I690821

(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 I690821 B**

(45)公告日： 中華民國 109 (2020) 年 04 月 11 日

(21)申請案號：104142501　(22)申請日： 中華民國 104 (2015) 年 12 月 17 日

(51)Int. Cl.：　*G06F21/60　(2013.01)*

(30)優先權：2015/06/02　中國大陸　201510295401.9

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED　(HK)
香港

(72)發明人：林長雄 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN	101187994A	CN	102882923A
CN	103262024A	CN	103620606A
US	2012/290926A1	US	2013/024424A1

審查人員：曾錦豐

申請專利範圍項數：16 項　圖式數：10　共 36 頁

(54)名稱

資料檔案的保護方法、裝置及終端設備

(57)摘要

本申請提供一種資料檔案的保護方法、裝置及終端設備，該方法包括：在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級；如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。在本發明的技術方案可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密。

指定代表圖：

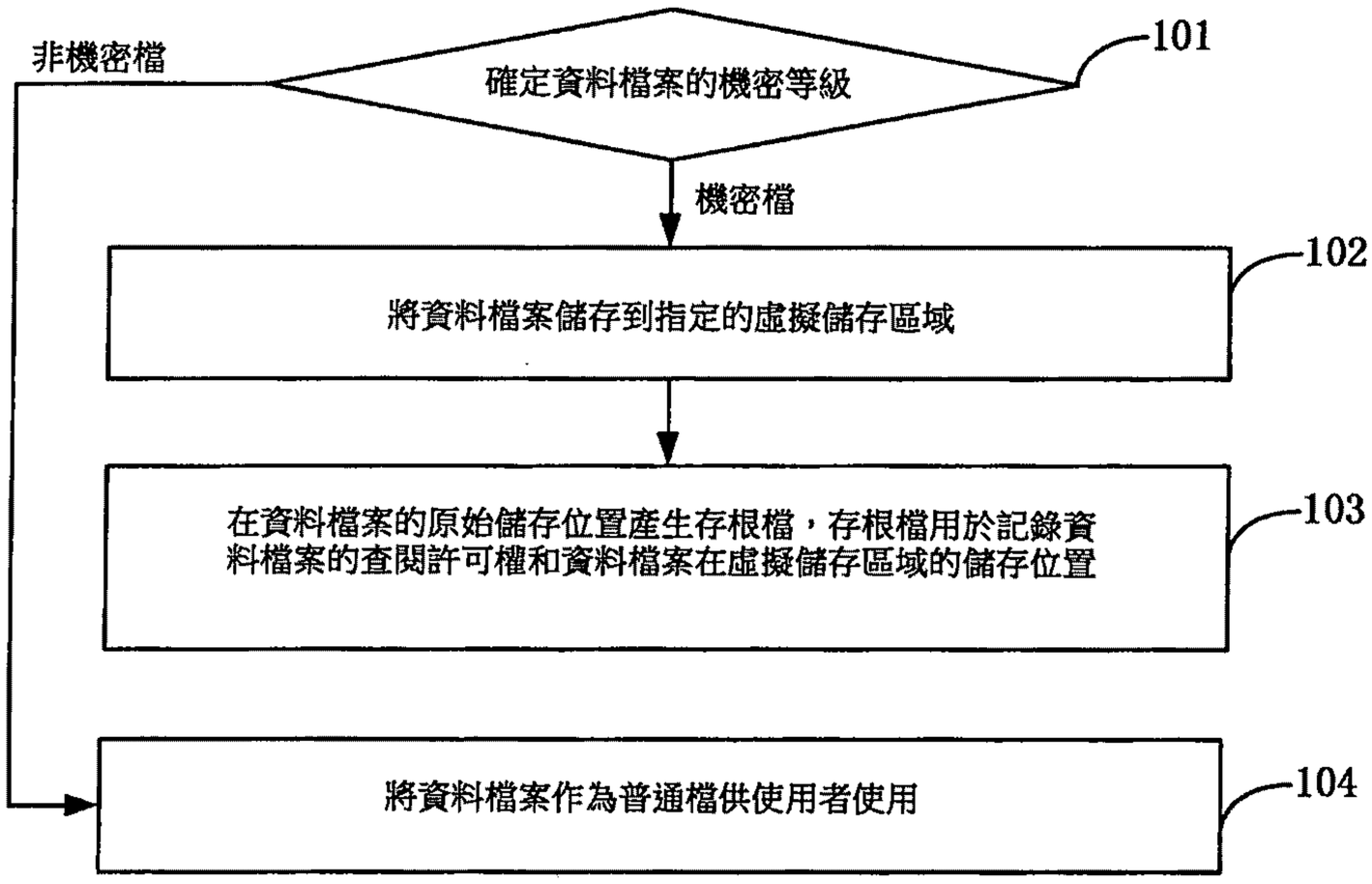
非機密檔
確定資料檔案的機密等級
101
機密檔
將資料檔案儲存到指定的虛擬儲存區域
102
在資料檔案的原始儲存位置產生存根檔，存根檔用於記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置
103
將資料檔案作為普通檔供使用者使用
104

圖 1

I690821

發明摘要

※申請案號：104142501

※申請日：104年12月17日　　※IPC 分類：*G06F 21/60* (2013.01)

【發明名稱】(中文/英文)

資料檔案的保護方法、裝置及終端設備

【中文】

本申請提供一種資料檔案的保護方法、裝置及終端設備，該方法包括：在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級；如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。在本發明的技術方案可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密。

【英文】

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

資料檔案的保護方法、裝置及終端設備

【技術領域】

本申請係關於網際網路技術領域，尤其是關於一種資料檔案的保護方法、裝置及終端設備。

【先前技術】

在網際網路自由開放的環境下，資料的使用、儲存、傳輸都存在洩漏的風險。現有技術通過檔透明加解密方法，實現對資料的保護，具體實現過程包括：終端設備的作業系統在底層處理時，將資料檔案進行加密處理，在用戶讀取資料檔案時，作業系統將資料檔案解密後放入記憶體中供使用者使用，當使用者需要保存資料檔案時，作業系統將資料檔案加密並最終寫入磁片，從而使使用者完全感覺不到對資料檔案的加解密行為。現有技術通過在磁片上寫入加密後的資料，進入記憶體解密資料的方式實現資料的防洩密，但是並不能確保記憶體中的檔不被外傳，因此仍存在檔被洩密的風險。

【發明內容】

有鑑於此，本申請提供一種新的技術方案，可以解決

在不影響資料檔案正常使用前提下的防洩密的技術問題。

為實現上述目的，本申請提供技術方案如下：

根據本申請的第一方面，提出了一種資料檔案的保護方法，應用於終端設備上，包括：

在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級；

如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；

在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

根據本申請的第二方面，提出了一種讀取資料檔案的方法，應用於終端設備上，包括：

在監聽到用戶關於存根文件的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

如果所述用戶有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

通過所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案。

根據本申請的協力廠商面，提出了一種資料檔案的保護裝置，應用於終端設備上，包括：

第一確定模組，用於在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級以及所述資料

檔案的原始儲存位置；

儲存模組，用於如果所述第一確定模組確定的所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；

存根產生模組，用於在所述第一確定模組確定的所述原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

根據本申請的第四方面，提出了一種讀取資料檔案的裝置，所述讀取資料檔案的裝置包括：

第四確定模組，用於在監聽到用戶關於所述存根產生模組產生的所述存根文件的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

啟動模組，用於如果所述第四確定模組確定所述使用者有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

訪問模組，用於通過所述啟動模組啟動的所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案。

根據本申請的第五方面，提出了一種終端設備，所述終端設備包括：

處理器；用於儲存所述處理器可執行指令的記憶體；

其中，所述處理器，用於在檢測到所述終端設備上有

資料檔案產生時，確定所述資料檔案的機密等級；

如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；

在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

根據本申請的第六方面，提出了一種終端設備，所述終端設備包括：

處理器；用於儲存所述處理器可執行指令的記憶體；

其中，所述處理器，用於在監聽到用戶關於存根文件的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

如果所述用戶有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

通過所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案

由以上技術方案可見，本申請在確定資料檔案為機密檔時，將資料檔案儲存到指定的虛擬儲存區域，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密；通過在資料檔案的原始儲存位置產生存根檔，由於存根檔只記錄記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，並未攜帶資料檔案本身的任何資料，因此使用者對存根檔的一切操作不會對資料檔案有任何影響。

【圖式簡單說明】

圖 1 示出了根據本發明的一示例性實施例的資料檔案的保護方法的流程示意圖；

圖 2 示出了根據本發明的又一示例性實施例的資料檔案的保護方法的流程示意圖；

圖 3 示出了根據本發明的一示例性實施例的讀取資料檔案的方法的流程示意圖；

圖 4 示出了根據本發明的又一示例性實施例的讀取資料檔案的方法的流程示意圖；

圖 5 示出了根據本發明的一示例性實施例的終端設備的結構示意圖；

圖 6 示出了根據本發明的又一示例性實施例的終端設備的結構示意圖；

圖 7 示出了根據本發明的一示例性實施例的資料檔案的保護裝置的結構示意圖；

圖 8 示出了根據本發明的又一示例性實施例的資料檔案的保護裝置的結構示意圖；

圖 9 示出了根據本發明的一示例性實施例的讀取資料檔案的裝置的結構示意圖；

圖 10 示出了根據本發明的又一示例性實施例的讀取資料檔案的裝置的結構示意圖。

【實施方式】

這裡將詳細地對示例性實施例進行說明，其示例表示在附圖中。下面的描述涉及附圖時，除非另有表示，不同附圖中的相同數字表示相同或相似的要素。以下示例性實施例中所描述的實施方式並不代表與本申請相一致的所有實施方式。相反，它們僅是與如所附申請專利範圍第書中所詳述的、本申請的一些方面相一致的裝置和方法的例子。

在本申請使用的術語是僅僅出於描述特定實施例的目的，而非旨在限制本申請。在本申請和所附申請專利範圍第書中所使用的單數形式的“一種”、“所述”和“該”也旨在包括多數形式，除非上下文清楚地表示其他含義。還應當理解，本文中使用的術語“和/或”是指並包含一個或多個相關聯的列出專案的任何或所有可能組合。

應當理解，儘管在本申請可能採用術語第一、第二、第三等來描述各種資訊，但這些資訊不應限於這些術語。這些術語僅用來將同一類型的資訊彼此區分開。例如，在不脫離本申請範圍的情況下，第一資訊也可以被稱為第二資訊，類似地，第二資訊也可以被稱為第一資訊。取決於語境，如在此所使用的詞語“如果”可以被解釋成為“在……時”或“當……時”或“回應於確定”。

本申請在確定資料檔案為機密檔時，將資料檔案儲存到指定的虛擬儲存區域，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密；通過在資料檔案的原始儲存位置產生存根

檔，由於存根檔只記錄記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，並未攜帶資料檔案本身的任何資料，因此使用者對存根檔的一切操作不會對資料檔案有任何影響。

為對本申請進行進一步說明，提供下列實施例：

圖 1 示出了根據本發明的一示例性實施例的資料檔案的保護方法的流程示意圖；可應用在終端設備上，如圖 1 所示，包括如下步驟：

步驟 101，在檢測到終端設備上有資料檔案產生時，確定資料檔案的機密等級，如果機密等級表示資料檔案為機密檔，執行步驟 102，如果機密等級表示資料檔案為非機密檔，執行步驟 104。

在一實施例中，可以通過拷貝、新建、下載等方式在終端設備上產生資料檔案。在一實施例中，資料檔案的機密等級可以通過使用者對資料檔案的保密程度來設置，例如，可以將機密等級設置為等級 0、等級 1、等級 2 等級別，不同的機密等級可以表示資料檔案的保密程度，例如，等級 0 表示使用者不需要對該資料檔案採用保密措施，等級 1 表示使用者需要對該資料檔案採用保密措施，或者，例如，等級 0 表示使用者不需要對該資料檔案採用保密措施，等級 1 表示使用者需要對該資料檔案在終端設備上採用保密措施，等級 2 表示使用者需要對資料檔案在終端設備上和雲端伺服器上均採用保密措施。

在一實施例中，可以先確定資料檔案的內容資訊，將

內容資訊與第一預設條件進行匹配，根據匹配的第一結果確定資料檔案的機密等級，例如，第一預設條件可以包括多個關鍵字組，例如，“加密”、“隱私”、“非公開”等等，如果檢測到資料檔案的內容資訊中包含有“加密”、“隱私”等內容時，例如，內容資訊包括“加密”，則將“加密”與第一預設條件進行匹配後，可以根據匹配的第一結果確定資料檔案為的機密等級為等級 1，如果內容資訊中不包含上述關鍵字組，則根據匹配的第一結果可以確定資料檔案的機密等級為等級 0；在另一實施例中，可以先確定資料檔案的檔案名稱，將檔案名稱與第二預設條件進行匹配，根據匹配的第二結果確定資料檔案的機密等級，例如，第二預設條件可以包括多個關鍵字組，例如，“機密”、“加密”等等，如果檢測到資料檔案的檔案名稱中包含有“機密”、“加密”等內容時，例如，檔案名稱包括“機密”，則將“機密”與第二預設條件進行匹配後，可以根據匹配的第二結果確定資料檔案為的機密等級為等級 1，如果檔案名稱中不包含上述關鍵字組，則根據匹配的第二結果可以確定資料檔案的機密等級為等級 0。

步驟 102，將資料檔案儲存到指定的虛擬儲存區域，執行步驟 103。

在一實施例中，虛擬儲存區域可以為終端設備的磁片上的用於儲存需要採取保密措施的資料檔案的特定的磁碟陣列部分，當使用者需要訪問儲存在虛擬儲存區域的資料檔案時，可以通過虛擬化技術啟動與終端設備的作業系統

相隔離（可包括儲存隔離、記憶體隔離等）的虛擬應用程式，通過虛擬應用程式訪問儲存在虛擬儲存區域的資料檔案，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密。

在另一實施例中，虛擬儲存區域可以為雲端伺服器的磁片上的用於儲存需要採取保密措施的資料檔案的特定的磁碟陣列部分，當使用者的終端設備不能夠儲存資料檔案或者不能夠對資料檔案採取保密措施時，可以通過虛擬化技術啟動與終端設備的作業系統相隔離（可包括儲存隔離、記憶體隔離等）的虛擬應用程式，通過虛擬應用程式訪問儲存在雲端伺服器上的虛擬儲存區域的資料檔案，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在雲端伺服器的虛擬環境中，避免資料檔案被洩密。

步驟 103，在資料檔案的原始儲存位置產生存根檔，存根檔用於記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，流程結束。

在一實施例中，存根檔所記錄的內容包括資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，在一實施例中，在用戶點擊到存根檔時，可以先確定用戶是否具有查閱許可權，只有在確保用戶具有查閱許可權時，資料檔案在虛擬儲存區域的儲存位置才能被獲知，進而從虛擬儲存區域的儲存位置查閱資料檔案；如果用戶不具有查閱許可權，則可以拒絕用戶的查閱操作。

步驟 104，將資料檔案作為普通檔供使用者使用，流程結束。

在一實施例中，對普通檔的讀取可以參見現有技術的描述，本公開不再詳述。

由上述描述可知，本發明實施例在確定資料檔案為機密檔時，將資料檔案儲存到指定的虛擬儲存區域，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密；通過在資料檔案的原始儲存位置產生存根檔，由於存根檔只記錄記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，並未攜帶資料檔案本身的任何資料，因此使用者對存根檔的一切操作不會對資料檔案有任何影響。

圖 2 示出了根據本發明的又一示例性實施例的資料檔案的保護方法的流程示意圖，如圖 2 所示，包括如下步驟：

步驟 201，在監聽到使用者需要將資料檔案共用給使用者指定的被共用使用者的第一指令時，確定被共用使用者的使用者資訊。

在一實施例中，用戶可以將資料檔案共用給其它用戶時，可以通過終端設備的用戶端應用程式或者存根檔的共用按鍵，啟動將存根檔共用給指定的被共用用戶。在一實施例中，使用者資訊可包括被共用使用者在用戶端應用程式的帳號，也可以包括被共用用戶能夠接收到該資料檔案的電子郵箱，也即，本申請對使用者資訊所包含的能夠接

收到資料檔案的位址不做限制，只要能夠使被共用用戶接收到該資料檔案即可。

步驟 202，根據使用者資訊確定被共用使用者是否有共用許可權，在確定被共用用戶具有共用許可權時，執行步驟 203，如果不具有共用許可權，提示無法共用。

步驟 203，將資料檔案上傳到雲端伺服器進行儲存。

在一實施例中，用戶可以將資料檔案上傳到雲端伺服器上進行備份儲存，可以通過終端設備的用戶端應用程式或者存根檔的上傳按鍵，將存根檔上傳到雲端伺服器，在一實施例中，用戶端應用程式可以為安裝在終端設備上的控制管理軟體。

步驟 204，根據使用者資訊向被共用使用者發送用於指示被共用使用者接收資料檔案的第二指令，在被共用使用者通過其終端設備確認接收資料檔案後，在被共用用戶的終端設備上產生資料檔案的存根檔，被共用使用者的終端設備根據存根檔從雲端伺服器的虛擬儲存區域獲取到資料檔案。

本實施例中，在需要對資料檔案進行共用時，根據使用者資訊向被共用使用者發送用於指示被共用使用者接收資料檔案的第二指令，在被共用使用者通過其終端設備確認接收資料檔案後，在被共用用戶的終端設備上產生資料檔案的存根檔，因此實現了通過存根檔的虛擬分享實現了對需要保密的資料檔案的共用，由於未將真實的資料檔案發送給被共用用戶，而存根檔只儲存資料檔案在虛擬儲存

區域的儲存位置，並未攜帶資料檔案本身的任何資料資訊，因此被共用使用者對存根檔的操作不會對資料檔案有任何影響，從而確保資料檔案在共用過程中不會被洩密。

圖 3 示出了根據本發明的一示例性實施例的讀取資料檔案的方法的流程示意圖；如圖 3 所示，包括如下步驟：

步驟 301，在監聽到用戶關於存根文件的點擊事件時，根據存根檔所記錄的查閱許可權確定使用者是否有訪問資料檔案的許可權，如果用戶有訪問資料檔案的許可權，執行步驟 302，如果使用者沒有訪問資料檔案的許可權，提示使用者沒有存取權限，流程結束。

在一實施例中，可以通過安裝在終端設備上的用戶端應用程式來監聽使用者關於存根檔的點擊事件，該用戶端應用程式需要具有登錄許可權的使用者登錄，在一實施例中，點擊事件可以為對存根檔的按兩下打開事件，也可以為通過觸發功能表後的打開事件。在一實施例中，用戶端應用程式可以記錄存根檔，從而能夠確定被點擊的檔是存根檔還是普通的資料檔案。

步驟 302，啟動資料檔案對應的虛擬應用程式，執行步驟 303。

步驟 303，在虛擬儲存區域的儲存位置通過虛擬應用程式訪問資料檔案，流程結束。

在步驟 302 和步驟 303 中，在一實施例中，虛擬應用程式為安裝在終端設備上的控制管理軟體虛擬化後的應用程式，可以與終端設備的作業系統隔離，在一實施例中，

虛擬應用程式與作業系統的隔離既可以包括與作業系統的儲存隔離，也可以包括與作業系統的記憶體隔離等，從而可以確保用戶任何對資料檔案的操作都隔離在虛擬應用程式所確定的虛擬環境中，避免非法使用者通過在虛擬應用程式的外部獲取到虛擬應用程式中的任何資料資源。在一實施例中，使用者通過虛擬應用程式對資料檔案的訪問可以包括正常閱讀、編輯、使用剪切板等。

本實施例中，在確定用戶具有訪問資料檔案的許可權後，在虛擬儲存區域的儲存位置通過虛擬應用程式訪問資料檔案，從而可以確保用戶任何對資料檔案的操作都隔離在虛擬應用程式所確定的虛擬環境中，避免非法使用者通過在虛擬應用程式的外部獲取到虛擬應用程式中的任何資料資源。

圖 4 示出了根據本發明的又一示例性實施例的讀取資料檔案的方法的流程示意圖；本實施例中，存根檔儲存在終端設備上，資料檔案儲存在雲端伺服器的虛擬儲存區域，以終端設備如何通過存根檔從雲端伺服器獲取到資料檔案進行示例性說明，如圖 4 所示，包括如下步驟：

步驟 401，終端設備在檢測到用戶點擊存根文件並打開存根檔後，根據存根檔所記錄的資訊啟動遠端桌面協定（Remote Desktop Protocol，簡稱為 RDP）元件，通過 RDP 元件連接到雲端伺服器。

步驟 402，終端設備通過 RDP 元件向雲端伺服器傳輸存根檔所記錄的資訊。

在一實施例中，存根檔所記錄的資料資訊均已通過用戶端應用程式加密，加密後的資料資訊記錄了存根檔對應的資料檔案、查看該資料檔案的用戶許可權、資料檔案分享的流轉過程、打開使用該資料檔案的相關歷史記錄。

步驟 403，雲端伺服器對所傳輸的資訊驗證後，雲端伺服器啟動終端設備上的遠端虛擬化程式，根據存根檔所記錄的虛擬儲存位置打開儲存在雲端伺服器上的資料檔案。

在一實施例中，傳輸的資訊可以包括用戶端應用程式的使用者許可權、使用者需要認證的資訊、請求打開的資料檔案在雲端伺服器上的虛擬儲存路徑。

步驟 404，雲端伺服器將文檔編輯器映射到終端設備。

在一實施例中，雲端伺服器可以通過文檔編輯器（例如，word）建立一個新的可編輯檔，並將該可編輯檔的整個可視表單傳送到終端設備的本地，從而可以在終端設備上映射了一個遠端的文檔編輯器。

步驟 405，終端設備利用文檔編輯器對儲存在雲端伺服器上的資料檔案進行操作。

在一實施例中，對資料檔案的操作可以包括查看、編輯資料檔案的內容，以及拷貝資料檔案等等，本公開對資料檔案的具體操作不做限制。

在一個示例性場景中，在通過上述圖 2 所示實施例使被共用用戶接收到存根檔後，當被共用使用者需要根據存

根檔從雲端伺服器上獲取到該資料檔案時，可以通過本實施例從雲端伺服器的虛擬儲存區域獲取到資料檔案。在另一示例性場景中，如果終端設備的磁片由於儲存空間的限制或者終端設備的磁片未設置有虛擬儲存區域，從而將資料檔案儲存到了雲端伺服器的虛擬儲存區域，在此情形下，當終端設備的使用者需要根據存根檔從遠端伺服器上獲取到該資料檔案時，同樣可以通過本實施例從雲端伺服器的虛擬儲存區域獲取到資料檔案。在再一示例性場景中，當使用者需要通過不同的終端設備從雲端伺服器操作資料檔案時，同樣也可以採用上述方法實現遠端讀取資料檔案，例如，用戶在終端設備 A 上產生了資料檔案的存根檔，並在終端設備 A 的虛擬儲存區域儲存了資料檔案，當使用者將存根檔從終端設備 A 發送給終端設備 B 時，並且終端設備 A 將資料檔案上傳給了雲端伺服器後，如果使用者需要從終端設備 B 讀取該資料檔案，則可以通過本實施例從雲端伺服器操作資料檔案。

通過上述實施例，由於現有技術中的 Citrix XenApp 等應用虛擬化實現成本較高，本申請通過採用基於 RDP 協議的應用虛擬化方案，可以使用任意 Windows 作業系統，利用遠端桌面 RDP 協定、RDP 控制元件、消息鉤子、表單剪裁技術實現遠端應用虛擬化技術，避免對作業系統具有依賴性，從而使雲端伺服器可以採用任意的 Windows 作業系統，因此具有較高的靈活性。

在上述圖 1-圖 4 所示實施例的基礎上，在資料檔案被

用戶操作時，還可以通過安裝在終端設備上的用戶端應用程式監控使用者對資料檔案所進行的操作；在一實施例中，用戶對資料檔案的操作既可以為用戶在終端設備上對資料檔案所進行的操作，還可以為用戶通過雲端伺服器映射到終端設備上的文檔編輯器對資料檔案所進行的操作，從而可以對用戶關於資料檔案的打開、操作、流轉等所有的針對資料檔案的行為都可以有效的監控和管理起來。

對應於上述的資料檔案的保護方法，本申請還提出了圖 5 所示的根據本申請的一示例性實施例的終端設備的示意結構圖。請參考圖 5，在硬體層面，該終端設備包括處理器、內部匯流排、網路介面、記憶體以及非易失性記憶體，當然還可能包括其他業務所需要的硬體。處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上形成資料檔案的保護裝置。當然，除了軟體實現方式之外，本申請並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

對應於上述的讀取資料檔案的方法，本申請還提出了圖 6 所示的根據本申請的另一示例性實施例的終端設備的示意結構圖。請參考圖 6，在硬體層面，該終端設備包括處理器、內部匯流排、網路介面、記憶體以及非易失性記憶體，當然還可能包括其他業務所需要的硬體。處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運

行，在邏輯層面上形成讀取資料檔案的裝置。當然，除了軟體實現方式之外，本申請並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

圖 7 為根據本發明的一示例性實施例的資料檔案的保護裝置的結構示意圖；如圖 7 所示，在軟體實施方式中，該資料檔案的保護裝置可以包括：第一確定模組 71、儲存模組 72、存根產生模組 73。其中：

第一確定模組 71，用於在檢測到終端設備上有資料檔案產生時，確定資料檔案的機密等級以及資料檔案的原始儲存位置；

儲存模組 72，用於如果第一確定模組 71 確定的機密等級表示資料檔案為機密檔，將資料檔案儲存到指定的虛擬儲存區域；

存根產生模組 73，用於在第一確定模組 71 確定的原始儲存位置產生存根檔，存根檔用於記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置。

圖 8 示出了根據本發明的又一示例性實施例的資料檔案的保護裝置的結構示意圖，在上述圖 7 所示實施例的基礎上，第一確定模組 71 可包括：

第一確定單元 711，用於確定資料檔案的內容資訊；

第一匹配單元 712，用於將第一確定單元 711 確定的內容資訊與第一預設條件進行匹配，根據匹配的第一結果

確定資料檔案的機密等級；和/或，

第二確定單元 713，用於確定資料檔案的檔案名稱；

第二匹配單元 714，用於將第二確定單元 713 確定的檔案名稱與第二預設條件進行匹配，根據匹配的第二結果確定資料檔案的機密等級。

在一實施例中，裝置還可包括：

第二確定模組 74，用於在監聽到使用者需要將儲存模組 72 儲存的資料檔案共用給使用者指定的被共用使用者器的第一指令時，確定被共用使用者的使用者資訊；

發送模組 75，用於根據第二確定模組 74 確定的使用者資訊向被共用使用者發送用於指示被共用使用者接收資料檔案的第二指令，在被共用使用者通過相應的終端設備確認接收資料檔案後，在被共用用戶的終端設備上產生資料檔案的存根檔。

在一實施例中，裝置還可包括：

第三確定模組 76，用根據第二確定模組 74 確定的使用者資訊確定被共用使用者是否有共用許可權；

上傳模組 77，用於在第三確定模組 76 確定被共用使用者具有共用許可權時，將資料檔案上傳到雲端伺服器進行儲存，以使被共用使用者根據存根檔從雲端伺服器的虛擬儲存區域獲取到資料檔案。

在一實施例中，裝置還可包括：

監控模組 78，在儲存模組 72 所儲存的資料檔案被使用者操作時，通過安裝在終端設備上的用戶端應用程式監

控使用者對資料檔案所進行的操作。

圖 9 示出了根據本發明的一示例性實施例的讀取資料檔案的裝置的結構示意圖；在軟體實施方式中，如圖 9 所示，讀取資料檔案的裝置可包括：第四確定模組 91、啟動模組 92、訪問模組 93；其中：

第四確定模組 91，用於在監聽到用戶關於存根根文件的點擊事件時，根據存根檔所記錄的查閱許可權確定使用者是否有訪問資料檔案的許可權；

啟動模組 92，用於如果第四確定模組 91 確定使用者有訪問資料檔案的許可權，啟動資料檔案對應的虛擬應用程式；

訪問模組 93，用於通過啟動模組 92 啟動的虛擬應用程式訪問儲存在存根檔所記錄的虛擬儲存區域的儲存位置的資料檔案。

圖 10 示出了根據本發明的又一示例性實施例的讀取資料檔案的裝置的結構示意圖；在上述圖 9 所示實施例的基礎上，訪問模組 93 可包括：

網路連接單元 931，用於根據存根檔所記錄的資訊通過遠端桌面協定元件連接到雲端伺服器；

傳輸單元 932，用於通過遠端桌面協定元件向雲端伺服器傳輸存根檔所記錄的資訊，以供雲端伺服器對儲存檔所記錄的資訊驗證通過後啟動終端設備上的遠端虛擬化程式，根據存根檔所記錄的虛擬儲存位置將儲存在雲端伺服器上的資料檔案的文檔編輯器映射到終端設備上；

操作單元 933，用於通過文檔編輯器對儲存在雲端伺服器上的資料檔案進行操作。

上述實施例可見，本申請在確定資料檔案為機密檔時，將資料檔案儲存到指定的虛擬儲存區域，從而可以使任何對儲存在虛擬儲存區域的資料檔案的操作都被隔離在虛擬環境中，避免資料檔案被洩密；通過在資料檔案的原始儲存位置產生存根檔，由於存根檔只記錄記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置，並未攜帶資料檔案本身的任何資料，因此使用者對存根檔的一切操作不會對資料檔案有任何影響。

本領域技術人員在考慮說明書及實踐這裡公開的發明後，將容易想到本申請的其它實施方案。本申請旨在涵蓋本申請的任何變型、用途或者適應性變化，這些變型、用途或者適應性變化遵循本申請的一般性原理並包括本申請未公開的本技術領域中的公知常識或慣用技術手段。說明書和實施例僅被視為示例性的，本申請的真正範圍和精神由下面的申請專利範圍第指出。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另

外的相同要素。

以上所述僅為本申請的較佳實施例而已，並不用以限制本申請，凡在本申請的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本申請保護的範圍之內。

【符號說明】

71：第一確定模組

711：第一確定單元

712：第一匹配單元

713：第二確定單元

714：第二匹配單元

72：存儲模組

73：存根產生模組

74：第二確定模組

75：發送模組

76：第三確定模組

77：上傳模組

91：第四確定模組

92：啟動模組

93：訪問模組

931：網路連接單元

932：傳輸單元

933：操作單元

101、102、103、104、201、202、203、204、301、302、303：步驟

申請專利範圍

1.一種資料檔案的保護方法，應用在終端設備上，其特徵在於，所述方法包括：

在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級；

如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；

在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

2.根據申請專利範圍第 1 項所述的方法，其中，所述確定所述資料檔案的機密等級，包括：

確定所述資料檔案的內容資訊；

將所述內容資訊與第一預設條件進行匹配，根據匹配的第一結果確定所述資料檔案的機密等級；和/或

確定所述資料檔案的檔案名稱；

將所述檔案名稱與第二預設條件進行匹配，根據匹配的第二結果確定所述資料檔案的機密等級。

3.根據申請專利範圍第 1 項所述的方法，其中，所述方法還包括：

在監聽到所述使用者需要將所述資料檔案共用給所述用戶指定的被共用使用者的第一指令時，確定所述被共用使用者的使用者資訊；

根據所述使用者資訊向所述被共用用戶相應的終端設

備發送用於指示所述被共用用戶接收所述資料檔案的第二指令，在所述被共用用戶通過相應的終端設備確認接收所述資料檔案後，在所述被共用用戶的終端設備上產生資料檔案的存根檔。

4.根據申請專利範圍第 3 項所述的方法，其中，所述方法還包括：

根據所述使用者資訊確定所述被共用用戶是否有共用許可權；

在確定所述被共用用戶具有所述共用許可權時，將所述資料檔案上傳到雲端伺服器，並儲存到所述雲端伺服器的虛擬儲存區域，以使所述被共用使用者根據所述存根檔從所述雲端伺服器的虛擬儲存區域獲取到所述資料檔案。

5.根據申請專利範圍第 1-4 項之任一項所述的方法，其中，所述方法還包括：

在所述資料檔案被所述用戶操作時，通過安裝在所述終端設備上的用戶端應用程式監控所述使用者對所述資料檔案所進行的操作。

6.一種讀取資料檔案的方法，應用在終端設備上，其特徵在於，所述方法包括：

在監聽到用戶關於存根文件的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

如果所述用戶有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

通過所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案。

7.根據申請專利範圍第 6 項所述的方法，其中，如果所記錄的虛擬儲存區域在雲端伺服器上，所述通過所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案，包括：

通過遠端桌面協定元件連接到存根檔所記錄的虛擬儲存區域的儲存位置對應的雲端伺服器；

通過所述遠端桌面協定元件向所述雲端伺服器傳輸存根檔所記錄的存取權限，以供所述雲端伺服器對所述儲存檔所記錄的存取權限驗證通過後啟動所述終端設備上的遠端虛擬化程式，根據所述存根檔所記錄的虛擬儲存位置將儲存在所述雲端伺服器上的資料檔案的文檔編輯器映射到所述終端設備上；

通過所述文檔編輯器對儲存在所述雲端伺服器上的資料檔案進行操作。

8.一種資料檔案的保護裝置，應用在終端設備上，其特徵在於，所述裝置包括：

第一確定模組，用於在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級以及所述資料檔案的原始儲存位置；

儲存模組，用於如果所述第一確定模組確定的所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到所述終端設備上的虛擬儲存區域；

存根產生模組，用於在所述第一確定模組確定的所述原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

9.根據申請專利範圍第 8 項所述的裝置，其中，所述第一確定模組包括：

第一確定單元，用於確定所述資料檔案的內容資訊；

第一匹配單元，用於將所述第一確定單元確定的所述內容資訊與第一預設條件進行匹配，根據匹配的第一結果確定所述資料檔案的機密等級；和/或

第二確定單元，用於確定所述資料檔案的檔案名稱；

第二匹配單元，用於將所述第二確定單元確定的所述檔案名稱與第二預設條件進行匹配，根據匹配的第二結果確定所述資料檔案的機密等級。

10.根據申請專利範圍第 8 項所述的裝置，其中，所述裝置還包括：

第二確定模組，用於在監聽到所述使用者需要將所述儲存模組儲存的所述資料檔案共用給所述用戶指定的被共用使用者器的第一指令時，確定所述被共用使用者的使用者資訊；

發送模組，用於根據所述第二確定模組確定的所述使用者資訊向所述被共用用戶相應的終端設備發送用於指示所述被共用用戶接收所述資料檔案的第二指令，在所述被共用用戶通過相應的終端設備確認接收所述資料檔案後，

在所述被共用用戶的終端設備上產生資料檔案的存根檔。

11.根據申請專利範圍第 10 項所述的裝置，其中，所述裝置還包括：

第三確定模組，用於根據所述第二確定模組確定的所述使用者資訊確定所述被共用用戶是否有共用許可權；

上傳模組，用於在所述第三確定模組確定所述被共用用戶具有所述共用許可權時，將資料檔案上傳到雲端伺服器進行儲存，以使所述被共用使用者根據所述存根檔從所述雲端伺服器的虛擬儲存區域獲取到所述資料檔案。

12.根據申請專利範圍第 8-11 項之任一項所述的裝置，其中，所述裝置還包括：

監控模組，用於在所述儲存模組儲存的所述資料檔案被所述用戶操作時，通過安裝在所述終端設備上的用戶端應用程式監控所述使用者對所述資料檔案所進行的操作。

13.一種讀取資料檔案的裝置，應用在終端設備上，其特徵在於，所述裝置包括：

第四確定模組，用於在監聽到用戶關於存根檔的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

啟動模組，用於如果所述第四確定模組確定所述使用者有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

訪問模組，用於通過所述啟動模組啟動的所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲

存位置的所述資料檔案。

14.根據申請專利範圍第 13 項所述的裝置，其中，所述訪問模組包括：

網路連接單元，用於根據存根檔所記錄的資訊通過遠端桌面協定元件連接到雲端伺服器；

傳輸單元，用於通過所述遠端桌面協定元件向雲端伺服器傳輸存根檔所記錄的資訊，以供所述雲端伺服器對所述儲存檔所記錄的資訊驗證通過後啟動所述終端設備上的遠端虛擬化程式，根據所述存根檔所記錄的虛擬儲存位置將儲存在所述雲端伺服器上的資料檔案的文檔編輯器映射到所述終端設備上；

操作單元，用於通過所述文檔編輯器對儲存在所述雲端伺服器上的資料檔案進行操作。

15.一種終端設備，其中，所述終端設備包括：

處理器；用於儲存所述處理器可執行指令的記憶體；

其中，所述處理器，用於在檢測到所述終端設備上有資料檔案產生時，確定所述資料檔案的機密等級；

如果所述機密等級表示所述資料檔案為機密檔，將所述資料檔案儲存到指定的虛擬儲存區域；

在所述資料檔案的原始儲存位置產生存根檔，所述存根檔用於記錄所述資料檔案的查閱許可權和所述資料檔案在所述虛擬儲存區域的儲存位置。

16.一種終端設備，　其特徵在於，所述終端設備包括：

處理器；以及用於儲存所述處理器可執行指令的記憶體；

其中，所述處理器，用於在監聽到用戶關於存根文件的點擊事件時，根據所述存根檔所記錄的查閱許可權確定所述用戶是否有訪問所述資料檔案的許可權；

如果所述用戶有訪問所述資料檔案的許可權，啟動所述資料檔案對應的虛擬應用程式；

通過所述虛擬應用程式訪問儲存在所述存根檔所記錄的虛擬儲存區域的儲存位置的所述資料檔案。

圖式

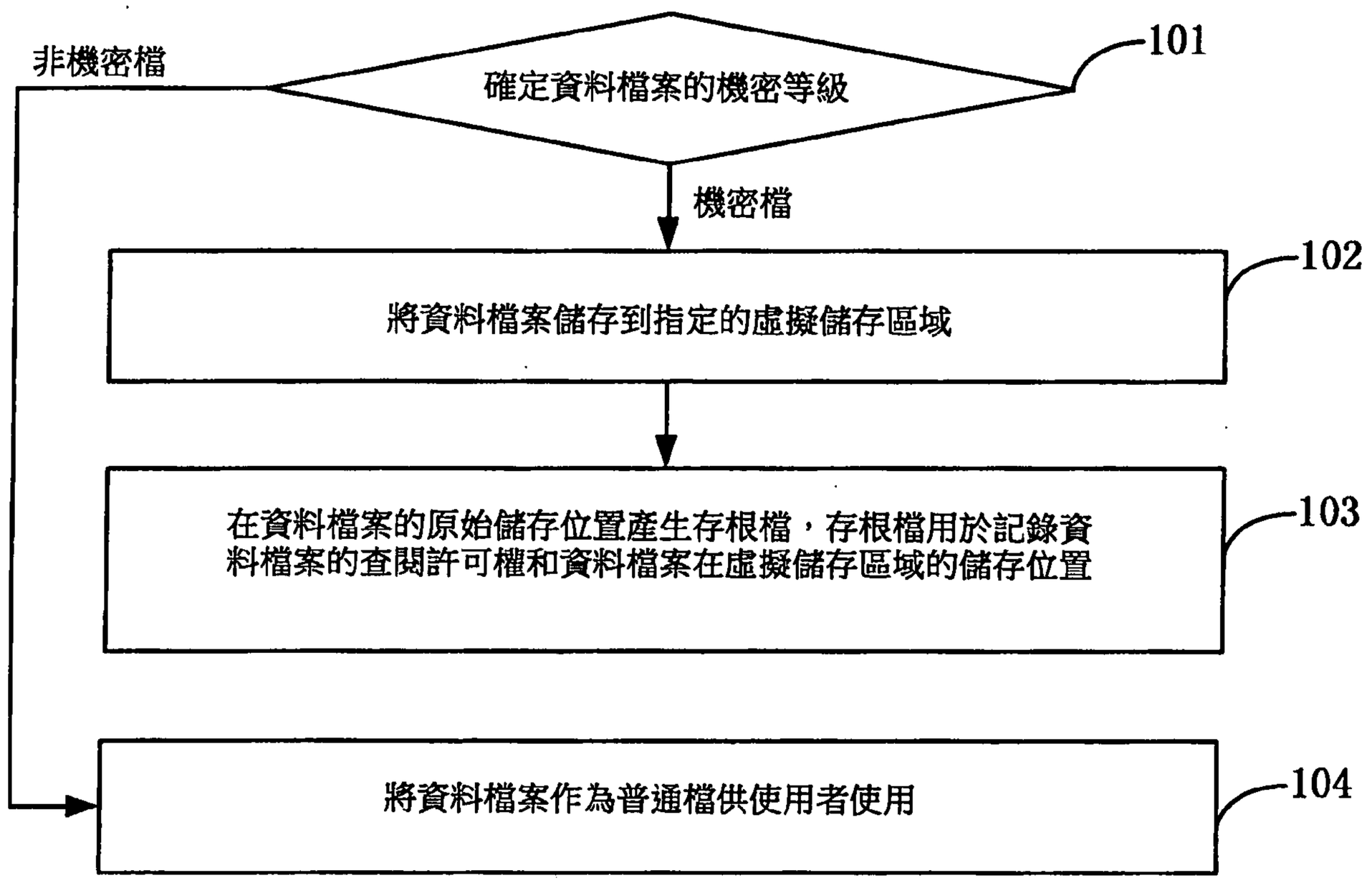
非機密檔
確定資料檔案的機密等級
101
機密檔
將資料檔案儲存到指定的虛擬儲存區域
102
在資料檔案的原始儲存位置產生存根檔，存根檔用於記錄資料檔案的查閱許可權和資料檔案在虛擬儲存區域的儲存位置
103
將資料檔案作為普通檔供使用者使用
104

圖 1

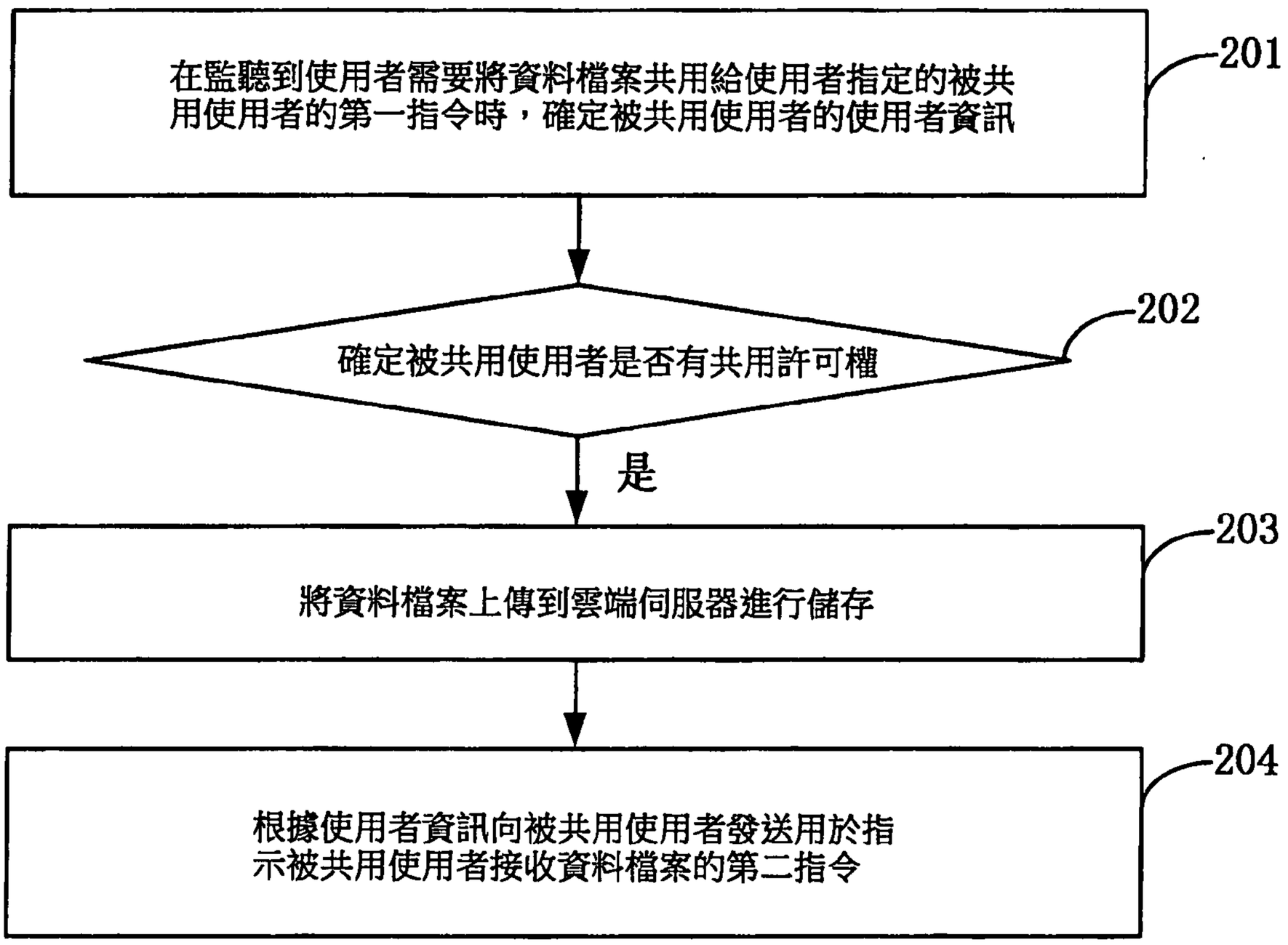
在監聽到使用者需要將資料檔案共用給使用者指定的被共用使用者的第一指令時，確定被共用使用者的使用者資訊
201
確定被共用使用者是否有共用許可權
202
是
將資料檔案上傳到雲端伺服器進行儲存
203
根據使用者資訊向被共用使用者發送用於指示被共用使用者接收資料檔案的第二指令
204

圖 2

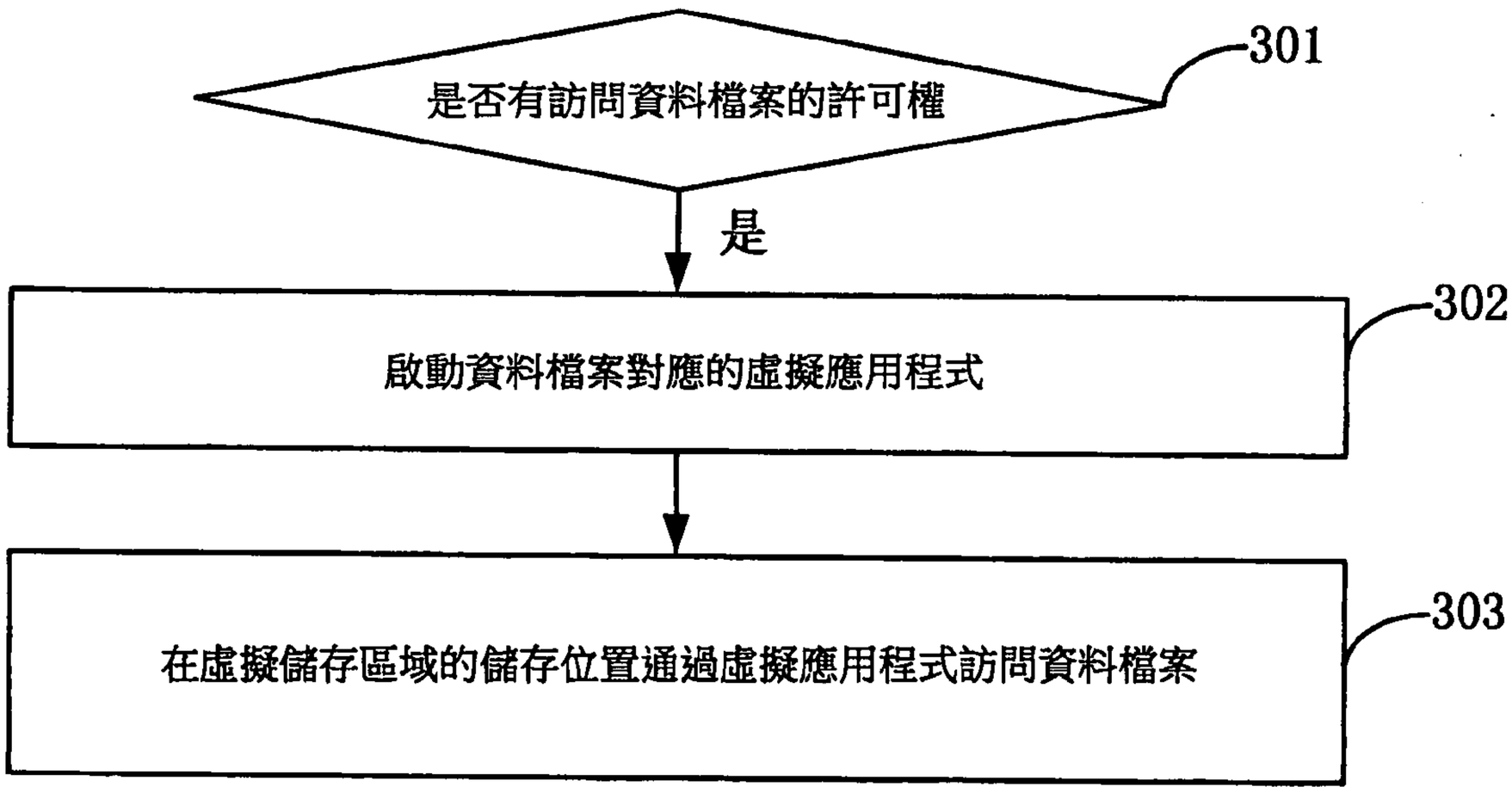
是否有訪問資料檔案的許可權
301
是
啟動資料檔案對應的虛擬應用程式
302
在虛擬儲存區域的儲存位置通過虛擬應用程式訪問資料檔案
303

圖 3

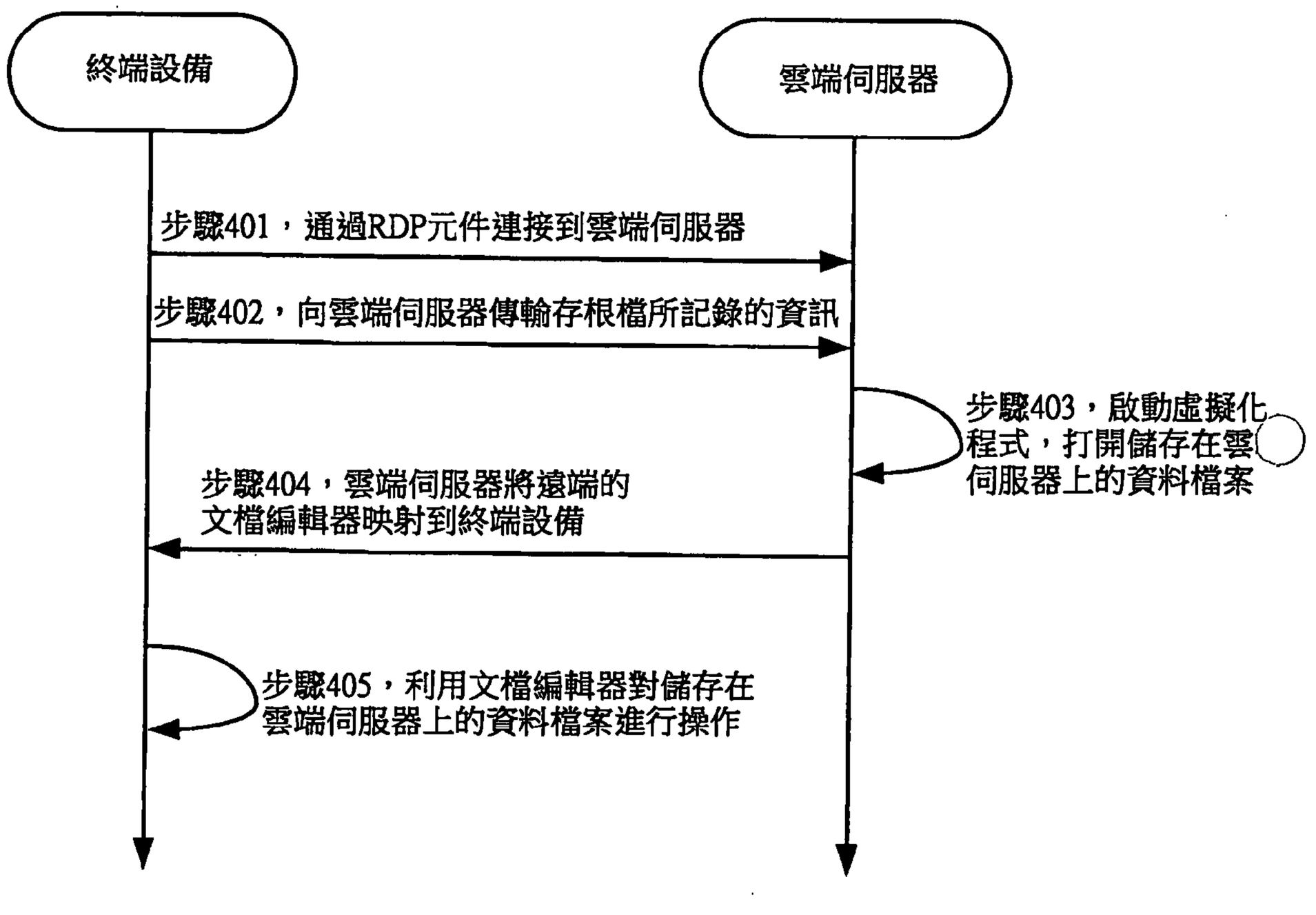
終端設備
雲端伺服器
步驟401，通過RDP元件連接到雲端伺服器
步驟402，向雲端伺服器傳輸存根檔所記錄的資訊
步驟403，啟動虛擬化程式，打開儲存在雲伺服器上的資料檔案
步驟404，雲端伺服器將遠端的文檔編輯器映射到終端設備
步驟405，利用文檔編輯器對儲存在雲端伺服器上的資料檔案進行操作

圖 4

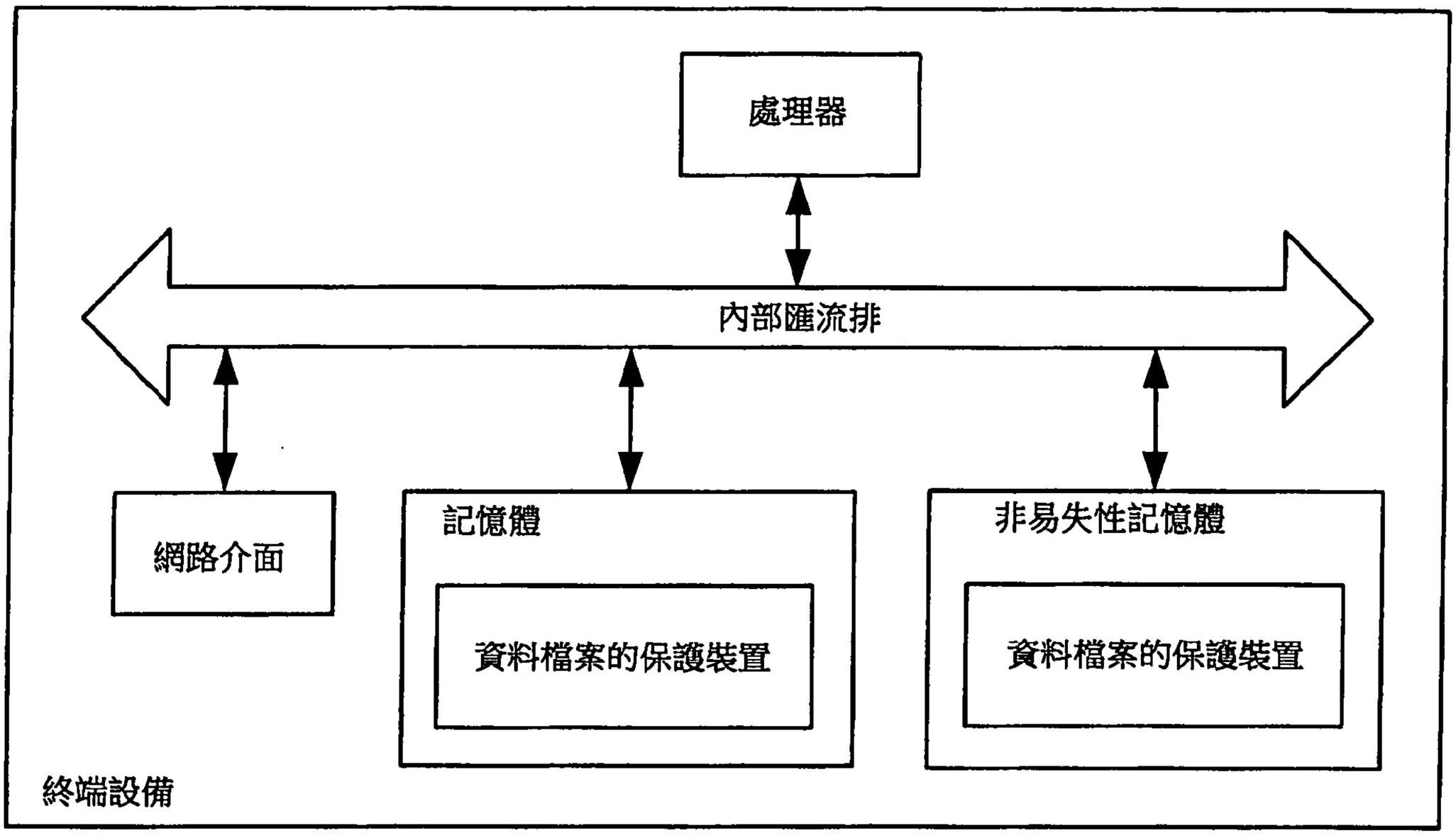
處理器
內部匯流排
網路介面
記憶體
資料檔案的保護裝置
非易失性記憶體
資料檔案的保護裝置
終端設備

圖 5

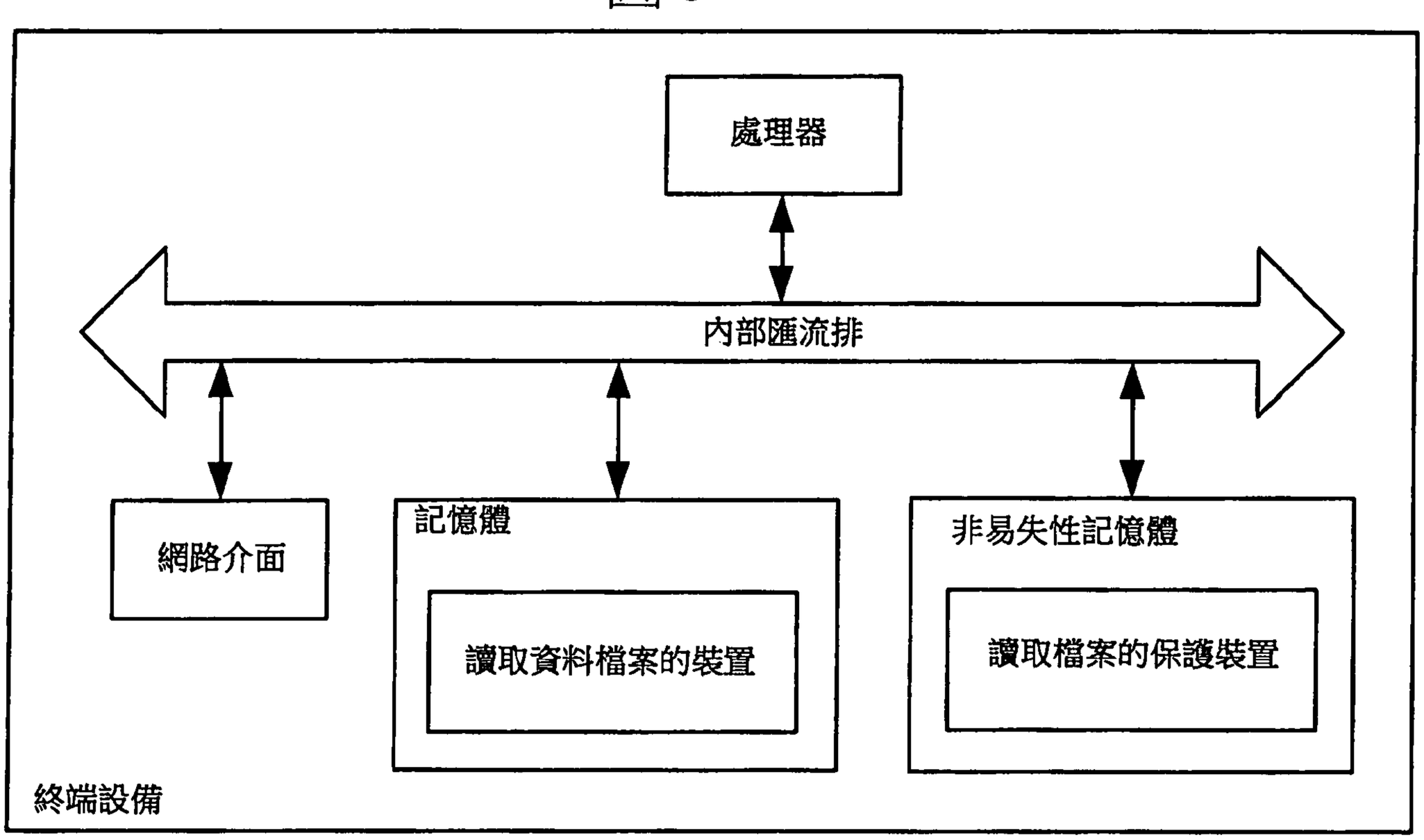
處理器
內部匯流排
網路介面
記憶體
讀取資料檔案的裝置
非易失性記憶體
讀取檔案的保護裝置
終端設備

圖 6

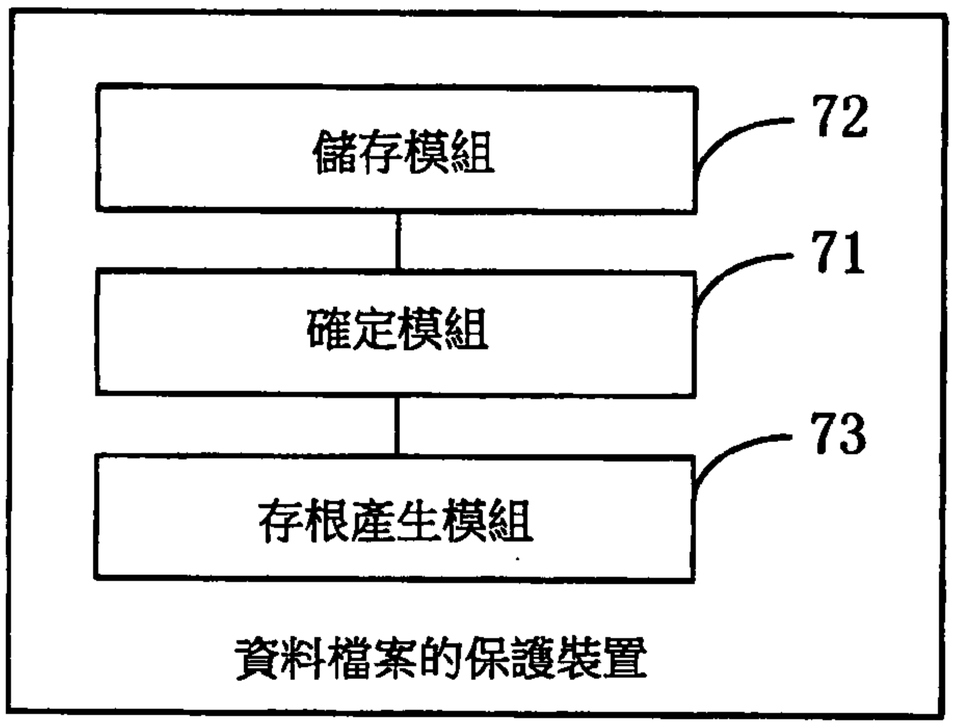
儲存模組
72
確定模組
71
存根產生模組
73
資料檔案的保護裝置

圖 7

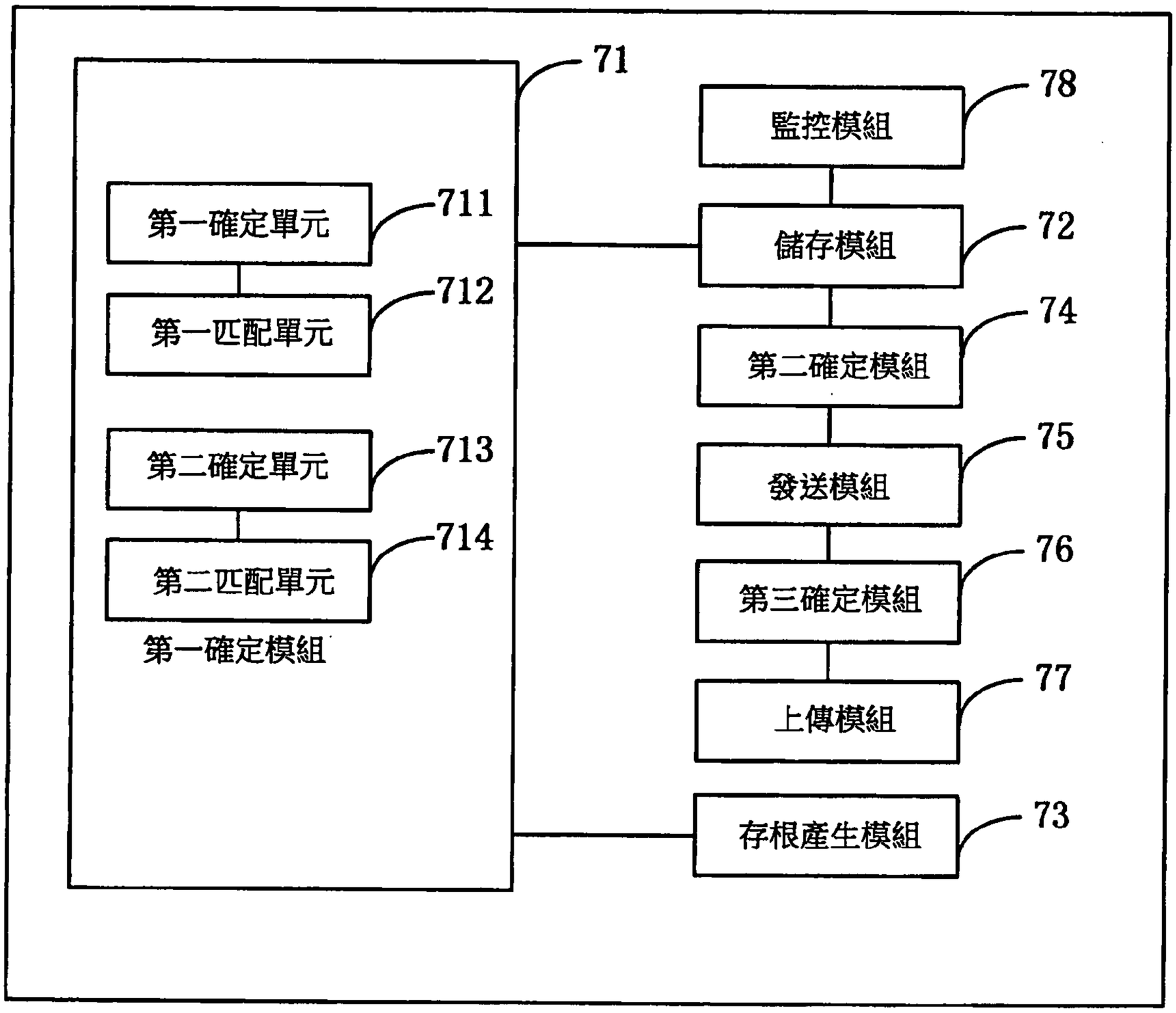
71
第一確定單元
711
第一匹配單元
712
第二確定單元
713
第二匹配單元
714
第一確定模組
78
監控模組
儲存模組
72
74
第二確定模組
75
發送模組
76
第三確定模組
77
上傳模組
存根產生模組
73

圖 8

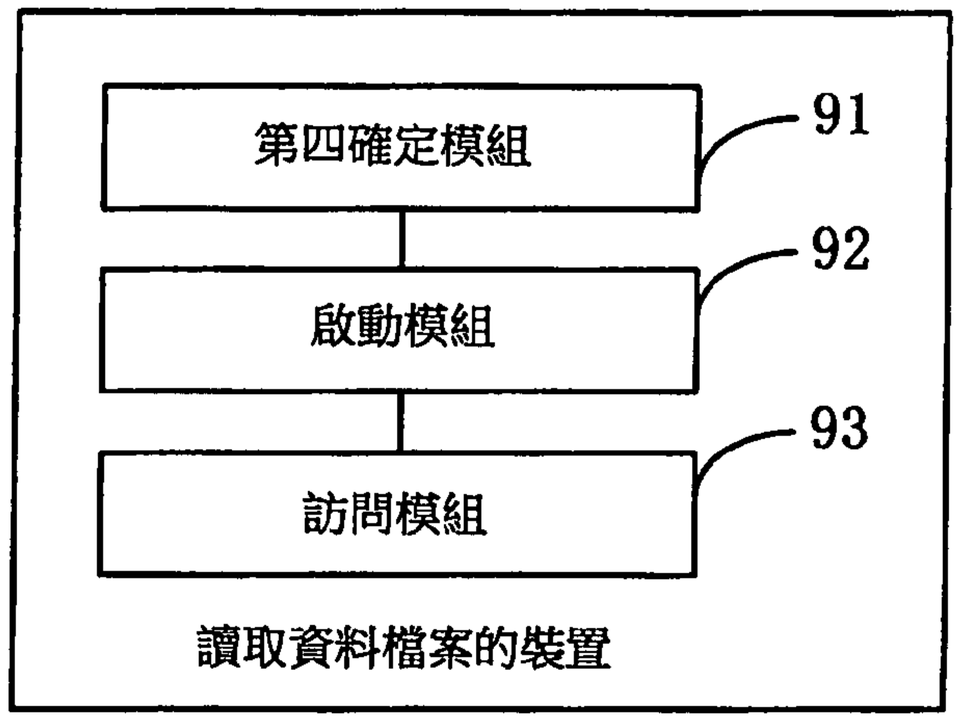
第四確定模組
91
啟動模組
92
訪問模組
93
讀取資料檔案的裝置

圖 9

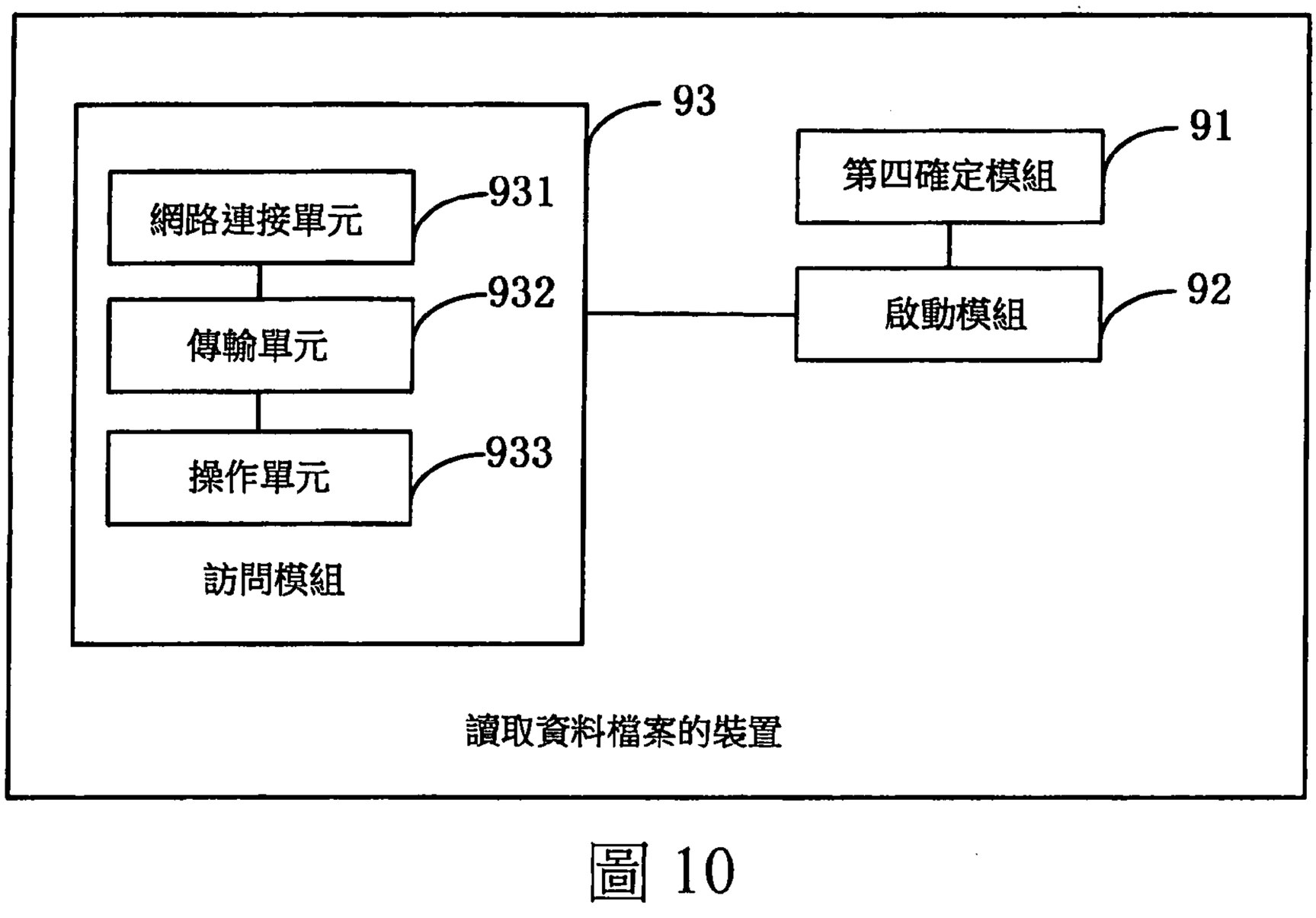
93
網路連接單元
931
傳輸單元
932
操作單元
933
訪問模組
第四確定模組
91
啟動模組
92
讀取資料檔案的裝置

圖 10