I729508

(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 I729508 B**

(45)公告日： 中華民國 110 (2021) 年 06 月 01 日

(21)申請案號：108134757　(22)申請日： 中華民國 108 (2019) 年 09 月 26 日

(51)Int. Cl.：　*G06F21/00　(2013.01)*　*H04L12/24　(2006.01)*

G06Q90/00　(2006.01)

(71)申請人：國立台灣大學 (中華民國) NATIONAL TAIWAN UNIVERSITY　(TW)

臺北市大安區羅斯福路 4 段 1 號

(72)發明人：林宗男 LIN, TSUNG NAN (TW) ；黃宇平 HUANG, YU PING (TW)

(74)代理人：張仲謙

(56)參考文獻：

TW	I413914	TW	201317823A
TW	201423427A	CN	110046521A
CN	110190945A	US	2019/0268150A1

Mohammed A. AlZain, Ben Soh, and Eric Pardede, " MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", In 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, pages 784-791. IEEE, 2011.

審查人員：黃彥豪

申請專利範圍項數：8 項　　圖式數：14　　共 29 頁

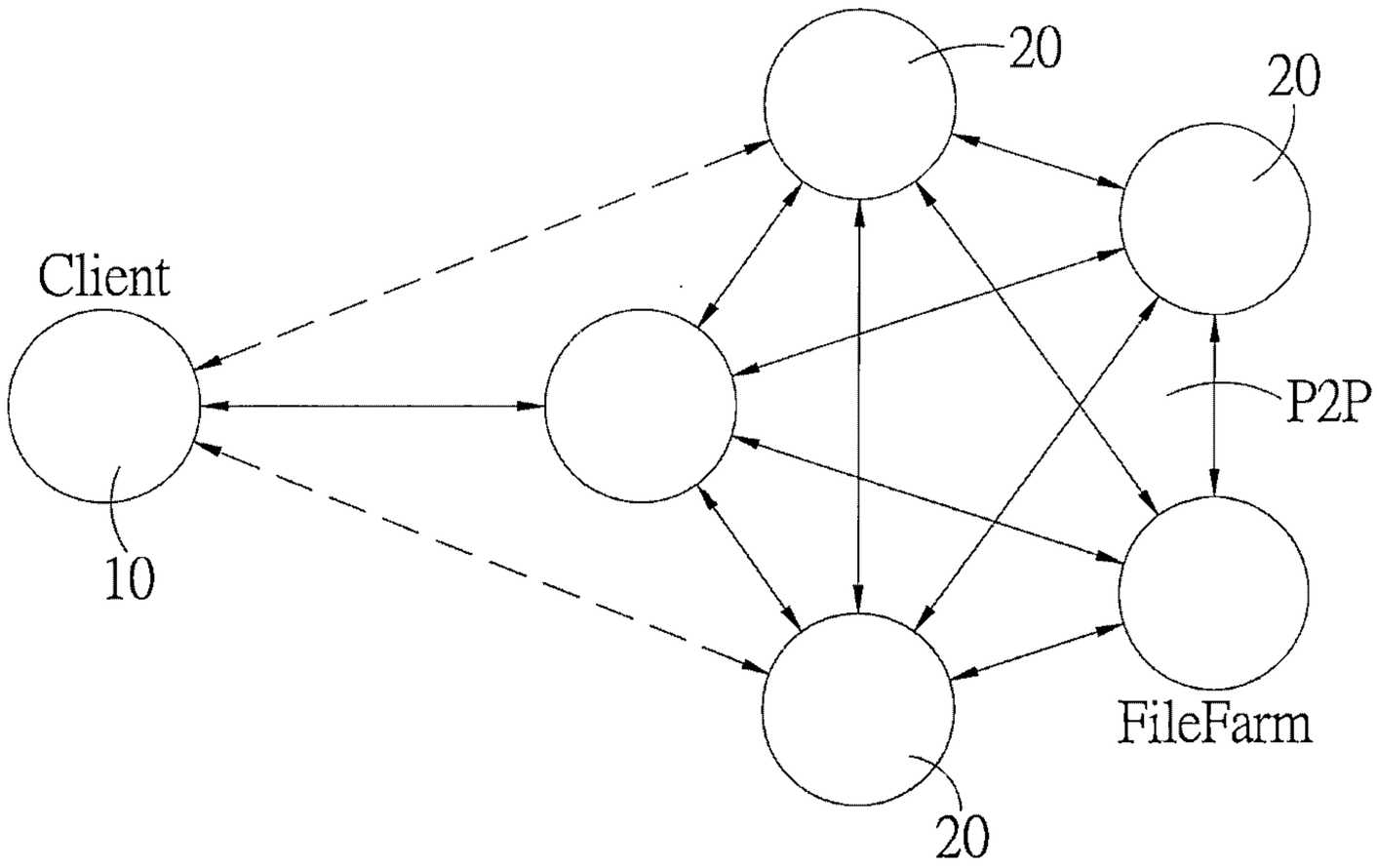
(54)名稱

雲端安全儲存系統

(57)摘要

一種雲端安全儲存系統，將使用者檔案分割及利用雜湊函數加密，並搭配資料分散演算法以產生複數個資料塊，複數個資料塊分別儲存至複數個雲端伺服器，複數個雲端伺服器為複數個資料塊備份為備份檔案；若複數個雲端伺服器之其一的資料塊遺失，鄰近雲端伺服器傳送備份檔案至遺失資料塊的雲端伺服器。本發明之雲端安全儲存系統，由於檔案分割、加密、備份檔案以及演算法的流程，成功讓使用者檔案安全儲存在複數個雲端伺服器，阻擋網路的惡意攻擊。

指定代表圖：



符號簡單說明：

10:使用者伺服器

20:雲端伺服器

Client:使用者端

FileFarm:農場端

P2P:點對點網路

【第1圖】

110年01月19日 所提修正

I729508

【發明摘要】

公告本

【中文發明名稱】

雲端安全儲存系統

【英文發明名稱】

CLOUD SECURED STORAGE SYSTEM

【中文】

一種雲端安全儲存系統，將使用者檔案分割及利用雜湊函數加密，並搭配資料分散演算法以產生複數個資料塊，複數個資料塊分別儲存至複數個雲端伺服器，複數個雲端伺服器為複數個資料塊備份為備份檔案；若複數個雲端伺服器之其一的資料塊遺失，鄰近雲端伺服器傳送備份檔案至遺失資料塊的雲端伺服器。本發明之雲端安全儲存系統，由於檔案分割、加密、備份檔案以及演算法的流程，成功讓使用者檔案安全儲存在複數個雲端伺服器，阻擋網路的惡意攻擊。

【指定代表圖】圖 1。

【代表圖之符號簡單說明】

10：使用者伺服器

20：雲端伺服器

Client：使用者端

FileFarm：農場端

P2P：點對點網路

【發明說明書】

【中文發明名稱】

雲端安全儲存系統

【英文發明名稱】

CLOUD SECURED STORAGE SYSTEM

【技術領域】

【0001】 本發明關於一種利用多個雲端伺服器並搭配檔案分割、加密、備份檔案以及演算法的流程阻擋網路惡意攻擊之雲端安全儲存系統。

【先前技術】

【0002】 雲端儲存服務為使用者帶來許多便利，提供雲端儲存服務的提供者隨之增加，例如：Google Cloud、Amazon S3、Microsoft Azure和Apple iCloud等。目前的雲端儲存服務乃以單個雲端硬碟提供給使用者，單個雲端硬碟僅能提供有限的儲存容量和資安保障，造成使用上的限制。

【0003】 台灣專利公告號M451587之專利前案為利用存取模組和保安模組控制檔案的輸入、輸出、加密以及解密，並搭配多個儲存模組提高儲存容量；然而，台灣專利前案以單個雲端硬碟進行加解密和儲存容量的改善，網路駭客仍容易入侵單個雲端硬碟進行資料竊取，且也並未考量到雲端硬碟中檔案遺失的狀況。

【0004】 綜觀前所述，本發明之發明者思索並設計一種雲端安全儲存系統，以期針對習知技術之缺失加以改善，進而增進產業上之實施利用。

【發明內容】

【0005】 有鑑於上述習知之問題，本發明的目的在於提供一種雲端安全儲存系統，用以解決習知技術中所面臨之問題。

【0006】 基於上述目的，本發明提供一種雲端安全儲存系統，設置於點對點網路且點對點網路包括使用者端和農場端，其包括使用者伺服器和複數個雲端伺服器。使用者伺服器設置於使用者端的節點，接收使用者檔案且其包括加解密引擎、演算法引擎以及第一傳輸介面，使用者伺服器將使用者檔案分割成複數個資料單元，加解密引擎為各複數個資料單元加密並利用雜湊函數運算出各資料單元的雜湊值，演算法引擎根據加密後的各資料單元的尺寸產生隨機矩陣，演算法引擎根據加密後的各資料單元和隨機矩陣演算出複數個資料塊，複數個資料塊和複數個資料單元的數目彼此相異，第一傳輸介面傳輸各複數個資料塊。複數個雲端伺服器設置於農場端的節點且各複數個雲端伺服器具有第二傳輸介面及編號，且複數個雲端伺服器之其一的第二傳輸介面接收複數個資料塊，接收複數個資料塊之雲端伺服器根據各編號及各複數個資料塊所對應的雜湊值，分配複數個資料塊至複數個雲端伺服器。本發明之雲端安全儲存系統，由於檔案分割、加密以及演算法的流程，成功讓使用者檔案安全儲存在複數個雲端伺服器，阻擋網路的惡意攻擊。

【0007】 較佳地，使用者伺服器具有資料庫，資料庫儲存使用者檔案的元資料以及其對應的複數個雜湊值。

【0008】 較佳地，若複數雲端伺服器包括閒置雲端伺服器，複數個雲端伺服器之其一偵測閒置雲端伺服器未運作時，將該閒置雲端伺服器排除於該農場端外。

【0009】 較佳地，各雲端伺服器備份複數個資料塊並儲存為備份檔案。

【0010】較佳地，當複數個雲端伺服器之其一所儲存的資料塊遺失時，遺失資料塊的雲端伺服器之鄰近雲端伺服器傳送備份檔案至遺失資料塊的雲端伺服器。

【0011】基於上述目的，本發明提供一種雲端安全儲存系統，設置於點對點網路且點對點網路包括使用者端和農場端，其包括使用者伺服器和複數個雲端伺服器。使用者伺服器設置於使用者端的節點且包括加解密引擎、演算法引擎以及第一傳輸介面，使用者伺服器發送具有雜湊值的的下載請求。複數個雲端伺服器設置於農場端的節點且各複數個雲端伺服器具有第二傳輸介面、編號以及資料塊，各複數個雲端伺服器之其一的第二傳輸介面接收下載請求，接收下載請求的雲端伺服器根據雜湊值尋找對應的該些雲端伺服器並收集其所具備的資料塊，接收下載請求的雲端伺服器將複數個資料塊傳送至使用者伺服器，使用者伺服器確認複數個資料塊的數目和尺寸，演算法引擎根據各資料塊所對應的逆隨機矩陣和各資料塊重建出複數個資料單元，加解密引擎為各複數個資料單元解密，使用者伺服器整合複數個資料單元為使用者檔案。本發明之雲端安全儲存系統，成功地從複數個雲端伺服器下載並搭配逆隨機矩陣重建使用者檔案。

【0012】較佳地，若複數個雲端伺服器包括閒置雲端伺服器，複數個雲端伺服器之其一偵測閒置雲端伺服器未運作時，將該閒置雲端伺服器排除於該農場端外。

【0013】較佳地，各雲端伺服器備份複數個資料塊並儲存為備份檔案。

【0014】較佳地，當複數個雲端伺服器之其一所儲存的資料塊遺失時，遺失資料塊的雲端伺服器之鄰近雲端伺服器傳送備份檔案至遺失資料塊的雲端伺

服器。透過前述的設置，將備份檔案即時傳送至遺失資料塊的雲端伺服器，使用者檔案能據此重建。

【0015】較佳地，複數個雲端伺服器分為私有伺服器和公有伺服器；其中，當私有伺服器的第二傳輸介面接收下載請求時，私有伺服器優先收集該些雲端伺服器所具備的資料塊；當公有伺服器的第二傳輸介面接收下載請求時，公有伺服器根據雜湊值尋找對應的複數個資料塊並從該些雲端伺服器收集複數個資料塊。

【0016】承上所述，本發明之雲端安全儲存系統，由於檔案分割、加密、備份檔案以及演算法的流程，成功讓使用者檔案安全儲存在複數個雲端伺服器，阻擋網路的惡意攻擊。

【圖式簡單說明】

【0017】第1圖為本發明之雲端安全儲存系統之第一實施例的配置圖。

【0018】第2圖為本發明之雲端安全儲存系統之第一實施例的方塊圖。

【0019】第3圖為本發明之雲端安全儲存系統之第一實施例的流程圖。

【0020】第4圖為本發明之雲端安全儲存系統之資料分散演算法的示意圖。

【0021】第5圖為本發明之雲端安全儲存系統之第二實施例的配置圖。

【0022】第6圖為本發明之雲端安全儲存系統之第二實施例的流程圖。

【0023】第7圖為本發明之雲端安全儲存系統之節點查詢(NODE_LOOKUP)的次數圖。

【0024】第8圖為本發明之雲端安全儲存系統之雜湊值查詢(VALUE_LOOKUP)的次數圖。

【0025】 第9圖為本發明之雲端安全儲存系統之上載速率圖。

【0026】 第10圖為本發明之雲端安全儲存系統之下載速率圖。

【0027】 第11A圖至第11D圖為本發明之雲端安全儲存系統之取得率圖。

【0028】 第12圖為本發明之雲端安全儲存系統之傳輸費圖。

【0029】 第13圖為本發明之雲端安全儲存系統之第三實施例的註冊示意圖。

【0030】 第14圖為本發明之雲端安全儲存系統之第三實施例的登錄示意圖。

【實施方式】

【0031】 本發明之優點、特徵以及達到之技術方法將參照例示性實施例及所附圖式進行更詳細地描述而更容易理解，且本發明可以不同形式來實現，故不應被理解僅限於此處所陳述的實施例，相反地，對所屬技術領域具有通常知識者而言，所提供的實施例將使本揭露更加透徹與全面且完整地傳達本發明的範疇，且本發明將僅為所附加的申請專利範圍所定義。

【0032】 應當理解的是，儘管術語「第一」、「第二」等在本發明中可用於描述各種元件、部件、區域、層及/或部分，但是這些元件、部件、區域、層及/或部分不應受這些術語的限制。這些術語僅用於將一個元件、部件、區域、層及/或部分與另一個元件、部件、區域、層及/或部分區分開。因此，下文討論的「第一元件」、「第一部件」、「第一區域」、「第一層」及/或「第一部分」可以被稱為「第二元件」、「第二部件」、「第二區域」、「第二層」及/或「第二部分」，而不悖離本發明的精神和教示。

【0033】另外，術語「包括」及/或「包含」指所述特徵、區域、整體、步驟、操作、元件及/或部件的存在，但不排除一個或多個其他特徵、區域、整體、步驟、操作、元件、部件及/或其組合的存在或添加。

【0034】除非另有定義，本發明所使用的所有術語(包括技術和科學術語)具有與本發明所屬技術領域的普通技術人員通常理解的相同含義。將進一步理解的是，諸如在通常使用的字典中定義的那些術語應當被解釋為具有與它們在相關技術和本發明的上下文中的含義一致的定義，並且將不被解釋為理想化或過度正式的意義，除非本文中明確地這樣定義。

【0035】請參閱第1圖至第2圖，其分別為本發明之雲端安全儲存系統之第一實施例的配置圖以及本發明之雲端安全儲存系統之第一實施例的方塊圖。如第1圖和第2圖所示，本發明之雲端安全儲存系統，設置於點對點網路P2P且點對點網路P2P包括使用者端Client和農場端FileFarm，其包括使用者伺服器10和複數個雲端伺服器20。使用者伺服器10設置於使用者端Client的節點，接收使用者檔案UF且其包括加解密引擎11、演算法引擎12、第一傳輸介面13以及資料庫14，使用者伺服器10將使用者檔案UF分割成複數個資料單元S，加解密引擎11為各複數個資料單元S加密並利用雜湊函數運算出各資料單元S的雜湊值，演算法引擎12根據加密後的各資料單元S的尺寸產生如第4圖的隨機矩陣R，演算法引擎12根據加密後的各資料單元S和隨機矩陣R演算出複數個資料塊C，複數個資料塊C和複數個資料單元S的數目彼此相異，第一傳輸介面13傳輸各複數個資料塊C，資料庫14儲存使用者檔案UF的元資料以及其對應的複數個雜湊值。複數個雲端伺服器20設置於農場端FileFarm的節點且各複數個雲端伺服器20具有第二傳輸介面21、分配模組22及編號ID，且複數個雲端伺服器20之其一的第二傳輸介面

21接收複數個資料塊C，接收複數個資料塊C之雲端伺服器20的分配模組22根據各編號ID及各複數個資料塊C所對應的雜湊值，分配複數個資料塊C至複數個雲端伺服器20，各雲端伺服器20備份複數個資料塊C並儲存為備份檔案CF。本發明之雲端安全儲存系統，由於檔案分割、加密以及演算法的流程，成功讓使用者檔案UF安全儲存在複數個雲端伺服器20，阻擋網路的惡意攻擊。

【0036】其中，演算法引擎12為利用資訊分散演算法(Information Dispersal Algorithm, IDA)進行隨機矩陣R的產生以及複數個資料塊C的演算，由於IDA演算法的設置，網路駭客難以從使用者伺服器10之外的節點進行使用者檔案UF的重建。複數個雲端伺服器20之編號ID的建立和各資料單元S的加密和雜湊值的取得為利用Kademlia網路結構(其為一種利用分散式雜湊表(Distributed Hash Table)實現的網路協定)來達成，各雲端伺服器20的分配模組根據各資料塊C的雜湊值找尋鄰近的多個雲端伺服器20及分配複數個資料塊C至鄰近的多個雲端伺服器20，複數個雲端伺服器20之編號ID的位元數根據實際所需來調整而其可例如為4或5，而未侷限於本發明所列舉的範圍。

【0037】此外，各雲端伺服器20的備份檔案CF為根據複數個雲端伺服器20的數目而調整(通常備份檔案CF的數目等於複數個雲端伺服器20的數目)，而未侷限於本發明所列舉的範圍；當複數個雲端伺服器20之其一所儲存的資料塊C遺失時(此時雲端伺服器20僅遺失部份資料塊C而非其內並無任何資料塊C)，遺失資料塊C的雲端伺服器20之鄰近雲端伺服器20察覺遺失部分資料塊C的雲端伺服器20而傳送備份檔案CF至遺失資料塊C的雲端伺服器20。若複數個雲端伺服器20包括閒置雲端伺服器(未正常運作的雲端伺服器20)，鄰近閒置雲端伺服器之雲端

伺服器察覺閒置雲端伺服器並未運作，將閒置雲端伺服器排除於農場端FileFarm外。

【0038】另，使用者伺服器10和雲端伺服器20可為工作站電腦以及超級電腦，當然也可為其他具有伺服器功能的電子裝置，而未侷限於本發明所列舉的範圍。

【0039】請參閱第3圖及第4圖，其分別為發明之雲端安全儲存系統之第一實施例的流程圖以及本發明之雲端安全儲存系統之資料分散演算法的示意圖。如第3圖和第4圖所示，並搭配第1圖和第2圖，說明本發明之雲端安全儲存系統之上傳使用者檔案UF的流程如下：(1)S11步驟：使用者透過電子裝置上傳使用者檔案UF至使用者伺服器10；或者，使用者所使用的電子裝置具有使用者伺服器10，使用者伺服器10接收使用者檔案UF。其中，電子裝置包括桌上型電腦、筆記型電腦、平板電腦以及手機，當然也可為其他具有網路功能的電子裝置，而未侷限於本發明所列舉的範圍。

【0040】(2)S12步驟：使用者伺服器10分割使用者檔案UF為複數個資料單元S。

【0041】(3)S13步驟：加解密引擎11利用雜湊函數對複數個資料單元S加密，加密後的每個資料單元S具有雜湊值，每個資料單元S依據其位元長度而具有不同的雜湊值，因此，每個資料單元S的雜湊值彼此相異。

【0042】(4)S14步驟：演算法引擎12如第4圖所示利用資訊分散演算法(IDA)演算各資料單元S的隨機矩陣R(隨機矩陣的尺寸為$(p+q)\times p$)，各資料單元S的尺寸為F bytes且具有p列，將各資料單元S和隨機矩陣R相乘而取得多個資料塊C，單個資料塊C的尺寸為$(p+q)\times\frac{|F|}{p}$；舉例來說，各資料單元S的尺寸為

16 bytes且具有4列，隨機矩陣R的尺寸為6 × 4，單個資料單元C的尺寸為6 × 4。接者，整合各資料單元S的多個資料塊C為複數個資料塊C。

【0043】(5)S15步驟：資料庫14儲存使用者檔案UF的元資料以及其對應的複數個雜湊值。

【0044】(6)S16步驟：第一傳輸介面13傳輸複數個資料塊C至複數個雲端伺服器20之其一的第二傳輸介面21。值得一提的是，由於點對點網路P2P的設置，將使用者伺服器10和複數個雲端伺服器20之間的網路結構去中心化(decentralization)，使用者伺服器10的第一傳輸介面13傳輸複數個資料塊C至任一個雲端伺服器20的第二傳輸介面21，而不需其他雲端伺服器20的存取同意(consent for a access)，簡化使用者伺服器10的傳輸。

【0045】(7)S17步驟：接收複數個資料塊C的雲端伺服器20的分配模組22根據Kademlia網路結構的特性及各雲端伺服器20的編號ID，分配複數個資料塊C至接收資料塊C的雲端伺服器20之鄰近多個雲端伺服器20，成功地完成複數個資料塊C的上傳。

【0046】請參閱第5圖及第6圖，其為本發明之雲端安全儲存系統之第二實施例的配置圖以及本發明之雲端安全儲存系統之第二實施例的流程圖。於本實施例中，相同元件符號之元件，其配置與前述類似，其類似處於此便不再加以贅述。

【0047】如第5圖所示，本發明之第二實施例與第一實施例的差異在於複數個雲端伺服器20分為公有伺服器23和私有伺服器24；一般來說，公有伺服器23為提供雲端服務者(例如：Google或Microsoft)所提供的，私有伺服器24為企業內部所建構，透過公有伺服器23和私有伺服器24的混合配置，降低公有伺服器

23之檔案傳輸費用，改善檔案下載的速度。其中，私有伺服器24享有優先下載(prioritized download)的權利，亦即，私有伺服器24較公有伺服器23立即優先下載複數個資料塊C，若複數個雲端伺服器20中並無私有伺服器24，公有伺服器23享有優先下載的權利；公有伺服器23和私有伺服器24的數目乃根據實際需求而調整，例如：公有伺服器23的數目為2，私有伺服器24的數目為3，前述僅為例舉，並未侷限於本發明所陳述的範圍。

【0048】 如第6圖所示，並搭配第1圖、第2圖以及第5圖，說明本發明之雲端安全儲存系統之上傳使用者檔案UF的流程如下：(1)S21步驟：使用者伺服器10發送下載請求，下載請求具有雜湊值。

【0049】 (2)S22步驟：複數個雲端伺服器20之其一的第二傳輸介面21接收下載請求。其中，若接收下載請求的雲端伺服器20為公有伺服器23，接續進行S23步驟；若接受下載請求的雲端伺服器20為私有伺服器24，私有伺服器24優先收集該些雲端伺服器20所具備的資料塊C，並直接進入S25步驟。

【0050】 (3)S23步驟：接收下載請求的雲端伺服器20取得下載請求的雜湊值。

【0051】 (4)S24步驟：接收下載請求的雲端伺服器20根據所取得的雜湊值及利用Kademlia網路結構中的節點查詢(NODE-LOOKUP)指令，尋找對應雜湊值之複數個資料塊C所屬的各雲端伺服器20；接收下載請求的雲端伺服器20根據所取得的雜湊值及利用Kademlia網路結構中的雜湊值查詢(VALUE-LOOKUP)指令，尋找對應雜湊值之複數個雲端伺服器20所儲存的複數個資料塊C，且會重複尋找各雲端伺服器20所儲存的複數個資料塊C直至找到對應雜湊值的資料塊C。

接著，各雲端伺服器20將對應雜湊值的複數個資料塊C傳輸至接收下載請求的雲端伺服器20。

【0052】(5)S25步驟：接收下載請求的雲端伺服器20將整合複數個資料塊C，並確認複數個資料塊C的數目和尺寸是否正確，若下載的複數個資料塊C的數目和尺寸並非上傳的複數個資料塊C的數目和尺寸，返回S24步驟，重新尋找對應雜湊值的複數個雲端伺服器20及其分別儲存的複數個資料塊C；若下載的複數個資料塊C的數目和尺寸和上傳的複數個資料塊C的數目和尺寸相符，接收下載請求的雲端伺服器20將複數個資料塊C傳輸至使用者伺服器10，進入S26步驟。

【0053】(6)S26步驟：第一傳輸介面13接收到複數個資料塊C，演算法引擎12根據各資料塊C所對應的逆隨機矩陣(逆隨機矩陣為隨機矩陣的逆矩陣)和各資料塊C重建出複數個資料單元S。

【0054】(7)S27步驟：加解密引擎11為各資料單元S解密。

【0055】(8)S28步驟：使用者伺服器10整合解密後複數個資料單元S為使用者檔案UF。

【0056】觀前所述，由於點對點網路P2P去中心化的設置和雲端伺服器20之遺失資料而自動修復的機制，使本發明的可靠度相較於以往的單一雲端伺服器而言大幅提升；另，由於加解密和資訊分散演算法的搭配，有效地防止使用者檔案UF被駭客竊取。

【0057】請參閱第7圖和第8圖，本發明之雲端安全儲存系統之節點查詢(NODE_LOOKUP)的次數圖以及本發明之雲端安全儲存系統之雜湊值查詢(VALUE_LOOKUP)的次數圖。如第7圖和第8圖所示，網路尺寸(複數個雲端伺服器20的數目)越大，節點查詢(NODE_LOOKUP)和雜湊值查詢

(VALUE_LOOKUP)的次數越多；雲端伺服器20的數目(K)越大，節點查詢(NODE_LOOKUP)和雜湊值查詢(VALUE_LOOKUP)的次數越多。其中，節點查詢(NODE_LOOKUP)的次數最大值為[log(n)] + c，n為網路尺寸，c為常數。

【0058】 請參閱第9圖和第10圖，其分別為本發明之雲端安全儲存系統之上傳速率圖以及本發明之雲端安全儲存系統之下載速率圖。如第9圖和第10圖所示，隨著資料單元S數目增加，上傳速率和下載速率都隨之增加而稍微減少，不論資料單元S數目的多寡，下載速率比上傳速率快(由於雲端伺服器20的備份檔案CF的緣故)。

【0059】 請參閱第11A圖至第11D圖，其為本發明之雲端安全儲存系統之取得率圖。如第11A圖至第11D圖所示，K為備份檔案CF的數目，q為第4圖及其對應段落所述之隨機矩陣的尺寸之q，α為雲端伺服器20在線上的機率；不論α的大小，取得率為接近1並大於0.75，亦即，複數個資料塊C的下載相當完整，使用者檔案UF的整合相當順利，而並未有資料塊C的遺失。

【0060】 舉例來說，如第11A圖所示，在K=2以及α=0.9的參數設定下，本發明可達到0.99的取得率；在K=2以及α=0.99的參數設定下，本發明可更近一步達到0.9999的取得率。

【0061】 請參閱第12圖，其為本發明之雲端安全儲存系統之傳輸費圖。如第12圖所示，公有伺服器23的數目(N)越多，傳輸費也隨之增加；採用優先下載權利的複數個雲端伺服器20則會降低傳輸費。

【0062】 請參閱第13圖以及第14圖，本發明之雲端安全儲存系統之第三實施例的註冊示意圖以及本發明之雲端安全儲存系統之第三實施例的登錄示意

圖。於本實施例中，相同元件符號之元件，其配置與前述類似，其類似處於此便不再加以贅述。

【0063】於第三實施例中，使用者檔案UF的上傳及下載與前述實施例相同，而不再重複敘述；第三實施例與其他實施例的差異之處在於加入註冊和登錄的機制，於此將描述註冊和登錄的細節如下。

【0064】如第13圖所示，並搭配第2圖，使用者從電子裝置的介面創建帳號$Account_U$和密碼$Passwd_U$，帳號$Account_U$透過雜湊函數的運算而演算出使用者編號ID_U，使用者伺服器10將使用者編號IDU傳送至農場端FileFarm的複數個雲端伺服器20，密碼$Passwd_U$透過雜湊函數的運算而演算出私鑰$PriKey_U$，使用者伺服器10確認帳號$Account_U$和密碼$Passwd_U$是否已經存在而允許使用者使用帳號$Account_U$和密碼$Passwd_U$，使用者伺服器10根據私鑰$PriKey_U$產生公鑰$PubKey_U$，使用者於電子裝置的簽章(signature)標示為SigU。

【0065】續言之，使用者伺服器10將帳號$Account_U$、使用者編號ID_U、公鑰$PubKey_U$、使用者資訊(例如姓名、電話或住址等)以及簽章Sig_U整合為憑證簽署需求CSR(certificate signing request)並將憑證簽署需求CSR傳送至管理者，管理者可決定是否同意使用者伺服器10所傳輸的憑證簽署需求CSR，若管理者同意，管理者創建同意簽章SigA並將其與帳號$Account_U$、使用者編號IDU、公鑰$PubKey_U$、使用者資訊(例如姓名、電話或住址等)以及簽章SigU整合為憑證CRT，管理者將憑證CRT傳送至農場端FileFarm的複數個雲端伺服器20，同時，管理者將憑證CRT傳送至使用者伺服器10以通知使用者註冊成功；若管理者不同意，管理者不創建同意簽章Sig_A。

【0066】如第14圖所示，使用者從電子裝置的介面登錄自己的帳號$Account_U$和密碼$Passwd_U$，使用者伺服器10據此產生使用者編號ID_U和私鑰$PriKey_U$，使用者伺服器10將使用者編號ID_U傳送至農場端FileFarm的複數個雲端伺服器20(此時，複數個雲端伺服器20已備有公鑰$PubKey_U$)，使用者伺服器10從農場端FileFarm的複數個雲端伺服器20下載憑證CRT及同意簽章Sig_A，使用者伺服器10驗證帳號$Account_U$和密碼$Passwd_U$為有效，亦即，使用者可使用農場端FileFarm的複數個雲端伺服器20進行上傳或下載使用者檔案UF。

【0067】綜上所述，本發明之雲端安全儲存系統，由於檔案分割、加密、備份檔案以及演算法的流程，成功讓使用者檔案UF安全儲存在複數個雲端伺服器20，阻擋網路的惡意攻擊。總括而言，本發明之雲端安全儲存系統，具有如上述的優點，降低傳輸費用。

【0068】以上所述僅為舉例性，而非為限制性者。任何未脫離本發明之精神與範疇，而對其進行之等效修改或變更，均應包含於後附之申請專利範圍中。

【符號說明】

【0069】

10：使用者伺服器
11：加解密引擎
12：演算法引擎
13：第一傳輸介面
14：資料庫
20：雲端伺服器
21：第二傳輸介面
22：分配模組
23：公有伺服器
24：私有伺服器

AccountU：帳號

C：資料塊

CF：備份檔案

Client：使用者端

CRT：憑證

CSR：憑證簽署需求

FileFarm：農場端

ID：編號

IDU：使用者編號

P2P：點對點網路

PasswdU：密碼

PriKeyU：私鑰

PubKeyU：公鑰

S：資料單元

SigA：同意簽章

SigU：簽章

UF：使用者檔案

S11~S17、S21~S28：步驟

【發明申請專利範圍】

【請求項1】 一種雲端安全儲存系統，設置於一點對點網路且該點對點網路包括一使用者端和一農場端(FileFarm)，其包括：

一使用者伺服器，設置於該使用者端的節點，接收一使用者檔案且其包括一加解密引擎、一演算法引擎以及一第一傳輸介面，該使用者伺服器將該使用者檔案分割成複數個資料單元，該加解密引擎為各該複數個資料單元加密並利用雜湊函數(hash function)運算出各該資料單元的雜湊值(hash value)，該演算法引擎根據加密後的各該資料單元的尺寸產生一隨機矩陣，該演算法引擎根據加密後的各該資料單元和該隨機矩陣演算出複數個資料塊，該複數個資料塊和該複數個資料單元的數目彼此相異，該第一傳輸介面傳輸各該複數個資料塊；以及

複數個雲端伺服器，設置於該農場端的節點且各該複數個雲端伺服器具有一第二傳輸介面及一編號，且該複數個雲端伺服器之其一的該第二傳輸介面接收該複數個資料塊，接收該複數個資料塊之該雲端伺服器根據各該編號及各該複數個資料塊所對應的雜湊值，分配該複數個資料塊至該複數個雲端伺服器；

其中，各該雲端伺服器備份該複數個資料塊並儲存為一備份檔案。

【請求項2】 如申請專利範圍第1項所述之雲端安全儲存系統，其中，該使用者伺服器具有一資料庫，該資料庫儲存該使用者檔案的元資料(metadata)以及其對應的該複數個雜湊值。

【請求項3】 如申請專利範圍第1項所述之雲端安全儲存系統，若該複數個雲端伺服器包括一閒置雲端伺服器，該複數個雲端伺服器之其一偵測該閒置雲端伺服器未運作時，將該閒置雲端伺服器排除於該農場端

外。

【請求項4】 如申請專利範圍第1項所述之雲端安全儲存系統，當該複數個雲端伺服器之其一所儲存的該資料塊遺失時，遺失該資料塊的該雲端伺服器之鄰近該雲端伺服器傳送該備份檔案至遺失該資料塊的該雲端伺服器。

【請求項5】 一種雲端安全儲存系統，設置於一點對點網路且該點對點網路包括一使用者端和一農場端(FileFarm)，其包括：

一使用者伺服器，設置於該使用者端的節點且包括一加解密引擎、一演算法引擎以及一第一傳輸介面，該使用者伺服器發送具有一雜湊值的一下載請求；

複數個雲端伺服器，設置於該農場端的節點且各該複數個雲端伺服器具有一第二傳輸介面、一編號以及一資料塊，各該複數個雲端伺服器之其一的該第二傳輸介面接收該下載請求，接收該下載請求的該雲端伺服器根據該雜湊值尋找對應的該些雲端伺服器並收集其所具備的該資料塊，接收該下載請求的該雲端伺服器將該複數個資料塊傳送至該使用者伺服器，該使用者伺服器確認該複數個資料塊的數目和尺寸，該演算法引擎根據各該資料塊所對應的一逆隨機矩陣和各該資料塊重建出該複數個資料單元，該加解密引擎為各該複數個資料單元解密，該使用者伺服器整合該複數個資料單元為一使用者檔案；

其中，各該雲端伺服器備份該複數個資料塊並儲存為一備份檔案。

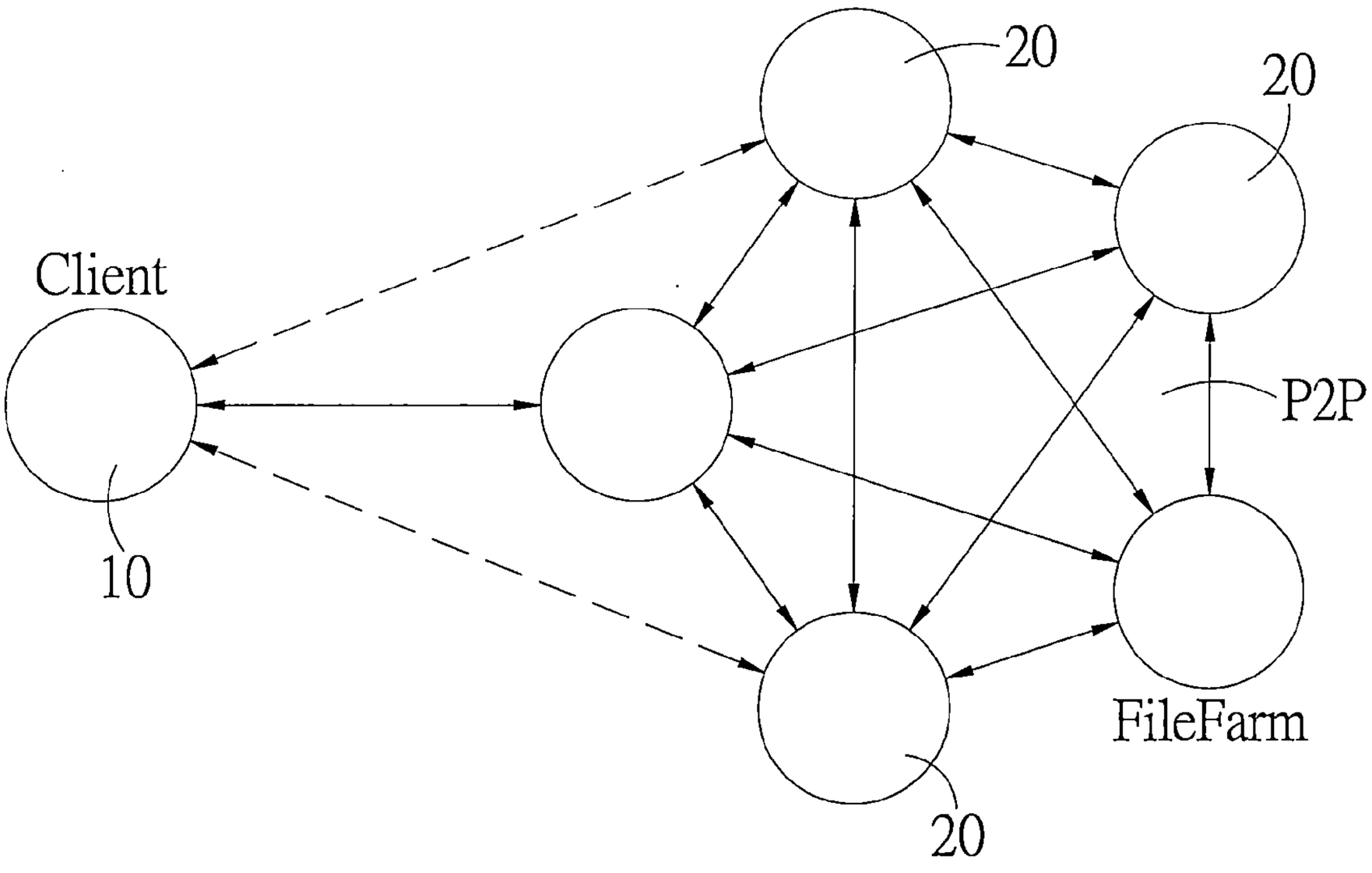
【請求項6】 如申請專利範圍第5項所述之雲端安全儲存系統，若該複數雲端伺服器包括一閒置雲端伺服器，該複數個雲端伺服器之其一偵測該閒置雲端伺服器未運作時，將該閒置雲端伺服器排除於該農場端外。

【請求項7】 如申請專利範圍第5項所述之雲端安全儲存系統，當該複數個雲端伺服器之其一所儲存的該資料塊遺失時，遺失該資料塊的該雲端伺服器之鄰近該雲端伺服器傳送該備份檔案至遺失該資料塊的該雲端伺服器。

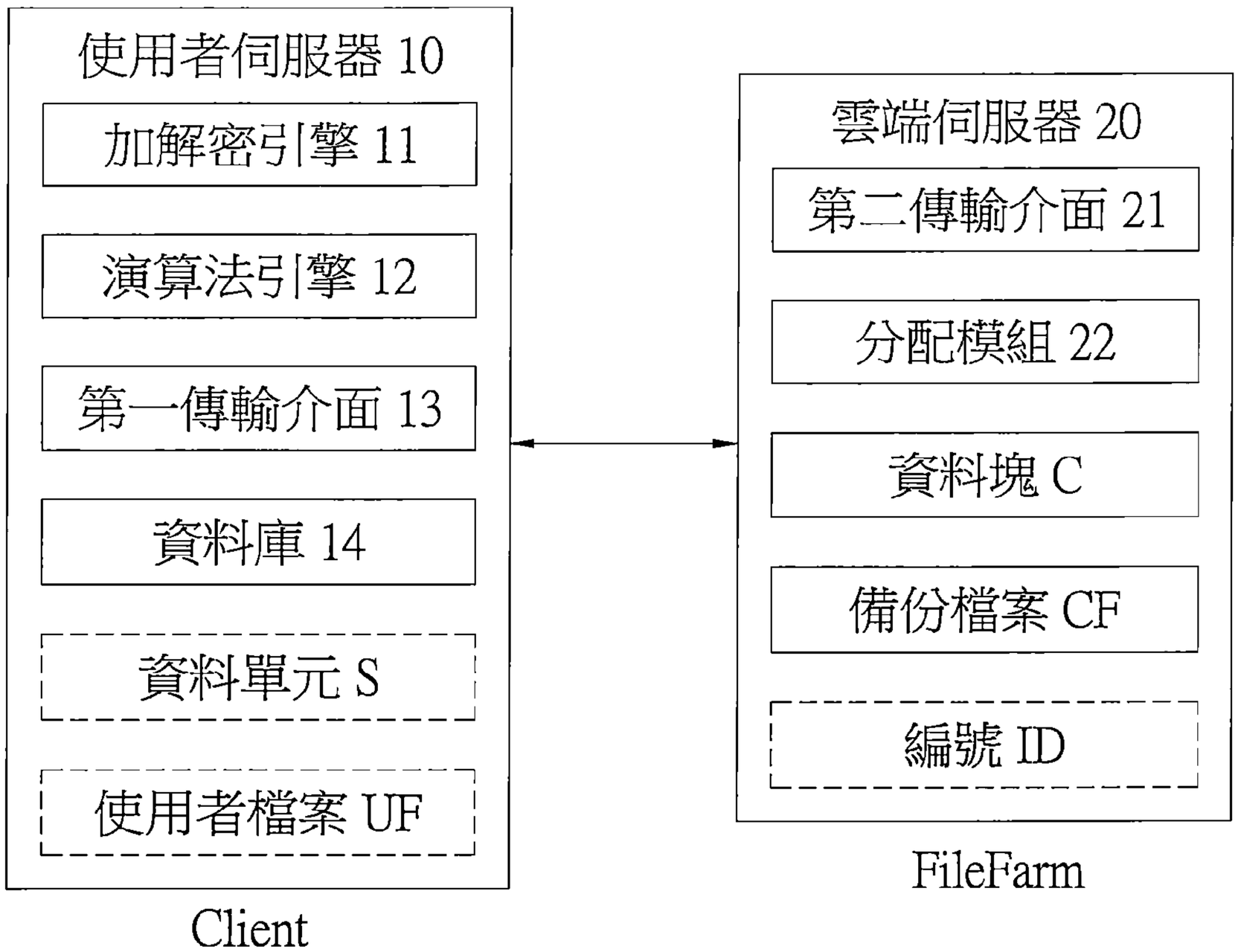
【請求項8】 如申請專利範圍第5項所述之雲端安全儲存系統，其中該複數個雲端伺服器分為一私有伺服器和一公有伺服器；

其中，當該私有伺服器的該第二傳輸介面接收該下載請求時，該私有伺服器優先收集該些雲端伺服器所具備的該資料塊；當該公有伺服器的該第二傳輸介面接收該下載請求時，該公有伺服器根據該雜湊值尋找對應的該複數個資料塊並從該些雲端伺服器收集該複數個資料塊。

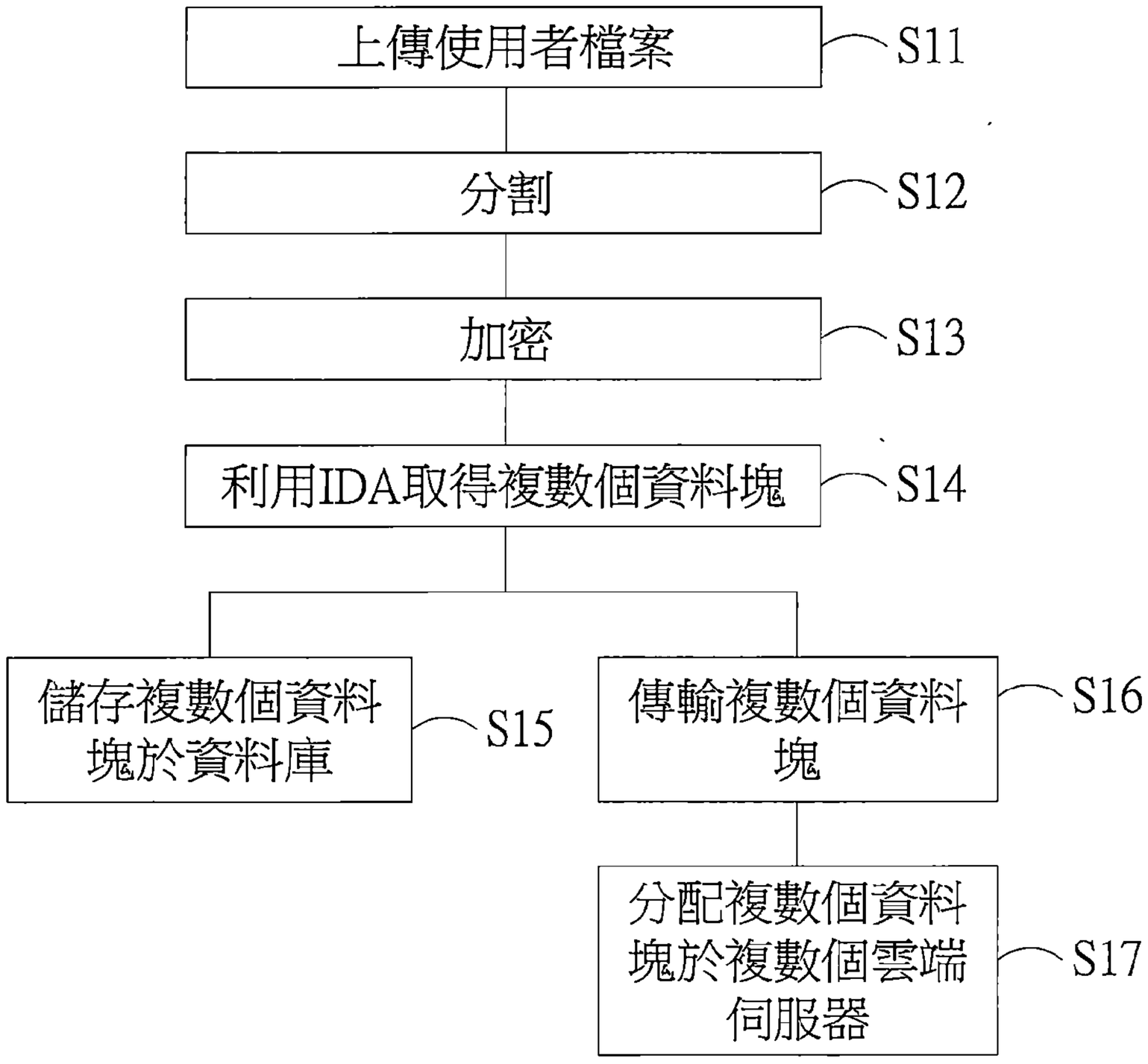
圖式



【第1圖】


使用者伺服器 10
加解密引擎 11
演算法引擎 12
第一傳輸介面 13
資料庫 14
資料單元 S
使用者檔案 UF
Client
雲端伺服器 20
第二傳輸介面 21
分配模組 22
資料塊 C
備份檔案 CF
編號 ID
FileFarm

【第2圖】


上傳使用者檔案
S11
分割
S12
加密
S13
利用IDA取得複數個資料塊
S14
儲存複數個資料塊於資料庫
S15
傳輸複數個資料塊
S16
分配複數個資料塊於複數個雲端伺服器
S17

【第3圖】

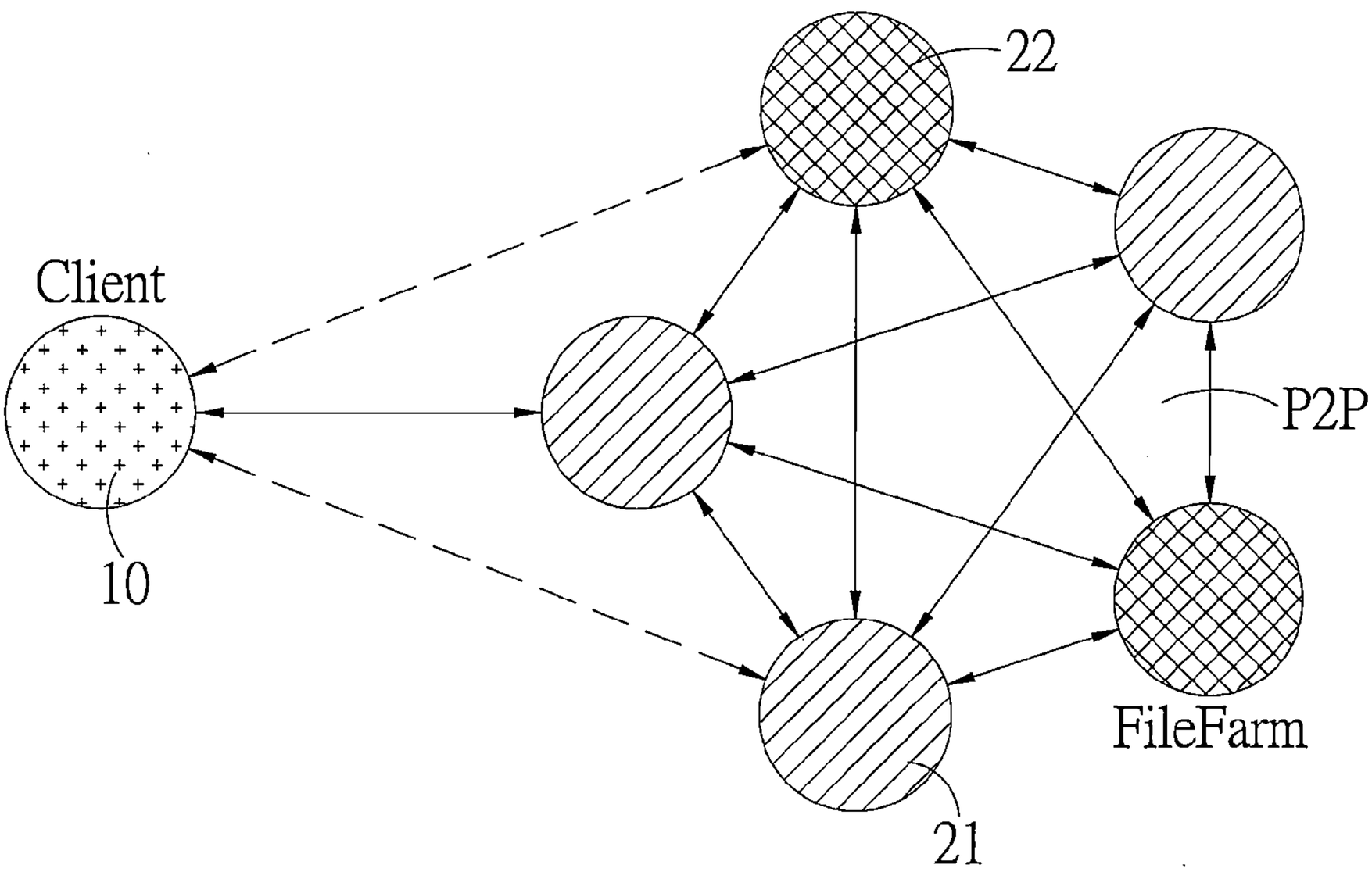
3	5	0	2	
7	4	3	2	
9	9	6	0	
0	9	3	2	
9	2	9	7	
4	8	1	9	R

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

UF

54	64	74	84	
80	96	112	128	
108	132	156	180	(p+q)資料塊
98	112	126	140	
191	218	245	272	
170	192	214	236	

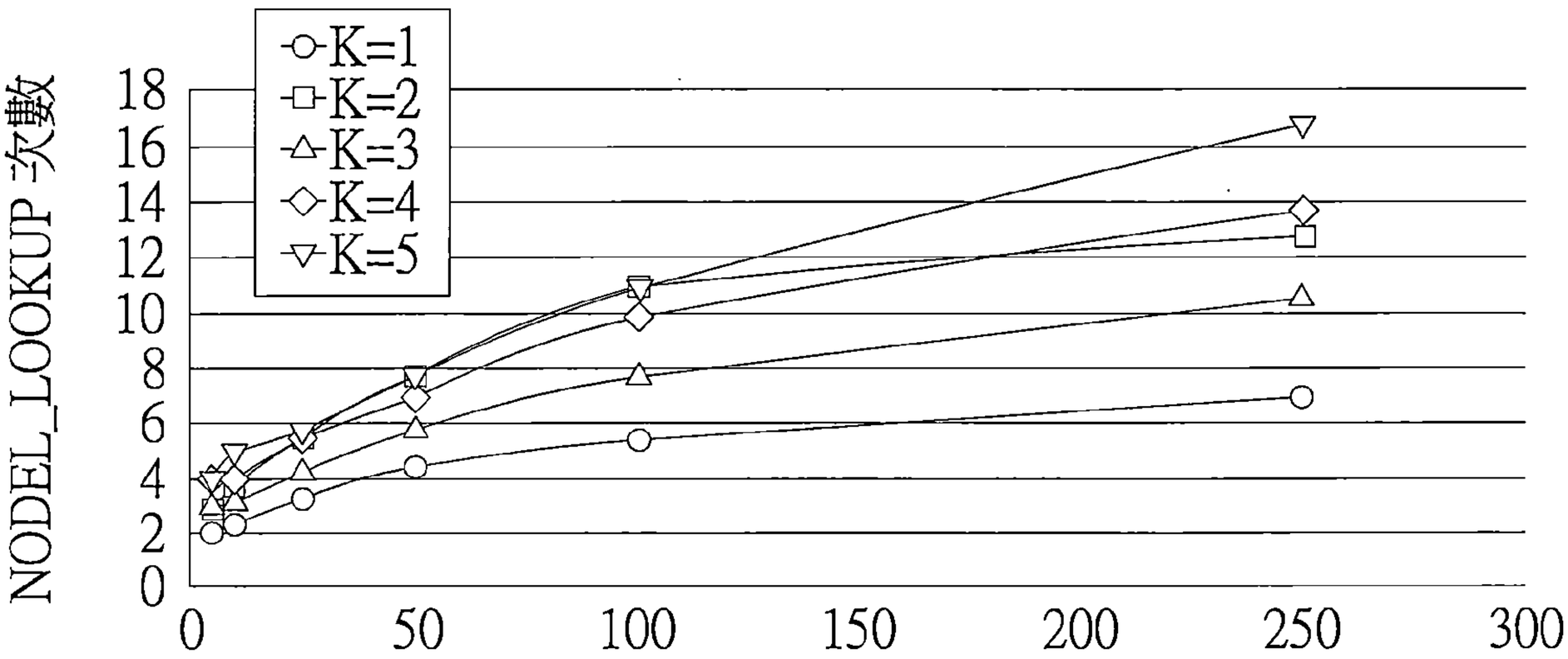
【第4圖】



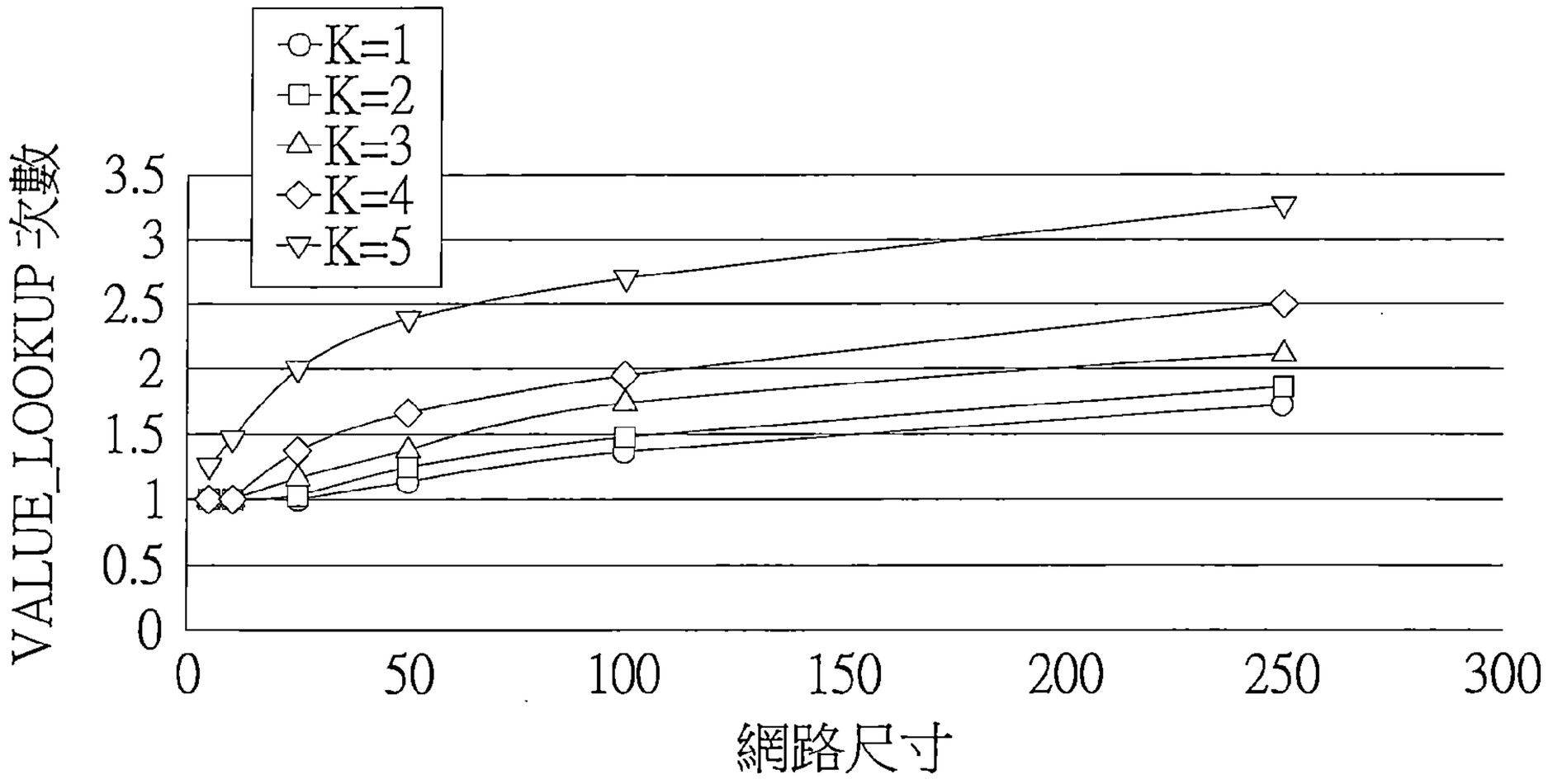
【第5圖】


發送下載請求
S21
接收下載請求
S22
取得雜湊值
S23
尋找對應的雲端伺服器
S24
確認複數個資料塊的數目和尺寸
S25
利用IDA重建複數個資料單元
S26
解密
S27
整合複數個資料單元
S28

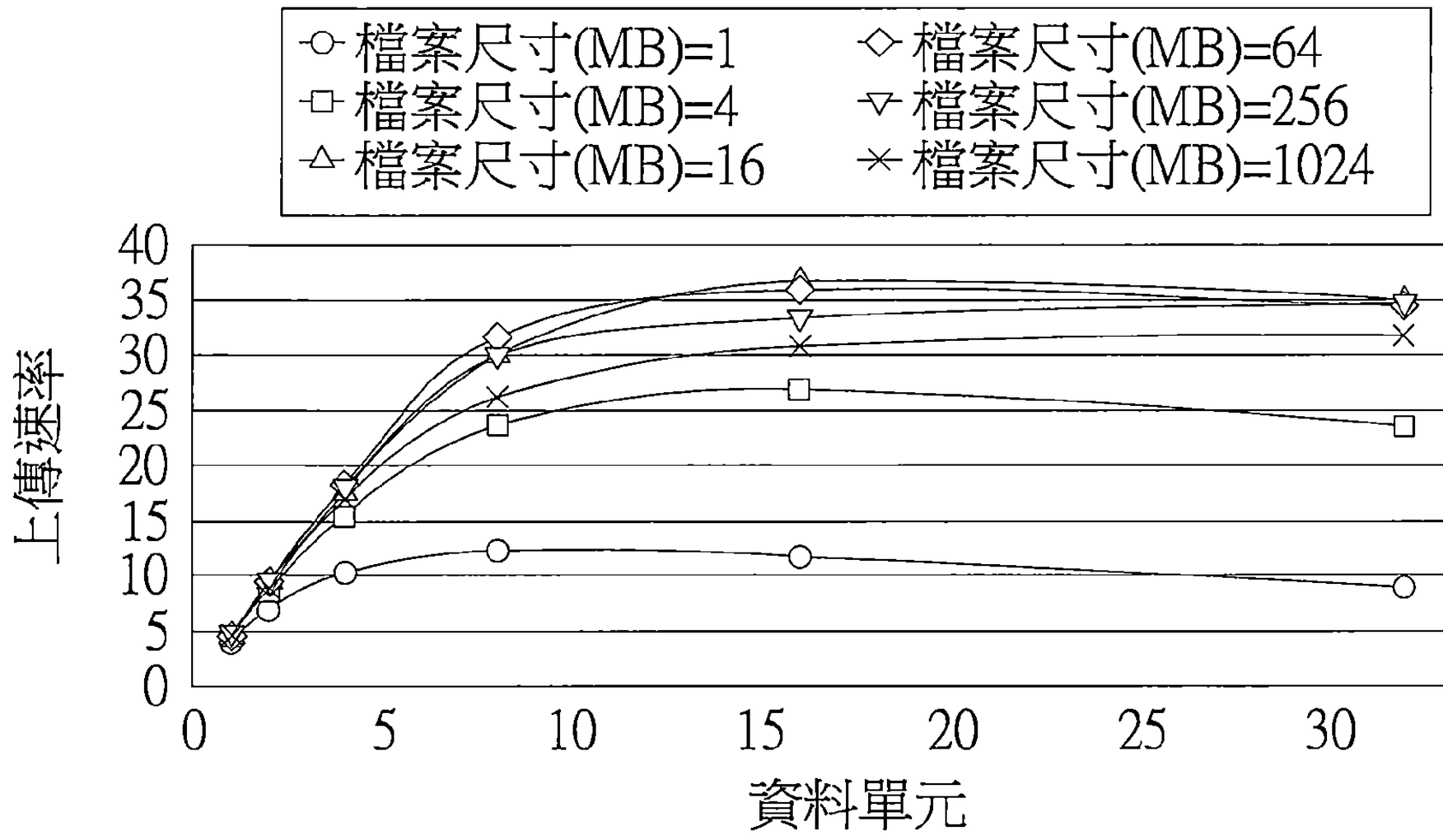
【第6圖】


K=1
K=2
K=3
K=4
K=5
NODEL_LOOKUP 次數
0
2
4
6
8
10
12
14
16
18
0
50
100
150
200
250
300
網路尺寸

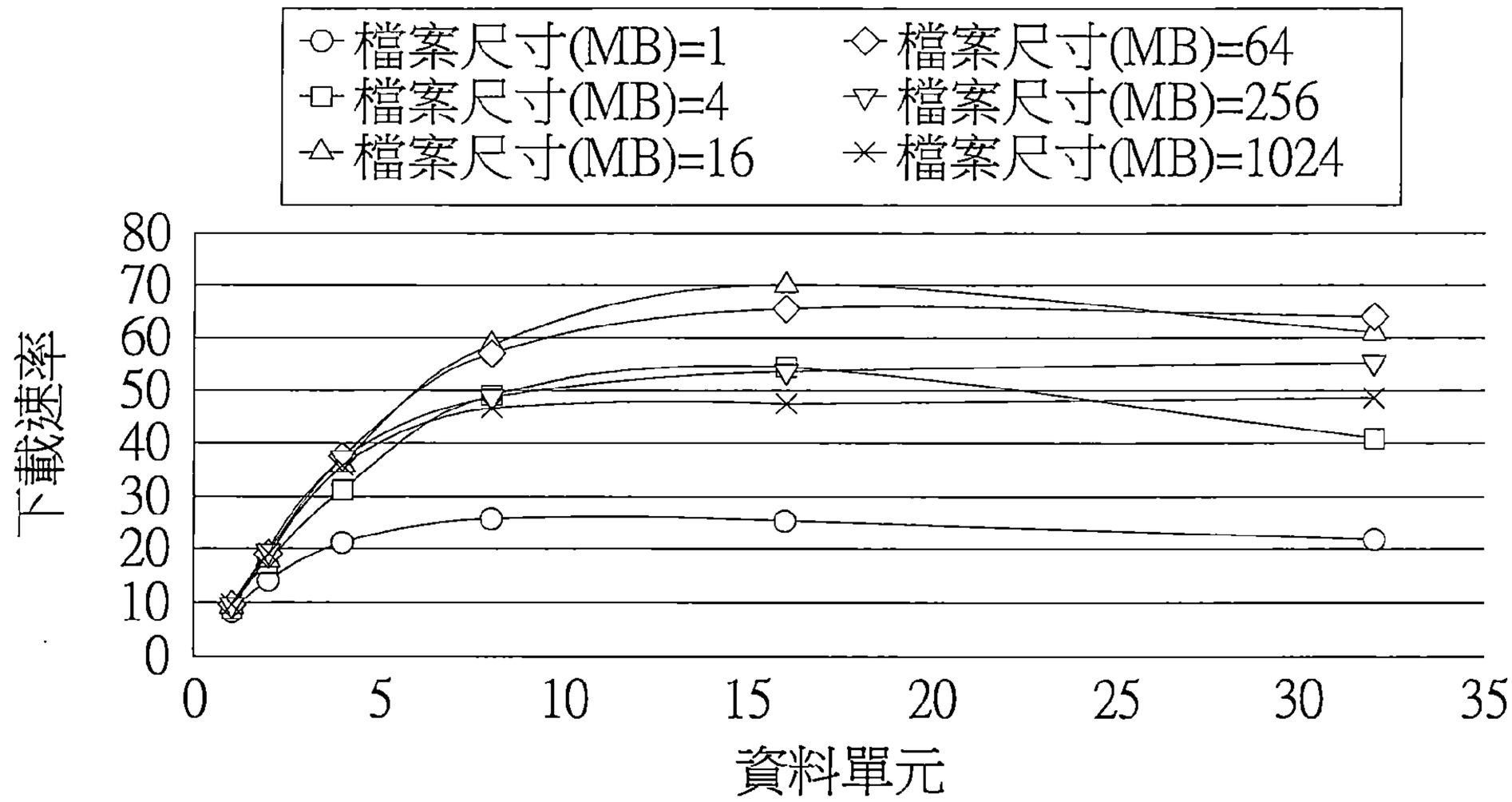
【第7圖】


K=1
K=2
K=3
K=4
K=5
VALUE_LOOKUP 次數
3.5
3
2.5
2
1.5
1
0.5
0
0
50
100
150
200
250
300
網路尺寸

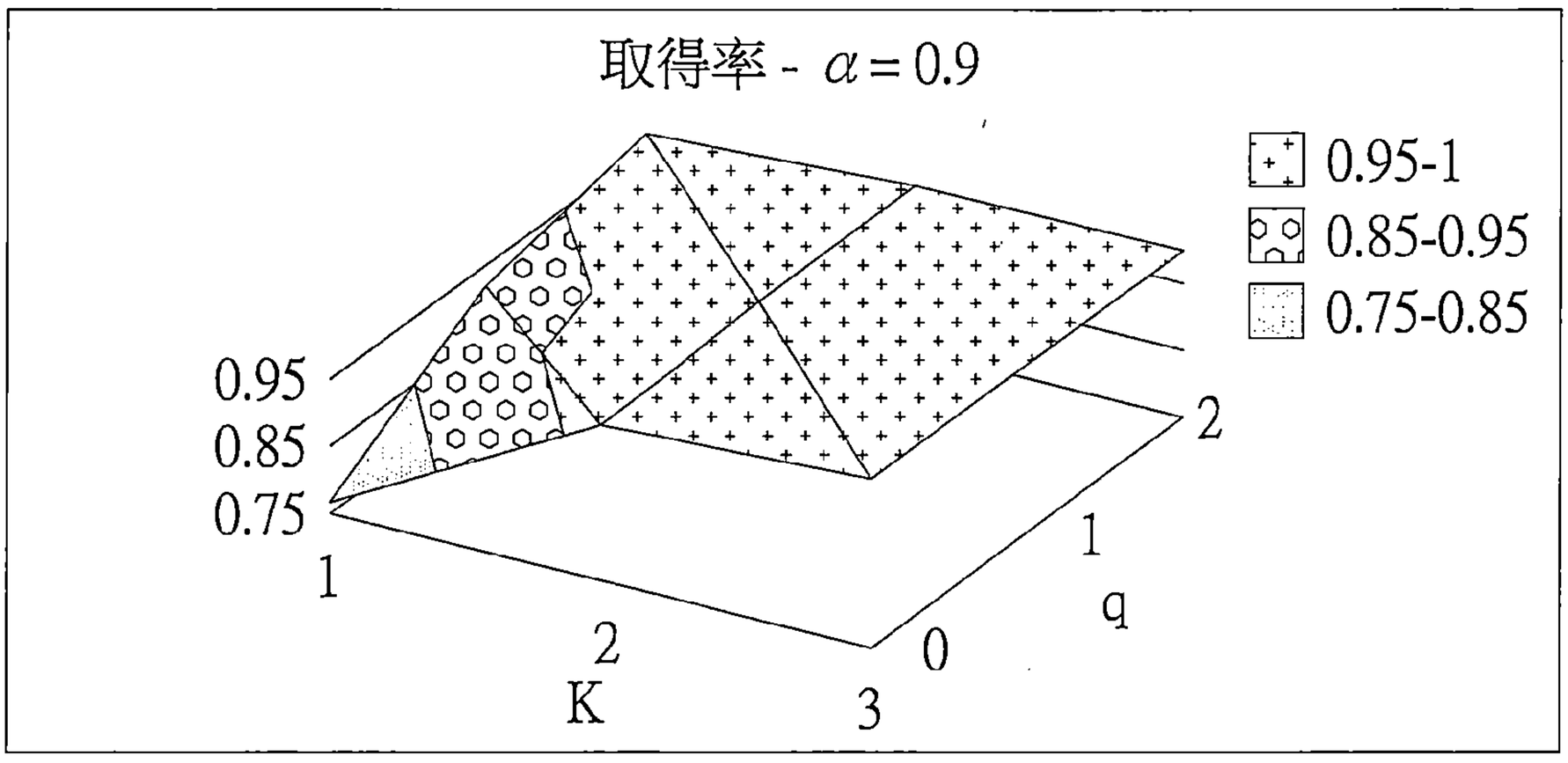
【第8圖】


檔案尺寸(MB)=1
檔案尺寸(MB)=4
檔案尺寸(MB)=16
檔案尺寸(MB)=64
檔案尺寸(MB)=256
檔案尺寸(MB)=1024
上傳速率
40
35
30
25
20
15
10
5
0
0
5
10
15
20
25
30
35
資料單元

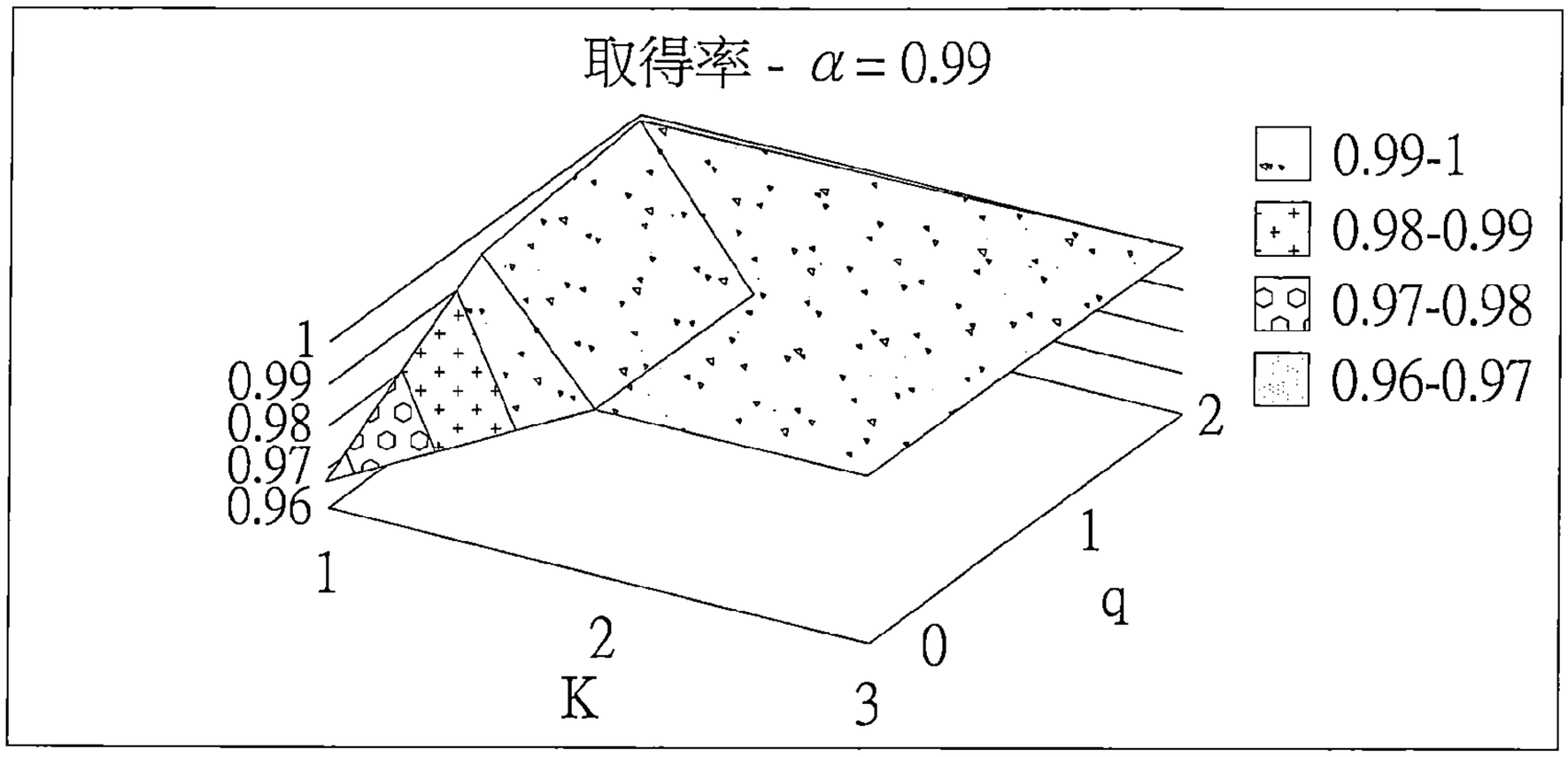
【第9圖】


檔案尺寸(MB)=1
檔案尺寸(MB)=4
檔案尺寸(MB)=16
檔案尺寸(MB)=64
檔案尺寸(MB)=256
檔案尺寸(MB)=1024
下載速率
80
70
60
50
40
30
20
10
0
0
5
10
15
20
25
30
35
資料單元

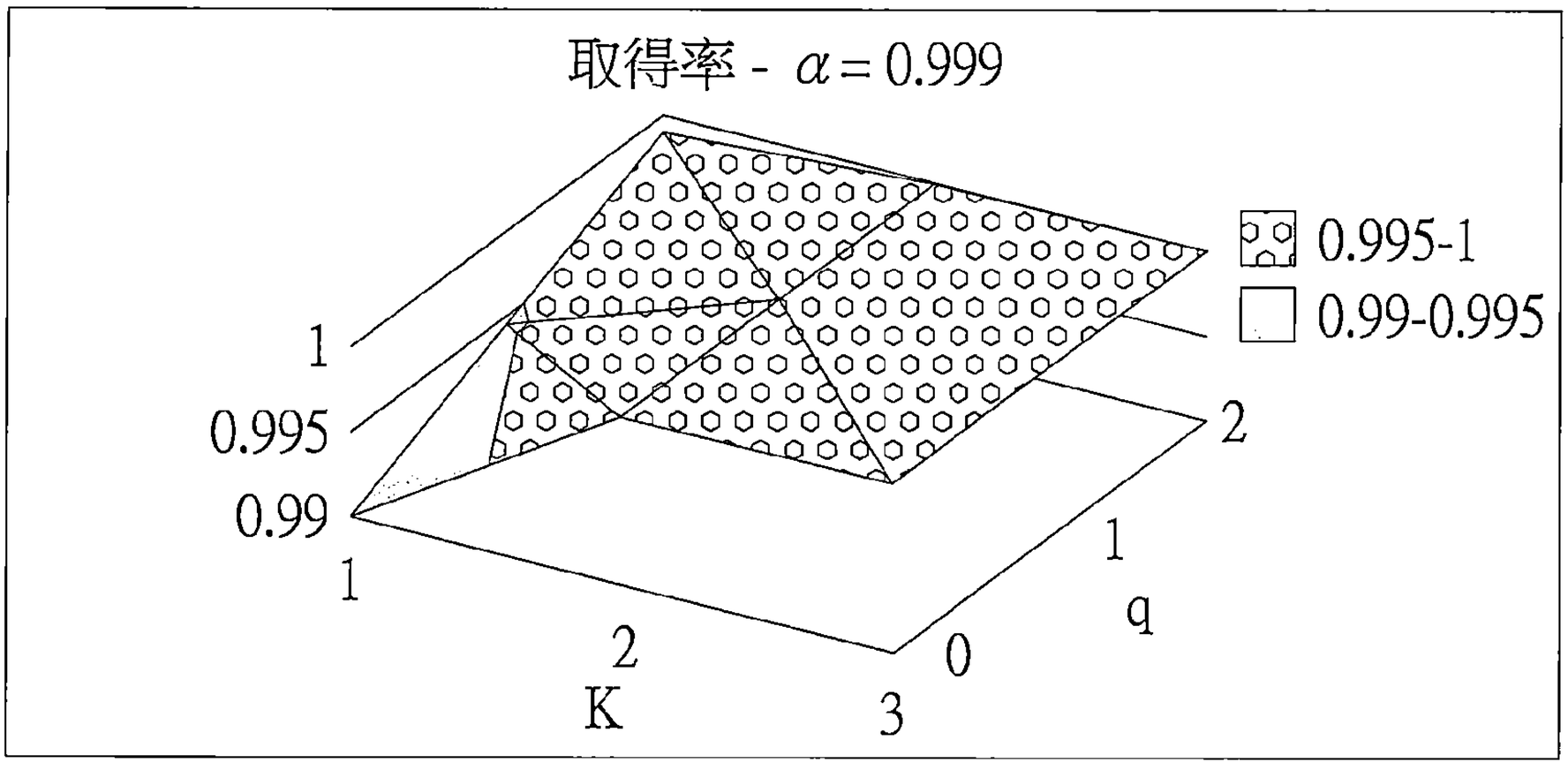
【第10圖】


取得率 - α = 0.9
0.95-1
0.85-0.95
0.75-0.85
0.95
0.85
0.75
1
2
K
3
0
1
2
q

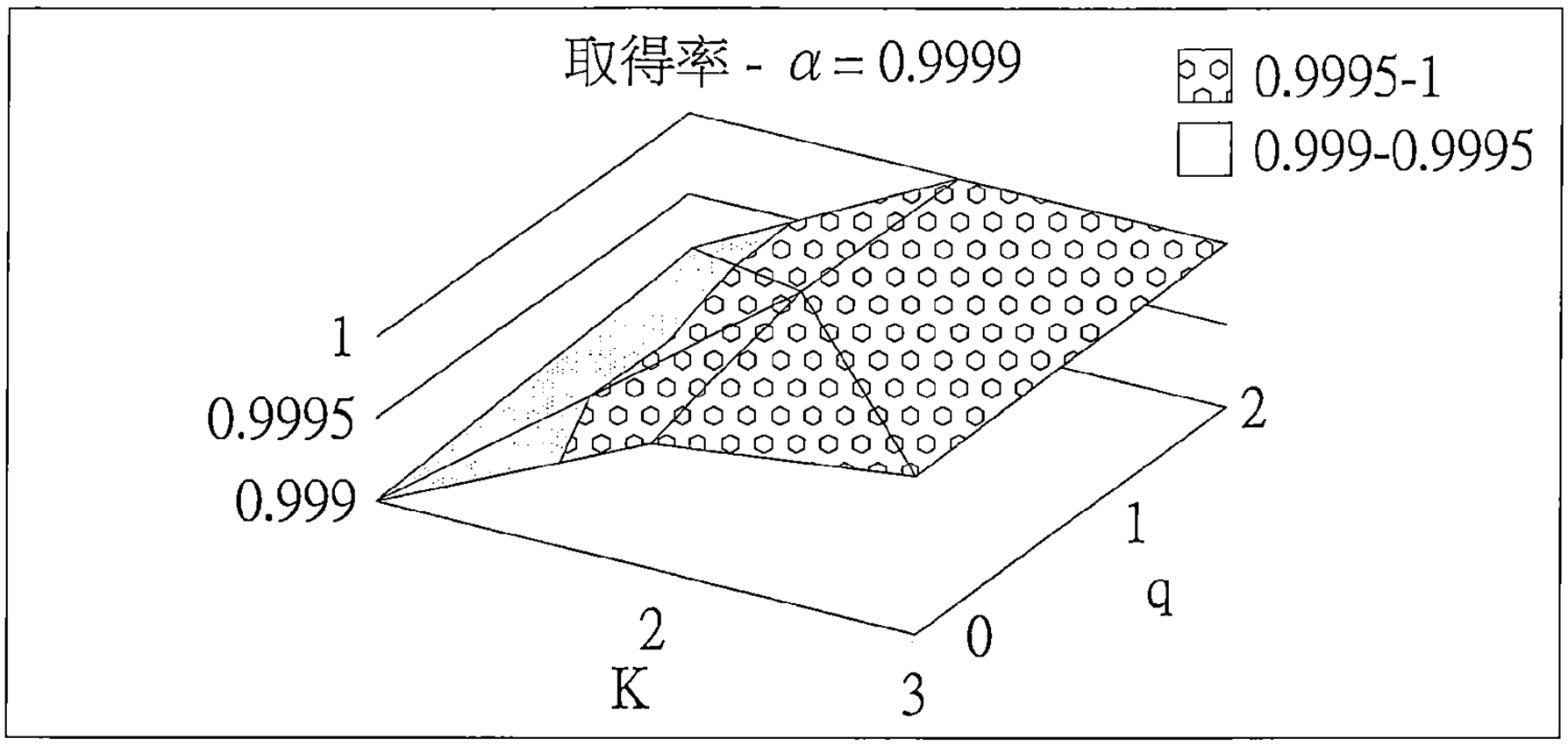
【第11A圖】


取得率 - $\alpha = 0.99$
0.99-1
0.98-0.99
0.97-0.98
0.96-0.97
1
0.99
0.98
0.97
0.96
1
2
K
2
3
0
1
q
1
2

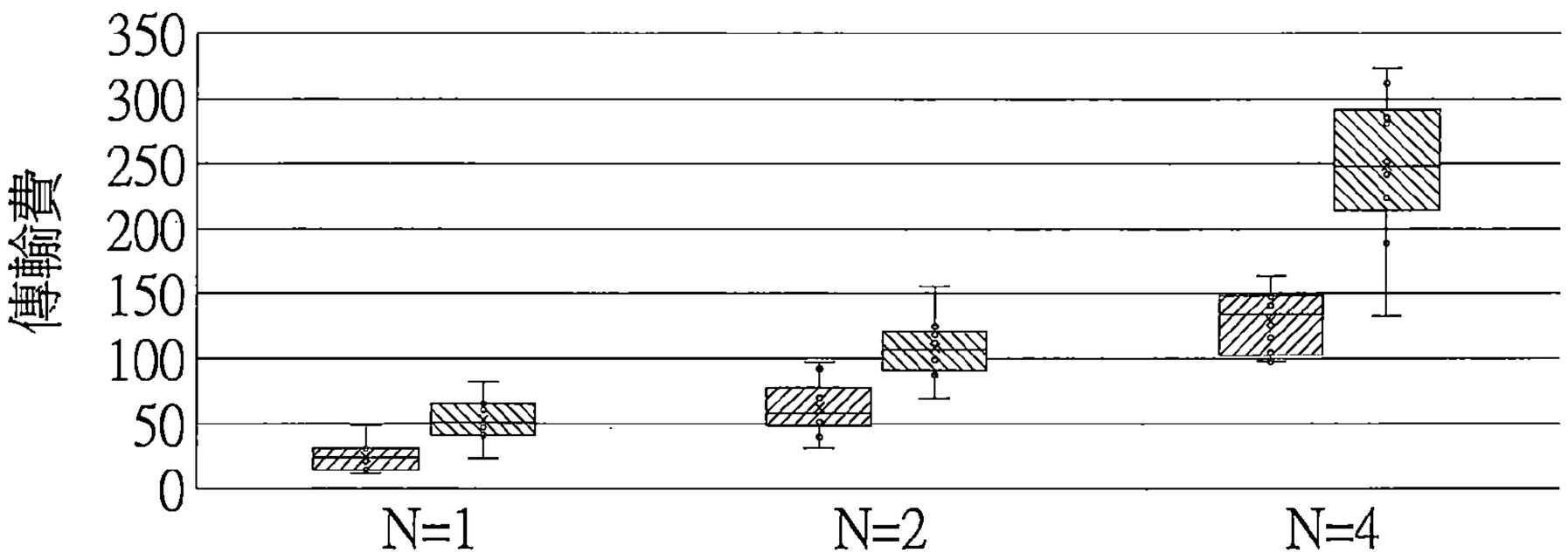
【第11B圖】


取得率 - $\alpha = 0.999$
0.995-1
0.99-0.995
1
0.995
0.99
1
2
K
2
3
0
1
q
1
2

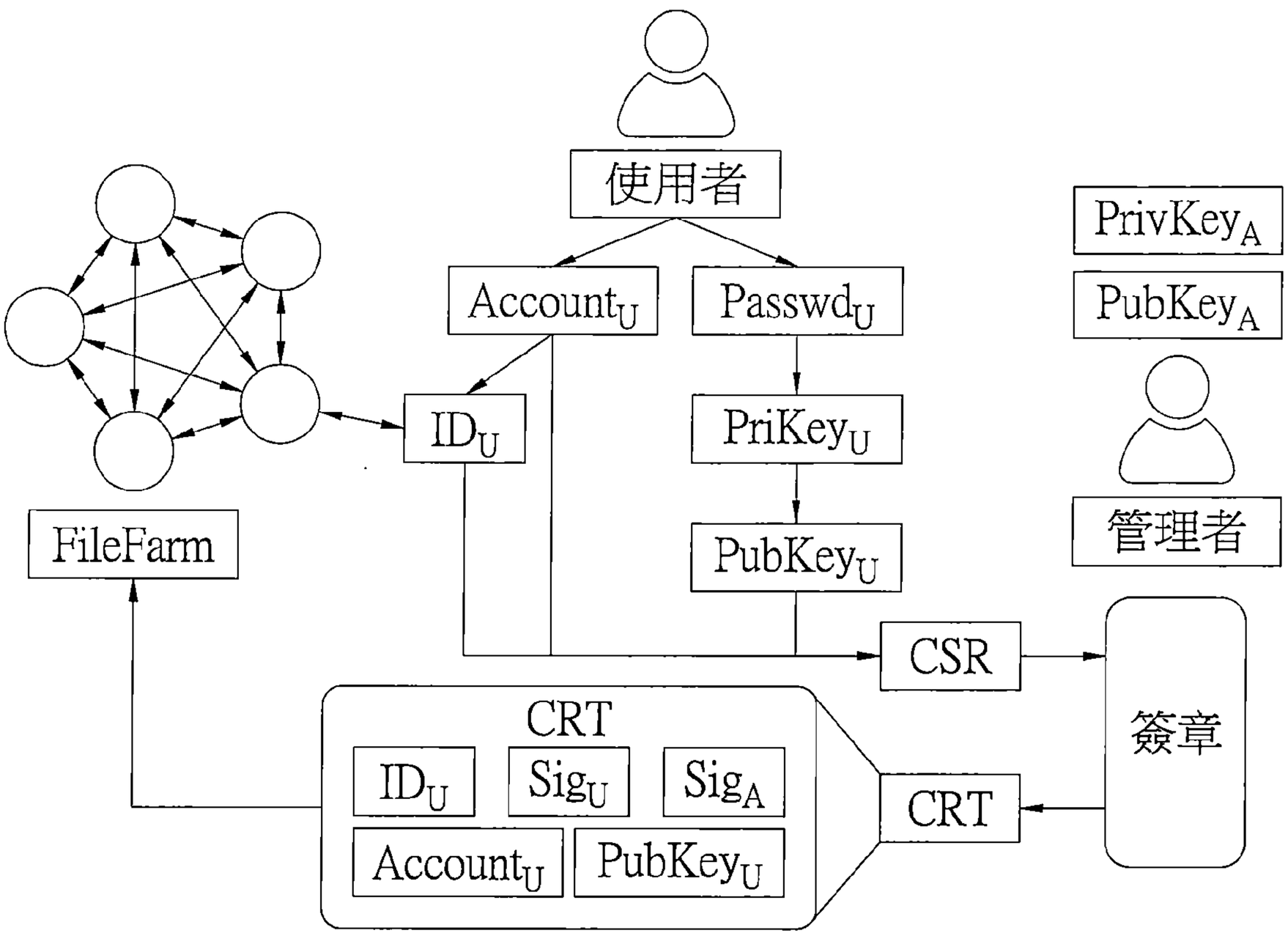
【第11C圖】


取得率 - $\alpha = 0.9999$
0.9995-1
0.999-0.9995
1
0.9995
0.999
2
1
q
2
K
0
3

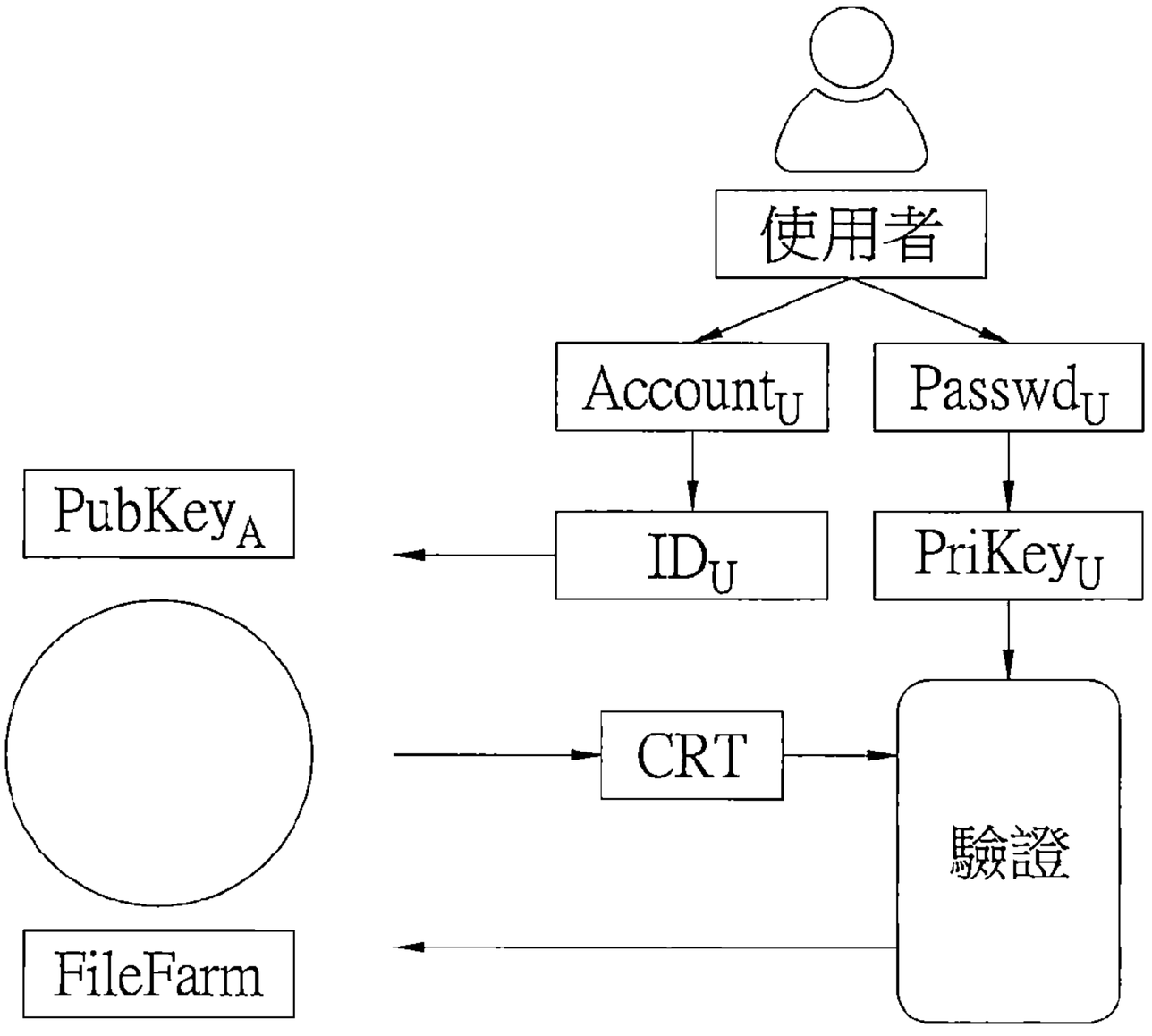
【第11D圖】


傳輸參
350
300
250
200
150
100
50
0
N=1
N=2
N=4
有優先下載
無優先下載

【第12圖】


使用者
$Account_U$
$Passwd_U$
ID_U
$PriKey_U$
$PubKey_U$
FileFarm
CSR
CRT
ID_U
Sig_U
Sig_A
$Account_U$
$PubKey_U$
CRT
簽章
$PrivKey_A$
$PubKey_A$
管理者

【第13圖】


使用者
$Account_U$
$Passwd_U$
$PubKey_A$
ID_U
$PriKey_U$
CRT
驗證
FileFarm

【第14圖】