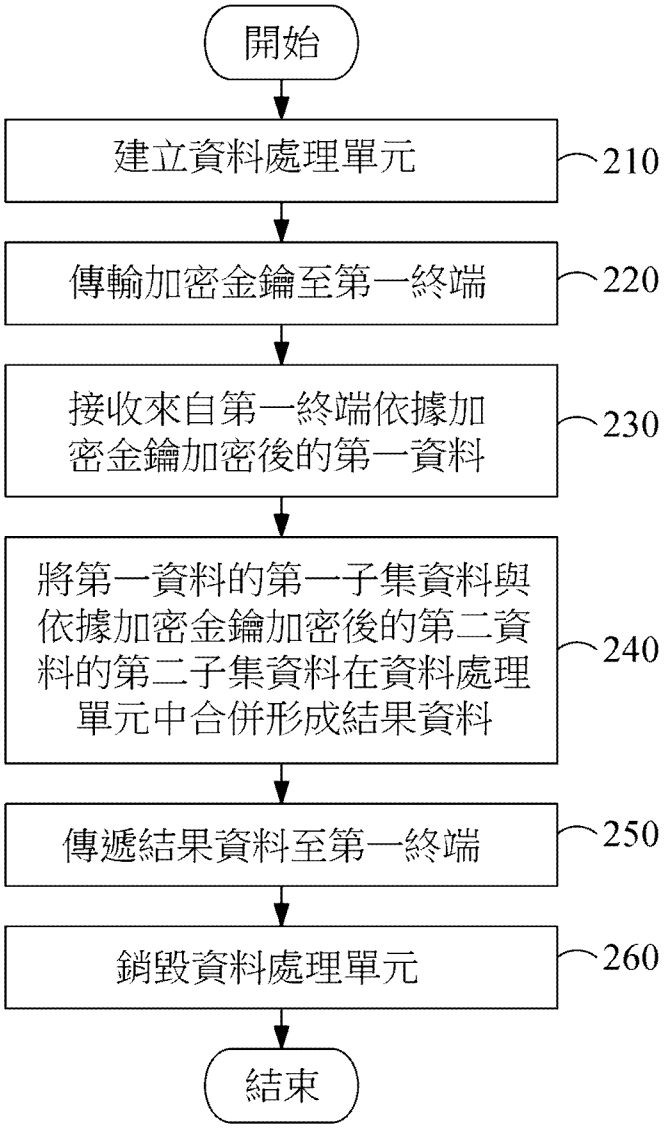
(57)摘要

本發明提供一種資料交換方法，用於執行一資料交換流程且包括以下步驟：建立一資料處理單元；傳輸一加密金鑰至一第一終端；接收來自第一終端依據加密金鑰加密後的一第一資料；將第一資料的一第一子集資料與依據加密金鑰加密後的一第二資料的一第二子集資料在資料處理單元中合併形成一結果資料，其中第一子集資料與第二子集資料分別具有一共同識別符；傳遞結果資料至第一終端；以及銷毀資料處理單元。此外，本發明還提供一種可執行上述資料交換方法的電腦可讀取媒體、電腦程式產品以及資料交換系統。

指定代表圖：

符號簡單說明：

210~260:步驟



【圖2】

公告本

I829406

【發明摘要】

【中文發明名稱】資料交換方法、電腦可讀取媒體、電腦程式產品及資料交換系統

【中文】

本發明提供一種資料交換方法，用於執行一資料交換流程且包括以下步驟：建立一資料處理單元；傳輸一加密金鑰至一第一終端；接收來自第一終端依據加密金鑰加密後的一第一資料；將第一資料的一第一子集資料與依據加密金鑰加密後的一第二資料的一第二子集資料在資料處理單元中合併形成一結果資料，其中第一子集資料與第二子集資料分別具有一共同識別符；傳遞結果資料至第一終端；以及銷毀資料處理單元。此外，本發明還提供一種可執行上述資料交換方法的電腦可讀取媒體、電腦程式產品以及資料交換系統。

【指定代表圖】　　圖2

【代表圖之符號簡單說明】

210~260　　步驟

【發明說明書】

【中文發明名稱】資料交換方法、電腦可讀取媒體、電腦程式產品及資料交換系統

【技術領域】

【0001】　本發明提供一種資料交換方法、電腦可讀取媒體、電腦程式產品及資料交換系統，且特別是關於一種可提供不同使用者間交換敏感性資料並提高資料防護的資料交換方法，以及實現上述資料交換方法的電腦可讀取媒體、電腦程式產品及資料交換系統。

【先前技術】

【0002】　廣告是一種日常生活中廣泛可見的商業行銷工具。一般而言，商家在向廣告經銷商購買廣告投放前，會先調查販賣商品的受眾資訊，例如年齡層、性別、居住地區以及興趣等等。透過這些資訊能夠較為精確地鎖定有意願且有對應消費能力的顧客，從而得到較大的廣告收益。因此，消費者的各種資訊對於不同的商家而言具有龐大的潛在商業價值。

【0003】　以網路廣告為例，商家可預先向擁有固定使用者的社群平台、影音平台、搜尋引擎或新聞網站等網路服務提供方購買廣告，並在購買時註明欲販賣商品預定投放的消費者的對應特徵。網路服務提供方在收到廣告委託後，會依據使用者同意網路服務提供方利用的個人資料，以及使用者在網路服務上的瀏覽資料歸納出使用者的特徵，從而將商家購買的廣告在對應特徵的使用者瀏覽時投放，提高使用者購買廣告商品的意願。

【發明內容】

【0004】 然而，使用者的瀏覽資料時常與敏感性個資有著難以區分的關係。目前市面上大部份的網路服務提供方在蒐集瀏覽資料時，均利用儲存於使用者客戶端的小型文字檔案(cookie)作為到訪網站的依據，但在歐盟訂定的《一般資料保護規則》(general data protection regulation, GDPR)中已將瀏覽器cookie、IP位置、行動裝置編號以及社群網站活動紀錄列為個人資料且需以假名化或匿名化等措施加以保護，因為這些資料一旦遭到惡意人士駭入或竊取時，對使用者的隱私將造成極大的危害。為此，部份網路服務提供方宣稱將於不久的未來停止使用cookie，改為依據使用者的長期使用習慣建立客製化的模型，進而定義使用者的各項特徵。這種作法有著以下缺點：(1)未來一般商家在購買廣告時僅能向特定的網路服務提供方購買，而無法驗證提供方建立的模型的準確度；(2)各個網路服務提供方的使用客群重疊性不高，若將網站A得到的消費者資訊套用於網站B時，提昇的收益效果有限；(3)由於模型是依據使用者的長期使用習慣建立，當使用者近期內改變消費習慣或有著與過去消費類型不同的需求時，模型無法準確捕捉到這種動態變化或隱性特徵，容易造成投放廣告的效益下降。

【0005】 發明人遂竭其心智悉心研究，進而研發出一種可提供不同使用者間交換敏感性資料並提高資料防護的資料交換方法，以期達到避免敏感性資料外洩以及提高使用者資料利用效益的效果。

【0006】 本發明提供一種資料交換方法，用於執行一資料交換流程且包括以下步驟：建立一資料處理單元；傳輸一加密金鑰至一第一終端；接收來自第一終端依據加密金鑰加密後的一第一資料；將第一資料的一第一子集資料與依據加密金鑰加密後的一第二資料的一第二子集資料在資料處理單元中合併形成一

結果資料，其中第一子集資料與第二子集資料分別具有一共同識別符；傳遞結果資料至第一終端；以及銷毀資料處理單元。

【0007】　此外，本發明還提供一種儲存電腦程式的電腦可讀取媒體，在一電腦執行此電腦程式時，可執行上述的資料交換方法。

【0008】　此外，本發明還提供一種電腦程式產品，經由一電腦載入此電腦程式並執行時，可執行上述的資料交換方法。

【0009】　此外，本發明還提供一種資料交換系統，包括一處理器以及一記憶體。記憶體耦接於處理器且用於儲存複數個指令，這些指令可透過處理器執行，使處理器執行複數個運作，包括：建立一資料處理單元；傳輸一加密金鑰至一第一終端；接收來自第一終端依據加密金鑰加密後的一第一資料；將第一資料的一第一子集資料與依據加密金鑰加密後的一第二資料的一第二子集資料在資料處理單元中合併形成一結果資料，其中第一子集資料與第二子集資料分別具有一共同識別符；傳遞結果資料至第一終端；以及銷毀資料處理單元。

【0010】　藉此，本發明提供的資料交換方法可將加密後的第一資料以及第二資料在資料處理單元中合併形成結果資料，即使惡意人士駭入資料處理單元也無法獲得具有敏感性資訊的內容，且當資料交換完畢後資料處理單元會立即銷毀，因此亦不會有敏感性資料留存或外洩的風險。此外，本發明提供的電腦可讀取媒體、電腦程式產品以及資料交換系統可透過電腦或處理器自動執行上述的資料交換方法，因此可大幅提高資料交換方法的效率及便利性。

【0011】　為讓本發明的上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【圖式簡單說明】

【0012】

圖1為本發明的資料交換系統的一實施例的示意圖。

圖2為本發明的資料交換方法的一實施例的方塊流程示意圖。

圖3為圖1中的雲端服務、第一終端以及第二終端的方塊示意圖。

圖4為本發明的資料交換方法中的原始資料的一實施例的示意圖。

圖5為圖4中的原始資料加密後的加密資料的示意圖。

圖6為圖5中的第一子集資料以及第二子集資料合併後的結果資料的示意圖。

圖7為本發明的資料交換方法的另一實施例的流程示意圖。

圖8為圖7的資料交換方法中關於解密金鑰與智慧型合約的部份流程示意圖。

圖9為本發明的另一資料交換方法的一實施例的方塊流程示意圖。

【實施方式】

【0013】 有關本發明之前述及其它技術內容、特點與功效，在以下配合參考圖式之較佳實施例的詳細說明中，將可清楚地呈現。值得一提的是，以下實施例所提到的方向用語，例如：上、下、左、右、前或後等，僅是參考附加圖式的方向。因此，使用的方向用語是用以說明，而非對本發明加以限制，且在下列各個實施例中，相同或相似的元件將採用相同或相似的標號。

【0014】 另外，以下實施例所揭露的方法、流程及步驟，除非在技術上明顯需協同進行或是變更後將產生時序或技術上的矛盾，否則本發明所屬技術領域中具有通常知識者可在不脫離本發明精神的範疇的情況下適當地增加、省略、

修改或單獨執行各方法、流程或步驟，且各方法、流程或步驟彼此間的次序亦可自由調整或變換。

【0015】 請參考圖1及圖2，其中圖1為本發明的資料交換系統的一實施例的示意圖，而圖2為本發明的資料交換方法的一實施例的方塊流程示意圖。如圖1所示，資料交換系統100示例性地可包括一雲端110以及複數個終端，其中雲端110例如包括一雲端服務112、一第一運算服務114以及一第二運算服務116，而終端例如包括一第一終端120、一第二終端130、一第三終端140以及一第四終端150且耦接於雲端110。藉此，各個終端可與雲端110進行資料交換及互動，且可進一步地透過雲端服務112與其它終端進行資料交換及互動，其中第一終端120、第二終端130、第三終端140以及第四終端150例如但不限於是不同使用者的平板電腦、個人電腦、商用電腦、伺服器或可攜式電子裝置，且各個終端可位於相同或不相同的位置，本發明對此不加以限制。

【0016】 在一實施例中，雲端服務112可選擇與一或多個終端互動以執行一資料交換流程。舉例而言，雲端服務112可包括一處理器以及一記憶體，其中記憶體耦接於處理器且用於儲存複數個指令，這些指令可透過處理器執行及/或借助第一運算服務114以及第二運算服務116協同運算，使處理器執行後進而執行如圖2所示的資料交換方法的複數個步驟或運作，包括：建立一資料處理單元(步驟210)；傳輸一加密金鑰至一第一終端(步驟220)；接收來自第一終端依據加密金鑰加密後的一第一資料(步驟230)；將第一資料的一第一子集資料與依據加密金鑰加密後的一第二資料的一第二子集資料在資料處理單元中合併形成一結果資料(步驟240)，其中第一子集資料與第二子集資料分別具有一共同識別符；傳遞結果資料至第一終端(步驟250)；以及銷毀資料處理單元(步驟260)。

【0017】 請參考圖3，圖3為圖1中的雲端服務、第一終端以及第二終端的方塊示意圖。如圖3所示，資料交換系統300的雲端服務310可視為提供資料交換服務的一平台，使第一終端320得以與第二終端330進行資料交換。詳細而言，雲端服務310包括一中央管理單元311、一連線管理單元312以及一認證單元313，其中中央管理單元311用以建立一資料處理單元314，從而進行下文中的資料交換流程。較佳地，雲端服務310還包括通訊連接於中央管理單元311的一元資料庫315以及一狀態資料庫316，其中元資料庫315例如是一關聯式資料庫(relational database)，用以儲存對應於交換中或交換完畢資料的元資料(metadata)；而狀態資料庫316例如是一記憶體資料庫(in-memory database)，用以紀錄資料交換流程中的每一筆運作的狀態。連線管理單元312通訊連接於中央管理單元311，用以作為各終端與雲端服務310之間的連線橋樑。認證單元313通訊連接於連線管理單元312，用以判斷通訊連接於雲端服務310的各個終端是否為雲端服務310認可的使用者，進而產生及分配各種連線所需的憑證。較佳地，雲端服務310還包括通訊連接於認證單元313的一終端資料庫317，其中終端資料庫317例如是一關聯式資料庫，用以儲存各個終端在雲端服務310中的使用者帳號、雜湊處理後(hashed)的密碼以及所屬的組織或身份等資訊。

【0018】 另一方面，資料交換系統300在第一終端320以及第二終端330內可分別包括一終端介面322,332、一資料傳輸介面324,334以及一資料儲存單元326,336，其中終端介面322,332可為用以互動的一視覺化介面，其功能包括但不限於資料上傳、資料販售、資料購買、瀏覽交易紀錄以及透過視覺化方式呈現正在進行交換的資料；資料傳輸介面324,334通訊連接於終端介面322,332以及資料儲存單元326,336之間，且可選擇性地建立與資料處理單元314之間的連線；而資

料儲存單元326,336例如是一普通檔案系統或一資料庫，用以儲存使用者欲上傳、販賣或購買的原始資料以及即將執行資料交換流程的加密後資料。

【0019】 當雲端服務310確立欲進行資料交換流程的第一終端320以及第二終端330後，中央管理單元311會隨即建立資料處理單元314，這個資料處理單元314為一次性及暫時性的，亦即其對應本次的資料交換流程而產生，且在資料交換流程結束後銷毀，從而確保進行交換的資料的安全性及隱密性。接著，資料處理單元314會產生一個隨機的加密金鑰，且中央管理單元311會透過連線管理單元312將加密金鑰分別傳輸至第一終端320以及第二終端330。當第一終端320接收來自雲端服務310的加密金鑰後，可透過終端介面322將儲存於資料儲存單元326中欲進行交換的第一原始資料依據加密金鑰加密形成第一資料；同理，第二終端330接收來自雲端服務310的加密金鑰後，可透過終端介面332將儲存於資料儲存單元336中欲進行交換的第二原始資料依據加密金鑰加密形成第二資料。

【0020】 之後，第一終端320以及第二終端330分別將加密後的第一資料以及第二資料傳輸至雲端服務310。當雲端服務310接收第一資料以及第二資料後，可將這些資料移動至資料處理單元314內進行運算處理，且資料處理單元314可將第一資料以及第二資料中的共同識別符對應的子集資料分別定義為第一子集資料以及第二子集資料，並將第一子集資料以及第二子集資料合併形成結果資料。此時，中央管理單元311可透過連線管理單元312將合併完成的結果資料傳遞至購買或要求結果資料的終端，在本實施例中例如是第一終端320。當結果資料順利傳遞至第一終端320後，雲端服務310會立即銷毀資料處理單元314，因此無論是第一終端320、第二終端330甚至是雲端服務310本身，或是未參與此次資料交換流程的外部終端或人員，均無法再對資料處理單元314進行存取或透過資料

處理單元314獲得任何與結果資料有關的資料。此外，由於第一資料以及第二資料傳輸至雲端服務310時已經是加密後的狀態，即使在資料處理單元314尚未銷毀前遭任何外部終端或人員駭入，亦不會有敏感性資料外洩的風險，從而提高資料交換流程的安全性及隱密性。

【0021】 以下將針對本實施例的系統架構做更為詳細的說明。首先，雲端服務310的提供方可建立屬於各個使用者的帳號及密碼，將這些帳號及密碼分配至各個使用者所屬的終端，並同時儲存於終端資料庫317中。當這些終端當中的其中一個終端，例如是第一終端320登入雲端服務310時，認證單元313會對第一終端320提供一個登入用憑證(token)，這個登入用憑證當終端登出或閒置時間超過設定時間後就會被清除，且每當第一終端320對雲端服務310送出任何指令或請求時，認證單元313皆會驗證登入用憑證的正確性及有效性，使得連線管理單元312僅允許伴隨有效憑證的指令或請求，從而確保連線及資料交換的安全性。

【0022】 對於中央管理單元311而言，由於雲端服務310處理的資料交換流程涉及諸多終端的連線以及運算，因此也容易產生錯誤。為此，狀態資料庫316會紀錄每一個步驟或運作的初始化狀態及完成狀態，當特定步驟的完成狀態被紀錄時，對應的初始化狀態會即時從狀態資料庫316中移除，因此服務提供者可迅速且準確地得知目前正在進行的資料交換流程的概況，這樣的作法具有以下兩個優點：(1)當特定終端所執行的運作對其它終端(例如是正在與其進行資料交換的另一終端)產生影響時，中央管理單元311可透過連線管理單元312傳送警示訊息至關聯的終端，使得這些終端在登入服務或執行下一個操作時可透過終端介面收到警示訊息，從而避免錯誤持續擴大；(2)當任一流程中產生系統錯誤時，

這個系統錯誤會被即時寫入狀態資料庫316中，而中央管理單元311會根據錯誤的類型判定需再次重啟指令或通知使用者需手動處理，因此可迅速排除錯誤。

【0023】 對於連線管理單元312而言，可採用Google遠端程序呼叫(google remote procedure call, gRPC)架構，從而能有效地在資料處理單元314內或跨越資料處理單元314建立連線，並同時兼具負載平衡、追蹤、系統狀態檢查以及認證的功能，且不受限於各終端不同的作業系統環境，因此有利於各種運算服務、終端以及系統後端的運算。此外，在連線認證部份採用雙向傳輸層安全性(transport layer security, TLS)協定，亦即每一筆操作的認證除了系統端的憑證外還需要使用者終端的憑證才能通過認證，對於敏感性資料的安全層面有著顯著的助益。

【0024】 對於資料處理單元314而言，最重要的原則是敏感性資料絕對不能以未加密的型式離開或留在資料處理單元314內。為此，由第一終端320以及第二終端330分別傳輸至資料處理單元314的第一資料以及第二資料，已經是透過加密金鑰將敏感性資料加密後的資料，且資料處理單元314傳遞至第一終端320及/或元資料庫315的結果資料亦以加密後的型式儲存，需要透過具有對應加密金鑰的解密金鑰的終端才能將結果資料解密還原為原始的資料。較佳地，本實施例的資料交換方法還包括：執行一資料保護配置，使資料處理單元314拒絕元資料庫315、第一終端320以及第二終端330以外的存取要求，即便是來自於中央管理單元311的指令操作，也需要在系統端以及使用者終端的憑證皆有效的情況下才能通過認證並執行，藉此可防止外部的惡意入侵或雲端服務310的控制權限遭駭導致敏感性資料外洩。

【0025】 請參考圖4至圖6，其中圖4為本發明的資料交換方法中的原始資料的一實施例的示意圖，圖5為圖4中的原始資料加密後的加密資料的示意圖，而

圖6為圖5中的第一子集資料以及第二子集資料合併後的結果資料的示意圖。在本實施例中，原始資料400包括位於第一終端320的第一原始資料410(包括在第一終端320的資料儲存單元326中的資料編號、電子郵件以及電子郵件持有者居住的城市)以及位於第二終端330的第二原始資料420(包括在第二終端330的資料儲存單元336中的資料編號、電子郵件以及各電子郵件持有者的興趣)，其中電子郵件為可直接或間接辨識出特定使用者的敏感性資料。當雲端服務310將加密金鑰分別傳輸至第一終端320以及第二終端330後，第一終端320以及第二終端330會依據加密金鑰將原始資料400加密為加密資料500，即圖5中電子郵件欄內容加密後的第一資料510以及第二資料520。

【0026】 由於第一終端320以及第二終端330均使用相同的加密金鑰進行加密，因此在第一原始資料410以及第二原始資料420中相同的電子郵件資料值加密後的內容依然相同。之後，第一終端320以及第二終端330可分別將第一資料510以及第二資料520傳輸至雲端服務310，此時資料處理單元314會依據第一資料510以及第二資料520建立一資料處理規則，並依據資料處理規則將第一資料510以及第二資料520的加密內容定義為一識別符，在本實施例中為電子郵件欄加密後的資料值。具體而言，由於第一原始資料410與第二原始資料420個別的電子郵件欄內容未必完全相同，有可能第一原始資料410的欄位相較於第二原始資料420的欄位較多或較少，或者是兩者的電子郵件資料值不盡相同。因此，當資料處理單元314分別將第一資料510中加密後的電子郵件資料值以及第二資料520中加密後的電子郵件資料值定義為識別符後，僅有相同的識別符(加密後資料值)會被定義為共同識別符，在圖5中共有三列。在本實施例中，這三列共同識別符在第一資料510中對應的一子集資料為共同識別符本身以及居住城市，而這三

列共同識別符在第二資料520中對應的一子集資料為共同識別符以及興趣。此時，資料處理單元314會分別將上述兩個子集資料定義為第一子集資料以及第二子集資料，從而進行後續的步驟。

【0027】 之後，資料處理單元314會將第一子集資料以及第二子集資料兩者合併，並對共同識別符賦予一去識別化標籤以形成結果資料600。在本實施例中資料合併的具體實現方式例如是內部連接(inner join)，而去識別化標籤的名稱例如是「代表符(token)」，但本發明並不限定於此。藉此，如圖6所示，形成的結果資料600包括代表符欄位的一系列加密資料，以及這些加密資料對應的使用者的居住城市以及興趣。此時，中央管理單元311會透過連線管理單元312將結果資料600傳遞至第一終端320，並在成功傳遞結果資料600後，銷毀資料處理單元314以及儲存於其中的全部資料，完成整個資料交換流程。

【0028】 具體而言，各終端的資料傳輸介面能讓使用者上傳的資料種類包括但不限於由分隔符(delimiter)進行分隔的純文字檔案，例如是CSV檔。此外，第一終端320以及第二終端330在將第一資料510以及第二資料520分別傳輸至雲端服務310時，可自行決定需進行加密的識別符欄位，以及是否定義此識別符欄位的屬性，這樣的作法可適用於以下兩種情況：(1)使用者怠於整理自身擁有的資料；(2)使用者不知道該如何利用自身擁有的資料，而僅是單純將其儲存下來。

【0029】 較佳地，各終端的終端介面的功能還包括對資料正規化處理。具體而言，使用者在將資料儲存至資料儲存單元前或儲存的當下，終端介面可對資料進行正規化處理，其中正規化處理包括但不限於將所有字元轉換為半形小寫、將通用字調整為共同拼寫方式(例如將E-Mail調整為email)以及透過自然語言處理(natural language processing, NLP)校正拼字錯誤或執行詞幹提取。

【0030】 在一較佳的實施例中，資料交換方法還可包括：依據第一終端提供的一樣本資料建立資料處理規則。詳細而言，為了減少資料處理時所產生的誤差，且使獲得的結果資料600更接近第一終端320可直接利用的型態，在資料交換流程開始前或過程當中，第一終端320可以先提供一樣本資料至雲端服務310，其中樣本資料包括但不限於最終所需資料的種類以及編排格式，也可以是結果資料600的一縮影。當雲端服務310接收樣本資料後，資料處理單元314將自動依據樣本資料的內部規則建立資料處理規則，藉此提高第一終端320對於結果資料600使用上的便利性。

【0031】 值得一提的是，即使第一終端320沒有提供樣本資料，資料處理單元314也可以依據第一終端320送出的要求對結果資料600執行一些簡單運算，例如統計結果資料600中共同識別符資料的數量，或是地區、興趣的種類等等。

【0032】 請參考圖7及圖8，其中圖7為本發明的資料交換方法的另一實施例的流程示意圖，而圖8為圖7的資料交換方法中關於解密金鑰與智慧型合約的部份流程示意圖。如圖7所示，資料交換方法可與商業方式結合執行，且由雲端服務710(負責媒合交易以及提供資料交換的平台)、第一終端720(擔任資料買方以及提供合併用的部份資料)以及第二終端730(擔任資料賣方以及提供買方所需的資料)共同參與。

【0033】 首先，第二終端730可透過終端介面332的販售資料功能，或藉由瀏覽第一終端720貼出的資料懸賞而提供一資料交換交易至雲端服務710(步驟732)，雲端服務710在接收第二終端730提供的資料交換交易後，會將資料交換交易提供至第一終端720(步驟734)。第一終端720接收上述的資料交換交易後，可透過終端介面322的購買資料功能，傳輸一資料交換交易要求至雲端服務710(步

驟736)，而當雲端服務710接收上述的資料交換交易要求後，會將此資料交換交易要求傳輸至第二終端730(步驟738)，從而確認買賣雙方的資料交換交易成立。

【0034】 在一較佳的實施例中，資料交換方法還可包括：傳輸一單一次性憑證至參與資料交換交易的一第一交易終端；接收來自第一待定終端的單一次性憑證；以及將第一待定終端認證為第一終端。詳細而言，本實施例的資料交換方法允許發出/接受資料交換交易要求的終端與提供交換用資料的終端為相異的終端。舉例而言，當第一終端720傳輸資料交換交易要求至雲端服務710後，雲端服務710可將參與本次資料交換交易的終端，即第一終端720定義為第一交易終端，透過認證單元313產生一單一次性憑證，並將憑證傳輸至第一交易終端。此時，第一終端720可以選擇將此單一次性憑證傳輸至其它的終端或是自行使用。當第一終端720或是其它的終端準備進行資料交換，並將此單一次性憑證傳輸至雲端服務710時，雲端服務710會將送出單一次性憑證的第一待定終端認證為參與資料交換流程的第一終端720，由其負責將第一資料510傳輸至雲端服務710，並賦予其接收或讀取結果資料600的權限。同理，第二終端730也可以將收到的單一次性憑證傳輸至其他的終端，並透過雲端服務710將送出此單一次性憑證的第二待定終端認證為第二終端730，由其負責將第二資料520傳輸至雲端服務710。

【0035】 值得一提的是，上述的資料處理規則除了可由資料處理單元314依據第一資料510自行建立，或是由第一終端720提供一樣本資料建立之外，亦可依據第一交易終端在本次資料交換交易中所選擇的資料建立，其中建立的規則包括資料的類型、大小以及儲存型式，但本發明並不以此為限。

【0036】 雲端服務710確認進行資料交換的兩個終端後，會分別將隨機產生的加密金鑰傳輸至第一終端720以及第二終端730(步驟740)，第一終端720接收

來自雲端服務710的加密金鑰後，可如圖4至圖5所示將第一原始資料410加密形成第一資料510，並傳輸第一資料510至雲端服務710(步驟742)；同理，第二終端730接收來自雲端服務710的加密金鑰後，可將第二原始資料420加密形成第二資料520，並傳輸第二資料520至雲端服務710(步驟744)。

【0037】 在一可能的實施例中，資料交換方法還包括：建立一雜湊規則，並將雜湊規則傳輸至第一終端；接收第一終端依據雜湊規則雜湊後的第一雜湊資料；將第一雜湊資料與依據雜湊規則雜湊後的一第二雜湊資料合併，並計算第一雜湊資料以及第二雜湊資料的一交集大小；以及將交集大小傳輸至第一終端。詳細而言，資料買方(第一終端720)可能在進行實際的資料交換流程前，就想要得知這次的資料交換流程可以獲得多少筆可利用的資料。因此，雲端服務710可將建立的雜湊規則傳輸至第一終端720以及第二終端730，在接收第一終端720以及第二終端730依據雜湊規則雜湊後的第一雜湊資料以及第二雜湊資料後，計算兩者的交集大小並傳輸至第一終端720。與真正資料交換流程中的加密處理不同，由於雜湊處理僅單純地將所有的資料值匿名化且不可還原，因此運算得到的交集大小不必然等同於第一終端720最終可獲得的結果資料600的大小，但依然可作為第一終端720在資料交換交易前的參考。

【0038】 在一較佳的實施例中，資料交換方法還包括：計算第一資料的資料大小；以及依據資料大小傳輸一付款要求至第一終端。詳細而言，在過往的資料交換流程中，部份不肖業者可能會將惡意cookie或由機器人生成的無效流量(invalid traffic, IVT)所產出的資料與買家進行交換，使得買家得到的結果充斥眾多無效的資料。此外，資料處理單元314銷毀所需的時間及運算成本，與存放於其中的資料大小彼此正相關，因此雲端服務710可合理地依據第一資料510以及

第二資料520的資料大小，分別傳輸不同的資料清洗費用要求至第一終端720以及第二終端730。由於每一筆的資料清洗均需要付出費用，這樣的設計可以有效防止買方或賣方使用無效資料與他人進行交易或交換，從而提高資料交換流程的效率以及結果資料600的品質。

【0039】 在一較佳的實施例中，資料交換方法還包括：傳輸一永久憑證至第一終端；將結果資料儲存至一元資料庫；接收第一終端具備永久憑證的一讀取要求；以及建立第一終端與元資料庫的通訊協定。詳細而言，資料交換方法可採用雙重認證的方式，確保提供資料的終端以及接收結果資料600的終端的正確性。以第一終端720為例，在雲端服務710依據單一次性憑證，將未知的第一待定終端認證為參與資料交換流程的第一終端720後，在傳輸加密金鑰的同時可將隨機產生的一永久憑證傳輸至第一終端720。具體而言，當第一終端720將單一次性憑證傳輸至雲端服務710執行身份認證後，此單一次性憑證會隨即消滅而無法再度使用。因此，在後續的資料交換流程中，無論是將第一資料510傳輸至雲端服務710、自雲端服務710接收結果資料600甚至是在資料交換流程結束後給予雲端服務710的回饋，都需要伴隨著永久憑證才能被連線管理單元312以及認證單元313核可及執行。

【0040】 此外，雲端服務710還可包括儲存結果資料600並供第一終端720不限次數讀取的功能。具體而言，當第一資料510以及第二資料520在資料處理單元314內合併形成結果資料600後，依據第一終端720的需求，中央管理單元311可選擇單純地將結果資料600直接傳輸至第一終端720；或者是不直接將結果資料600傳輸至第一終端720，而是將結果資料600儲存至元資料庫315，並在資料交換流程結束且資料處理單元314銷毀後，由第一終端720憑藉永久憑證向雲端服務

710送出讀取要求，再透過連線管理單元312建立第一終端720與元資料庫315間的通訊協定，間接地允許第一終端720自元資料庫315下載結果資料600；又或者可選擇既直接將結果資料600傳輸至第一終端720，亦將結果資料600的備份儲存至元資料庫315，以供未來第一終端720在有讀取或下載結果資料600的需求時可隨時讀取或下載。由於儲存於元資料庫315中的結果資料600依然是加密後的資料，因此即使雲端服務710遭到惡意人士入侵，亦可防止敏感性資料遭到竊取。

【0041】 在一可能的實施例中，資料交換方法還包括：在合併形成結果資料時同步將結果資料傳輸至第一終端；以及將一銷毀進度資訊傳輸至第一終端。詳細而言，當第一資料510或第二資料520相當龐大時，第一終端720的使用者可能想要快速得到結果資料600。為此，雲端服務710可允許第一終端720及/或第二終端730的資料傳輸介面324,334直接與資料處理單元314建立連線(如圖3中所示彼此間的虛線)，並在結果資料600生成的當下即時傳輸至第一終端720及/或第二終端730，之後雲端服務710再選擇性地將結果資料600儲存至元資料庫315，並銷毀資料處理單元314。這個作法的優點在於，當消費者瀏覽網站時，廣告購買方可即時投放具有時效性的廣告，例如是限時特價或清倉拍賣，而毋需等待消費者完成瀏覽後才得到廣告訊息，因此有利於商業上俗稱尖峰時刻(rush hour)時的行銷。此外，當資料處理單元314銷毀的當下，第一終端720及/或第二終端730可即時監測資料處理單元314的銷毀進度，確保所提供的資料不會被濫用或竊取。

【0042】 在一較佳的實施例中，資料交換方法還包括：在將第一子集資料與第二子集資料在資料處理單元中合併形成結果資料的過程中，或第一終端的複數次資料交換流程中修正資料處理規則；依據修正後的資料處理規則分別對第一資料以及第二資料的一自定義識別符賦予對應的一自定義標籤；以及將第

一資料以及第二資料中的各自定義識別符以及各自定義標籤整合至結果資料中。

【0043】 承上所述，每一個使用者在使用雲端服務710時都擁有各自的使用者帳號及密碼，因此資料處理單元314無論是依據第一交易終端選擇交易的資料，或是第一終端720提供的樣本資料所建立的資料處理規則，有相當大的程度能夠符合第一終端720交換其它資料的準則而被沿用。因此，即便在當次的資料交換流程結束後，對應於第一終端720的資料處理規則依然可被儲存下來並在下一次資料交換流程中使用。另外，雖然第一資料510以及第二資料520在傳輸至雲端服務710前，可透過終端介面322,332正規化而提高資料處理單元314辨識及利用的可能性，但當中仍然可能存有資料處理單元314無法辨識的資料值而被視為雜訊(noise)。然而，當單次的資料交換流程中交換的資料較為龐大，或者是第一終端720已進行複數次資料交換，使得資料處理單元314能透過例如機器學習等方式修正或改良所建立的資料處理規則。藉此，對於一些一開始無法辨識或利用的雜訊，修正後的資料處理規則可嘗試性地在不改變資料本質的前提下，對這些雜訊進行微調或賦予自定義標籤，從而使這些資料值成為對第一終端720可能具有使用價值的自定義識別符，再將這些自定義識別符以及自定義標籤整合至結果資料600中，而一併提供至第一終端720。舉例而言，在圖5中第一資料510可能還包括「年紀」欄位，而第二資料520可能還包括「歲數」欄位，雖然兩者在字面上無法被直接判定為相同性質的資料，但在資料交換的過程中，資料處理單元314學習到這兩種資料具有相近的處理規則或邏輯，因此會試著賦予此欄位自定義識別符以及自定義標籤，並將有關「年齡」的資料值一併呈現在結果資料600內並傳遞至第一終端720。

【0044】 請再次參考圖7及圖8，在一較佳的實施例中，資料交換方法還包括：建立一解密金鑰以及一智慧型合約；將解密金鑰拆解為一第一子金鑰以及一第二子金鑰；傳輸結果資料以及第一子金鑰至第一終端；以及接收來自第一終端的確認訊息及/或付款通知後，傳輸智慧型合約以及第二子金鑰至第一終端。詳細而言，為了確保每一次的資料交換交易中雲端服務710可作為公正的第三方平台，且資料買方及資料賣方在完成交易後均能得到所需的資料及報酬，本實施例的資料交換方法引入智慧型合約作為交易雙方履約及驗證的工具。詳細而言，當資料交換流程開始時，雲端服務710會初始化交易(步驟832)並建立資料處理單元314(步驟834)，當資料處理單元314產生加密金鑰時，也同時建立對應此加密金鑰的智慧型合約以及解密金鑰(步驟836)。換言之，獲得結果資料600的終端需要透過解密金鑰才能將加密後的結果資料600解密還原成可利用的資料。之後，雲端服務710可將解密金鑰拆解為第一子金鑰以及第二子金鑰(步驟838)，在透過資料處理單元314將第一資料510以及第二資料520合併形成加密的結果資料600(步驟840)後，將第一子金鑰與結果資料600整合封裝(步驟842)，並將第二子金鑰與整份智慧型合約整合封裝(步驟844)。此時，雲端服務710會將封裝完成的第一子金鑰與結果資料600傳輸至資料買方，也就是第一終端720(步驟746、步驟846)。第一終端720雖然得到第一子金鑰以及結果資料600，但由於仍欠缺第二子金鑰，因此這時結果資料600為無法解密亦無法被利用的狀態，然而仍足以使第一終端720確認其收到了處理後的結果資料600。因此，在第一終端720確認並付款至雲端服務710的提供方(步驟748)後，雲端服務710會將剩下的第二子金鑰與智慧型合約傳輸至第一終端720(步驟750、步驟848)，並將第二終端730販賣資料所得到的費用扣除提供資料交換交易所需的服務費用後，支付給第二終端730(步驟

752)。第一終端720收到了第二子金鑰以及智慧型合約後，可將第一子金鑰以及第二子金鑰結合還原成解密所需的解密金鑰(步驟850)，而智慧型合約則是在解密時作為身份驗證用途，使第一終端720能成功解密結果資料600(步驟852)。之後，第一終端720以及第二終端730可分別選擇性地將本次資料交換交易的回饋意見傳輸至雲端服務710(步驟754)，其中第一終端720(資料買方)的回饋意見可包括對於資料處理規則的修正建議，例如特定識別符的資料筆數需大於一定閾值才需要傳輸，或是自定義標籤的賦予有誤等等，如此一來雲端服務710可依據回饋意見修正資料處理規則，可助於下一次的資料交換流程。

【0045】 請參考圖9，圖9為本發明的另一資料交換方法的一實施例的方塊流程示意圖。如圖所示，本發明還提供一種適於資料交換終端使用的資料交換方法，包括：傳輸一資料交換交易要求至一雲端服務(步驟910)；接收來自雲端服務的一加密金鑰(步驟920)；將一第一原始資料依據加密金鑰加密形成一第一資料(步驟930)；傳輸第一資料至雲端服務(步驟940)；以及接收來自雲端服務的結果資料(步驟950)。透過本實施例的資料交換方法，使用者可將加密後的第一資料510傳輸至雲端服務710，並透過雲端服務710的處理得到結果資料600，由於傳輸至雲端服務710的第一資料510已經過加密處理，因此即使雲端服務710遭到惡意人士入侵，亦不會有敏感性資料外洩的風險，從而提高交換時的資料防護。

【0046】 除此之外，本發明還提供一種儲存電腦程式的電腦可讀取媒體以及電腦程式產品，在一電腦執行此電腦可讀取媒體或此電腦程式產品的電腦程式時，可執行上述的資料交換方法。需注意的是，電腦可讀取媒體可包括但不限於暫存器、處理器快取、隨機存取記憶體、唯讀記憶體、光碟、磁片、USB或隨

身硬碟，且執行的電腦可為平板電腦、個人電腦、工業電腦、商用電腦、工作站、伺服器、電腦叢集或可攜式電子裝置，本發明對此不加以限制。

【0047】 本發明在上文中已以較佳實施例揭露，然熟習本項技術者應理解的是，上述實施例僅用於描繪本發明，而不應解讀為限制本發明之範圍。且應注意的是，舉凡與上述實施例等效之變化與置換，均應視為涵蓋於本發明之範疇內。因此，本發明之保護範圍當以申請專利範圍所界定者為準。

【符號說明】

【0048】

100	資料交換系統
110	雲端
112	雲端服務
114	第一運算服務
116	第二運算服務
120	第一終端
130	第二終端
140	第三終端
150	第四終端
210~260	步驟
300	資料交換系統
310	雲端服務
311	中央管理單元
312	連線管理單元
313	認證單元
314	資料處理單元
315	元資料庫

316	狀態資料庫
317	終端資料庫
320	第一終端
322	終端介面
324	資料傳輸介面
326	資料儲存單元
330	第二終端
332	終端介面
334	資料傳輸介面
336	資料儲存單元
400	原始資料
410	第一原始資料
420	第二原始資料
500	加密資料
510	第一資料
520	第二資料
600	結果資料
710	雲端服務
720	第一終端
730	第二終端
732~754	步驟
832~852	步驟
910~950	步驟

【發明申請專利範圍】

【請求項1】一種用於執行一資料交換流程的資料交換方法，包括以下步驟：

建立一資料處理單元；

傳輸一加密金鑰至一第一終端；

接收來自該第一終端依據該加密金鑰加密後的一第一資料；

將該第一資料的一第一子集資料與依據該加密金鑰加密後的一第二資料的一第二子集資料在該資料處理單元中合併形成一結果資料，其中該第一子集資料與該第二子集資料分別具有一共同識別符；

傳遞該結果資料至該第一終端；以及

銷毀該資料處理單元。

【請求項2】如請求項1所述的資料交換方法，還包括以下步驟：

提供一資料交換交易；

傳輸一單一次性憑證至參與該資料交換交易的一第一交易終端；

接收來自一第一待定終端的該單一次性憑證；以及

將該第一待定終端認證為該第一終端。

【請求項3】如請求項2所述的資料交換方法，還包括以下步驟：

依據該第一交易終端在該資料交換交易中選擇交易的資料或該第一終端提供的一樣本資料建立一資料處理規則；

其中，該將該第一子集資料與該第二子集資料在該資料處理單元中合併形成該結果資料的步驟包括：

依據該資料處理規則分別將該第一資料以及該第二資料的一加密內容定義為一識別符；

將該第一資料與該第二資料中相同的各該識別符定義為該共同識別符，並將各該共同識別符在該第一資料以及該第二資料中對應的一子集資料分別定義為該第一子集資料以及該第二子集資料；以及

合併該第一子集資料以及該第二子集資料，並對該共同識別符賦予一去識別化標籤以形成該結果資料。

【請求項4】如請求項3所述的資料交換方法，還包括以下步驟：

在該將該第一子集資料與該第二子集資料在該資料處理單元中合併形成該結果資料的步驟或該第一終端的複數次資料交換流程中修正該資料處理規則；

依據修正後的該資料處理規則分別對該第一資料以及該第二資料的一自定義識別符賦予對應的一自定義標籤；以及

將該第一資料以及該第二資料中的各該自定義識別符以及各該自定義標籤整合至該結果資料中。

【請求項5】如請求項1所述的資料交換方法，其中該傳輸該加密金鑰至該第一終端的步驟包括：

傳輸一永久憑證至該第一終端；

其中，該傳遞該結果資料至該第一終端的步驟包括：

將該結果資料儲存至一元資料庫；

接收該第一終端具備該永久憑證的一讀取要求；以及

建立該第一終端與該元資料庫的通訊協定。

【請求項6】如請求項5所述的資料交換方法，還包括以下步驟：

執行一資料保護配置，使該資料處理單元拒絕該第一終端、該元資料庫以及提供該第二資料的一第二終端以外的存取要求。

【請求項7】如請求項1所述的資料交換方法，還包括以下步驟：

建立一解密金鑰以及一智慧型合約；以及

將該解密金鑰拆解為一第一子金鑰以及一第二子金鑰；

其中，該傳遞該結果資料至該第一終端的步驟包括：

傳輸該結果資料以及該第一子金鑰至該第一終端；以及

接收來自該第一終端的確認訊息及/或付款通知後，傳輸該智慧型合約以及該第二子金鑰至該第一終端。

【請求項8】如請求項1所述的資料交換方法，其中該將該第一子集資料與該第二子集資料在該資料處理單元中合併形成該結果資料的步驟包括：

在合併形成該結果資料時同步將該結果資料傳輸至該第一終端；

其中，該銷毀該資料處理單元的步驟包括：

將一銷毀進度資訊傳輸至該第一終端。

【請求項9】如請求項1所述的資料交換方法，還包括以下步驟：

建立一雜湊規則，並將該雜湊規則傳輸至該第一終端；

接收該第一終端依據該雜湊規則雜湊後的一第一雜湊資料；

將該第一雜湊資料與依據該雜湊規則雜湊後的一第二雜湊資料合併，並計算該第一雜湊資料以及該第二雜湊資料的一交集大小；以及

將該交集大小傳輸至該第一終端。

【請求項10】一種儲存電腦程式的電腦可讀取媒體，在一電腦執行該電腦程式時執行如請求項1-9中任一項所述的資料交換方法。

【請求項11】一種電腦程式產品，經由一電腦載入該電腦程式並執行時，可執行如請求項1-9中任一項所述的資料交換方法。

【請求項12】一種資料交換系統，包括：

一處理器；以及

一記憶體，耦接於該處理器且用於儲存複數個指令，該複數個指令可透過該處理器執行，使該處理器執行複數個運作，該複數個運作包括：

建立一資料處理單元；

傳輸一加密金鑰至一第一終端；

接收來自該第一終端依據該加密金鑰加密後的一第一資料；

將該第一資料的一第一子集資料與依據該加密金鑰加密後的一第二資料的一第二子集資料在該資料處理單

元中合併形成一結果資料，其中該第一子集資料與該第二子集資料分別具有一共同識別符；

傳遞該結果資料至該第一終端；以及

銷毀該資料處理單元。

【請求項13】如請求項12所述的資料交換系統，其中該複數個運作還包括：

提供一資料交換交易；

傳輸一單一次性憑證至參與該資料交換交易的一第一交易終端；

接收來自一第一待定終端的該單一次性憑證；以及

將該第一待定終端認證為該第一終端。

【請求項14】如請求項13所述的資料交換系統，其中該複數個運作還包括：

依據該第一交易終端在該資料交換交易中選擇交易的資料或該第一終端提供的一樣本資料建立一資料處理規則；

依據該資料處理規則分別將該第一資料以及該第二資料的一加密內容定義為一識別符；

將該第一資料與該第二資料中相同的各該識別符定義為該共同識別符，並將各該共同識別符在該第一資料以及該第二資料中對應的一子集資料分別定義為該第一子集資料以及該第二子集資料；以及

合併該第一子集資料以及該第二子集資料，並對該共同識別符賦予一去識別化標籤以形成該結果資料。

【請求項15】如請求項14所述的資料交換系統，其中該複數個運作還包括：

在該將該第一子集資料與該第二子集資料在該資料處理單元中合併形成該結果資料的運作或該第一終端的複數次資料交換流程中修正該資料處理規則；

依據修正後的該資料處理規則分別對該第一資料以及該第二資料的一自定義識別符賦予對應的一自定義標籤；以及

將該第一資料以及該第二資料中的各該自定義識別符以及各該自定義標籤整合至該結果資料中。

【請求項16】如請求項12所述的資料交換系統，其中該複數個運作還包括：

傳輸一永久憑證至該第一終端；

將該結果資料儲存至一元資料庫；

接收該第一終端具備該永久憑證的一讀取要求；以及

建立該第一終端與該元資料庫的通訊協定。

【請求項17】如請求項16所述的資料交換系統，其中該複數個運作還包括：

執行一資料保護配置，使該資料處理單元拒絕該第一終端、該元資料庫以及提供該第二資料的一第二終端以外的存取要求。

【請求項18】如請求項12所述的資料交換系統，其中該複數個運作還包括：

建立一解密金鑰以及一智慧型合約；

將該解密金鑰拆解為一第一子金鑰以及一第二子金鑰；

傳輸該結果資料以及該第一子金鑰至該第一終端；以及

接收來自該第一終端的確認訊息及/或付款通知後，傳輸該智慧型合約以及該第二子金鑰至該第一終端。

【請求項19】如請求項12所述的資料交換系統，其中該複數個運作還包括：

在合併形成該結果資料時同步將該結果資料傳輸至該第一終端；以及

將一銷毀進度資訊傳輸至該第一終端。

【請求項20】如請求項12所述的資料交換系統，其中該複數個運作還包括：

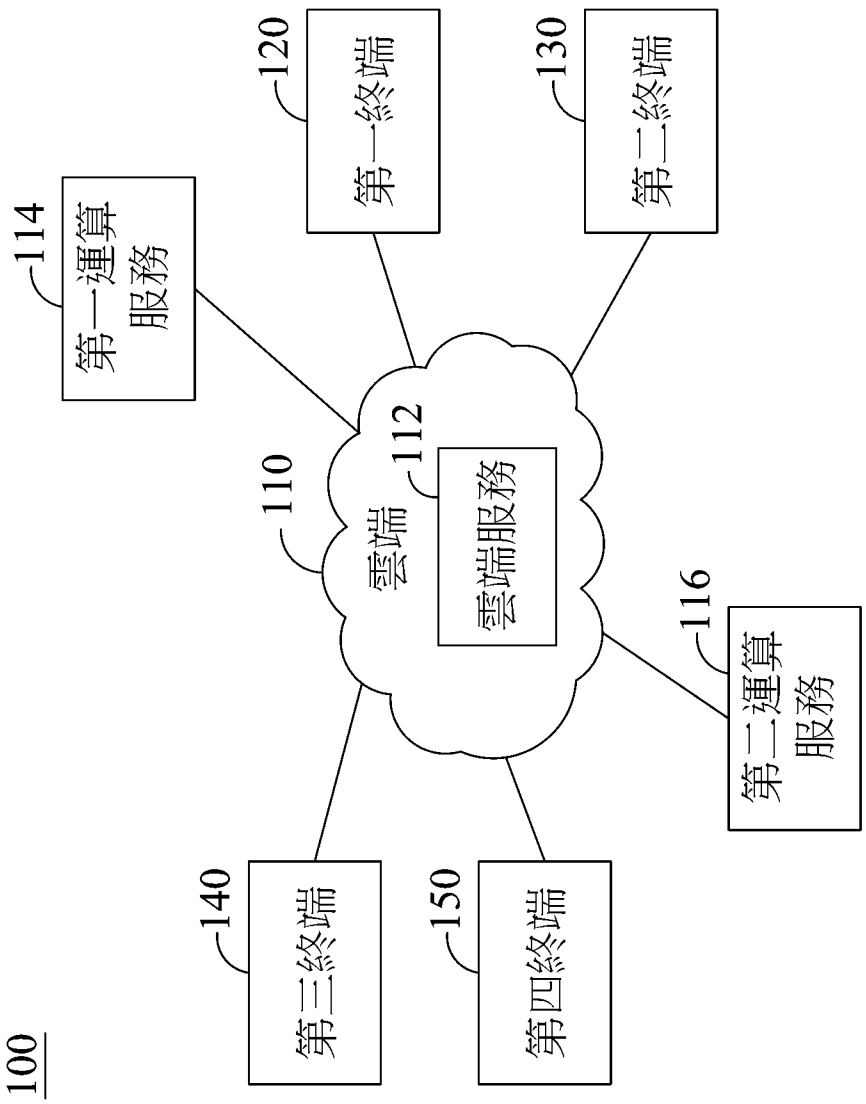
建立一雜湊規則，並將該雜湊規則傳輸至該第一終端；

接收該第一終端依據該雜湊規則雜湊後的一第一雜湊資料；

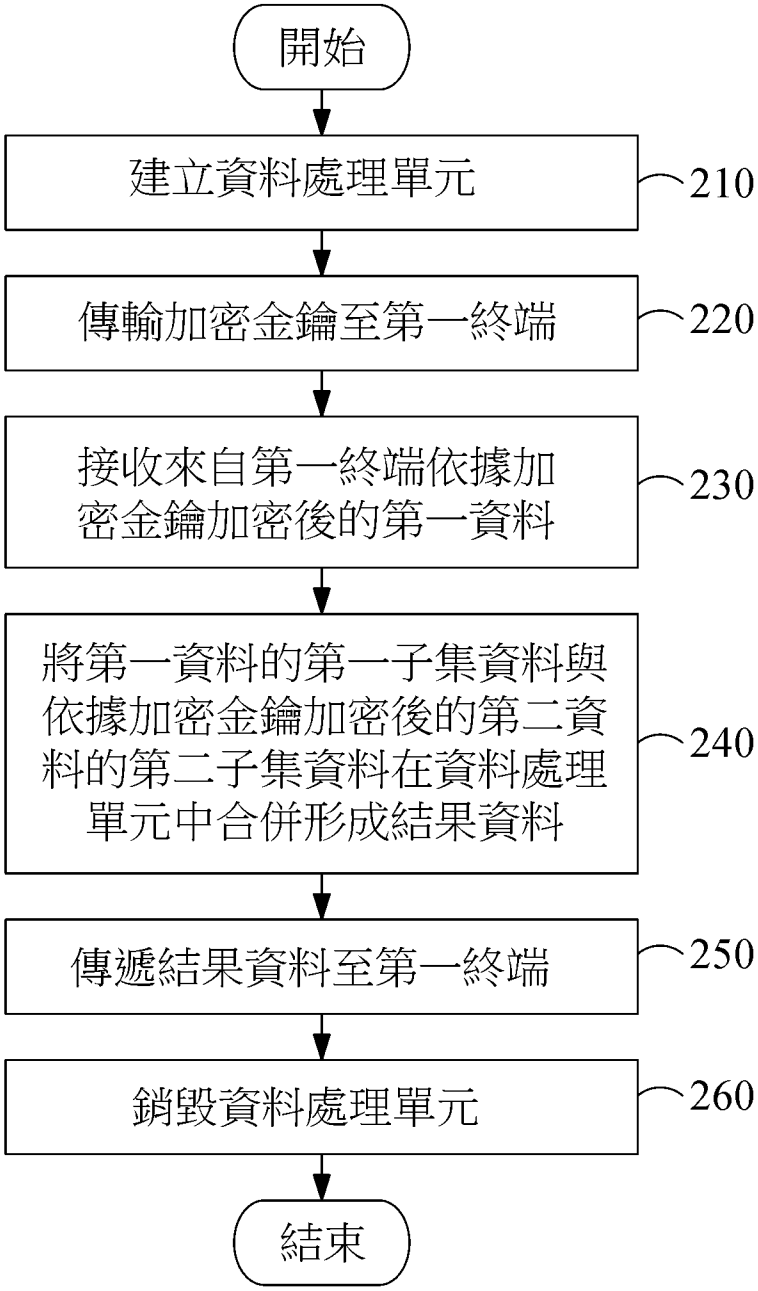
將該第一雜湊資料與依據該雜湊規則雜湊後的一第二雜湊資料合併，並計算該第一雜湊資料以及該第二雜湊資料的一交集大小；以及

將該交集大小傳輸至該第一終端。

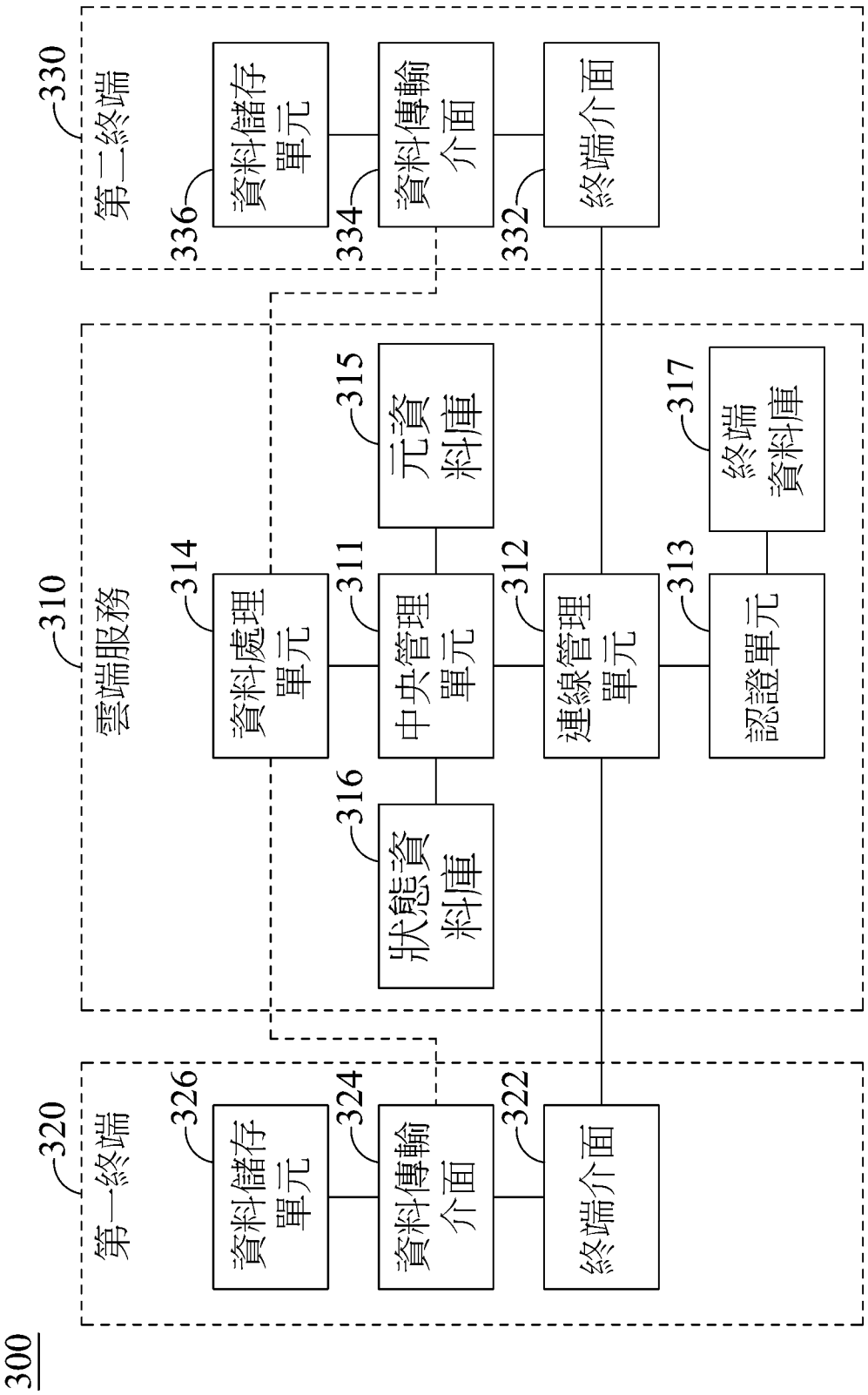
【發明圖式】


100
雲端
110
雲端服務
112
第一運算服務
114
第一終端
120
第二終端
130
第二運算服務
116
第三終端
140
第四終端
150

【圖1】


開始
建立資料處理單元
210
傳輸加密金鑰至第一終端
220
接收來自第一終端依據加密金鑰加密後的第一資料
230
將第一資料的第一子集資料與依據加密金鑰加密後的第二資料的第二子集資料在資料處理單元中合併形成結果資料
240
傳遞結果資料至第一終端
250
銷毀資料處理單元
260
結束

【圖2】


300
第一終端
320
資料儲存單元
326
資料傳輸介面
324
終端介面
322
雲端服務
310
資料處理單元
314
中央管理單元
311
連線管理單元
312
認證單元
313
元資料庫
315
狀態資料庫
316
終端資料庫
317
第二終端
330
資料儲存單元
336
資料傳輸介面
334
終端介面
332

【圖3】

400

410

第一終端		
編號	電子郵件	城市
A1	u1@email.com	台北
A2	u2@email.com	台南
A3	u3@email.com	高雄

420

第二終端		
編號	電子郵件	興趣
B1	u1@email.com	足球
B2	u2@email.com	漫畫
B3	u3@email.com	棒球

【圖4】

500

510

第一終端		
編號	電子郵件	城市
A1	13f1UY$T8a	台北
A2	1k2m$#8ads	台南
A3	p.09&12a*x	高雄

520

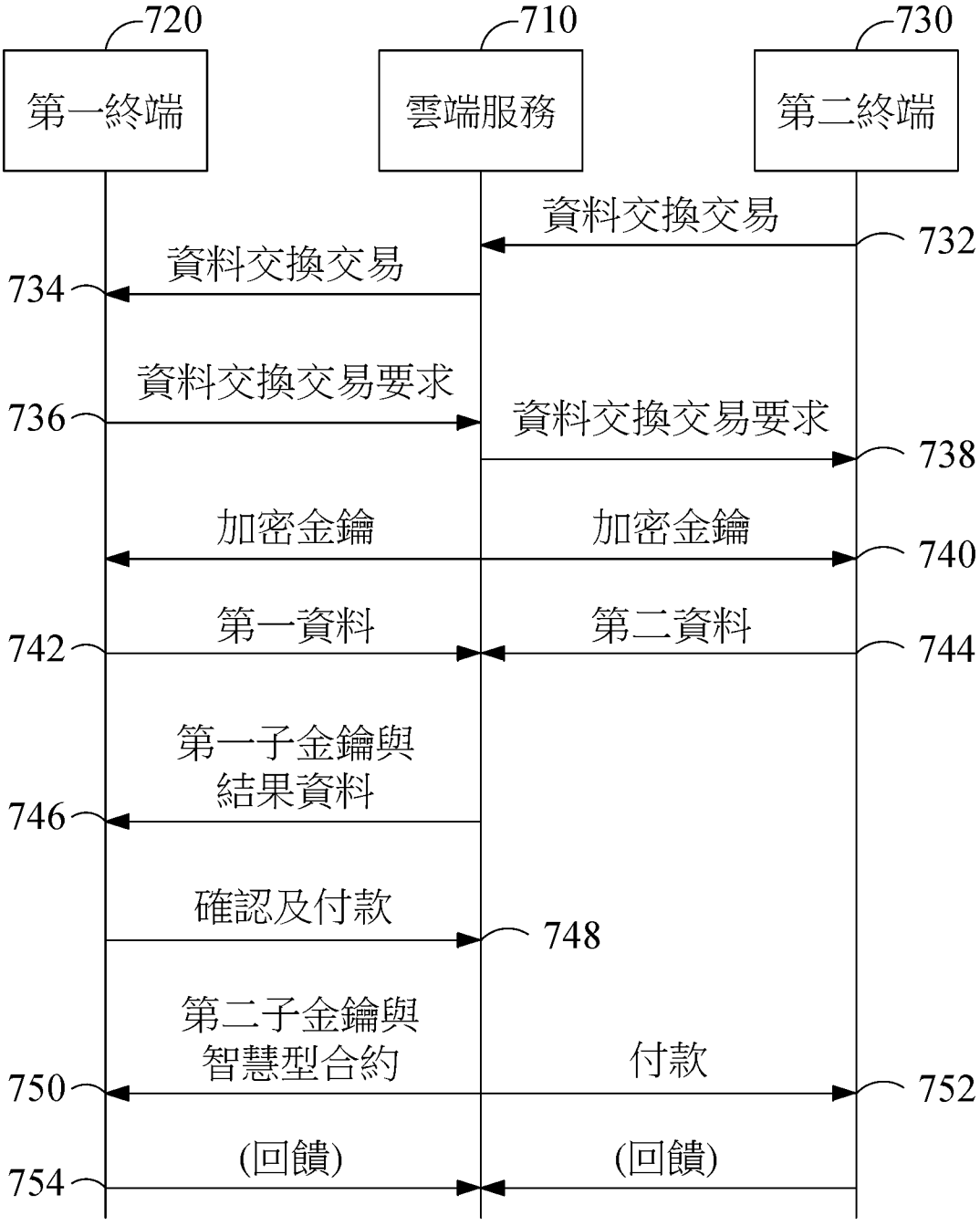
第二終端		
編號	電子郵件	興趣
B1	13f1UY$T8a	足球
B2	1k2m$#8ads	漫畫
B3	p.09&12a*x	棒球

【圖5】

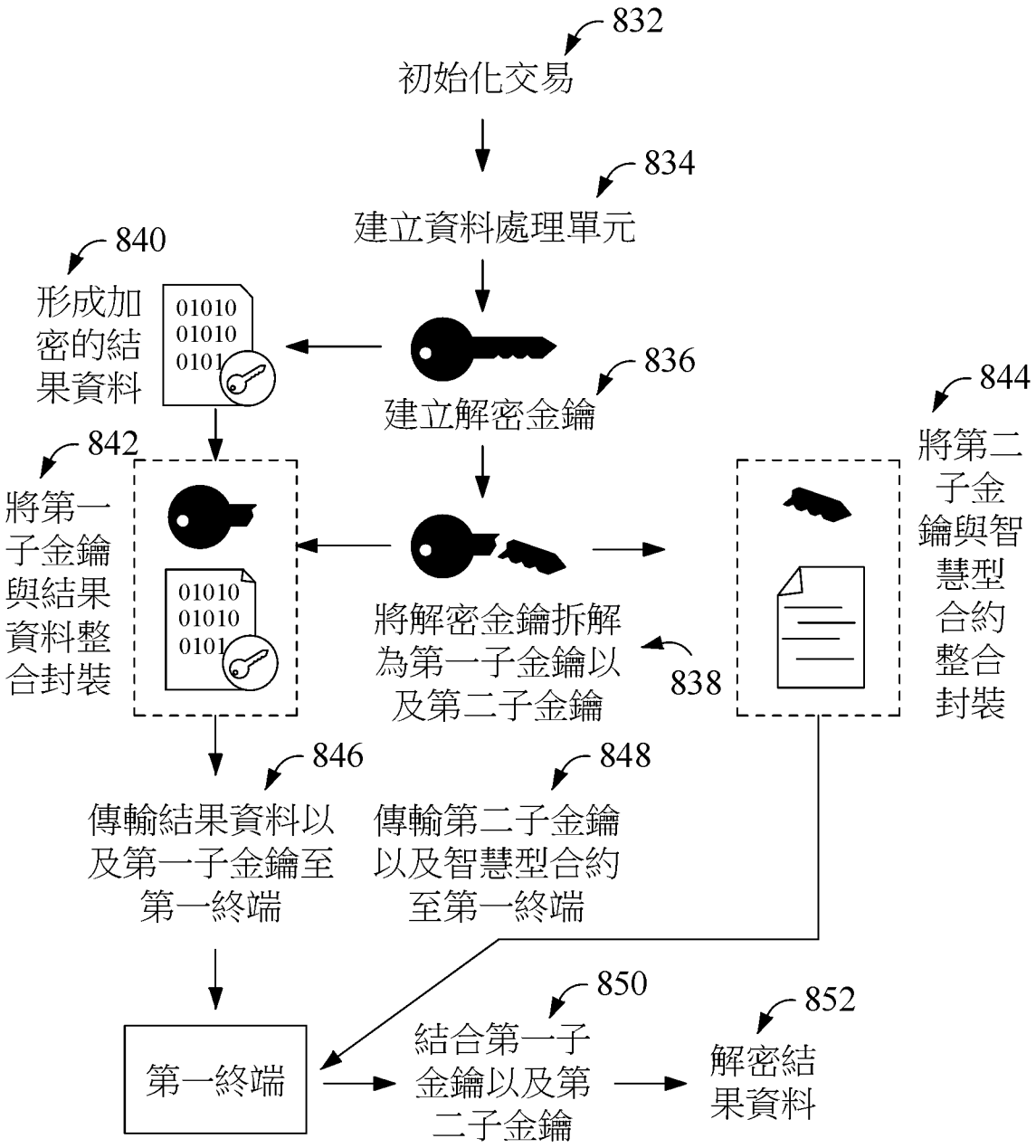
600

雲端服務		
代表符	城市	興趣
13f1UY$T8a	台北	足球
1k2m$#8ads	台南	漫畫
p.09&12a*x	高雄	棒球

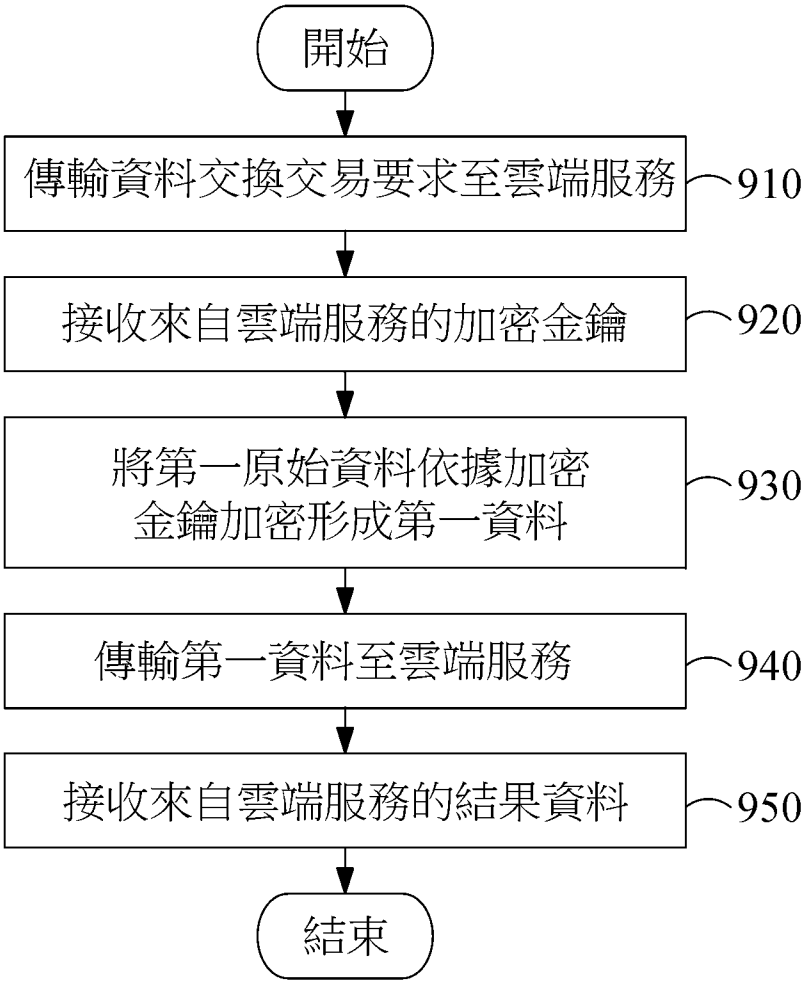
【圖6】


720
710
730
第一終端
雲端服務
第二終端
資料交換交易
732
資料交換交易
734
資料交換交易要求
736
資料交換交易要求
738
加密金鑰
加密金鑰
740
第一資料
第二資料
742
744
第一子金鑰與
結果資料
746
確認及付款
748
第二子金鑰與
智慧型合約
付款
750
752
(回饋)
(回饋)
754

【圖7】


832
初始化交易
834
建立資料處理單元
840
形成加密的結果資料
01010
01010
0101
836
建立解密金鑰
844
將第二子金鑰與智慧型合約整合封裝
842
將第一子金鑰與結果資料整合封裝
01010
01010
0101
將解密金鑰拆解為第一子金鑰以及第二子金鑰
838
846
傳輸結果資料以及第一子金鑰至第一終端
848
傳輸第二子金鑰以及智慧型合約至第一終端
850
結合第一子金鑰以及第二子金鑰
852
解密結果資料
第一終端

【圖8】


開始
傳輸資料交換交易要求至雲端服務
910
接收來自雲端服務的加密金鑰
920
將第一原始資料依據加密金鑰加密形成第一資料
930
傳輸第一資料至雲端服務
940
接收來自雲端服務的結果資料
950
結束

【圖9】