(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201301077 A1
(43)公開日： 中華民國 102 (2013) 年 01 月 01 日

(21)申請案號：100122980 (22)申請日： 中華民國 100 (2011) 年 06 月 30 日
(51)Int. Cl.： *G06F21/20 (2006.01)* *G06F21/24 (2006.01)*
(30)優先權：2011/06/23 中國大陸 201110171086.0
(71)申請人：鴻海精密工業股份有限公司 (中華民國) HON HAI PRECISION INDUSTRY CO., LTD. (TW)
新北市土城區自由街 2 號
(72)發明人：鍾明導 CHUNG, MING TAW (TW) ；賓煒靈 BIN, WEI-LING (CN) ；陳枝地 CHEN, CHIH TI (TW)
申請實體審查：無 申請專利範圍項數：10 項 圖式數：5 共 30 頁

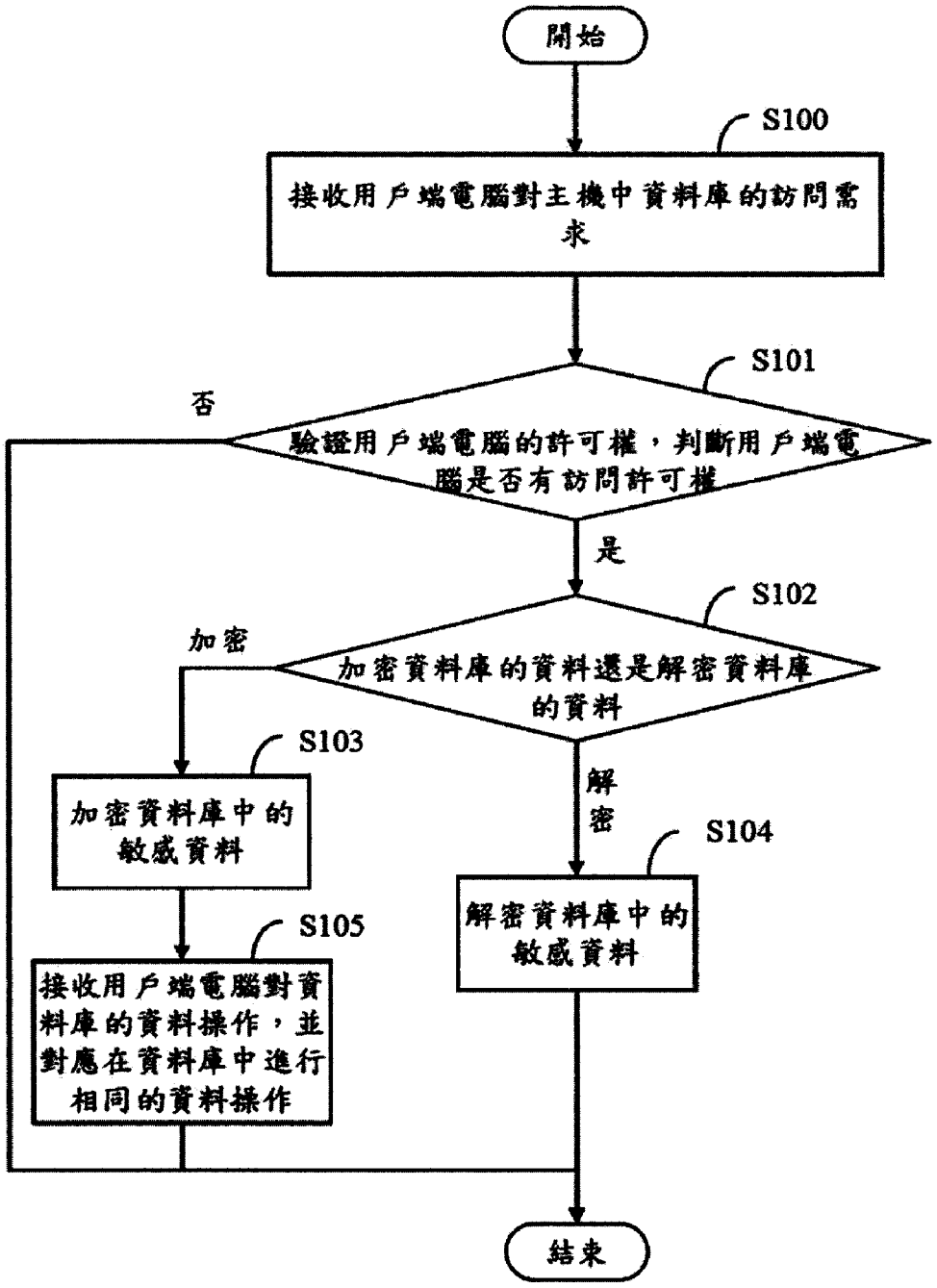
(54)名稱

資料庫資料管理方法及系統

DATABASE DATA MANAGEMENT METHOD AND SYSTEM

(57)摘要

一種資料庫資料管理方法及系統，該方法包括：接收用戶端電腦對主機中資料庫的訪問需求；驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，當用戶端電腦有訪問許可權時，則選擇用戶端電腦對主機的訪問需求，當用戶端電腦需要加密資料庫的資料時，則加密資料庫中的敏感資料，接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作；當用戶端電腦需要解密資料庫的資料時，則解密資料庫中的敏感資料。本發明可以對敏感資料進行保護，實現對資料庫資料安全的加密及解密過程。



S100：接收用戶端電腦對主機中資料庫的訪問需求

S101：驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權

S102：加密資料庫的資料還是解密資料庫的資料

S103：加密資料庫中的敏感資料

S104：解密資料庫中的敏感資料

S105：接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201301077 A1
(43)公開日： 中華民國 102 (2013) 年 01 月 01 日

(21)申請案號：100122980 (22)申請日： 中華民國 100 (2011) 年 06 月 30 日
(51)Int. Cl.： *G06F21/20 (2006.01)* *G06F21/24 (2006.01)*
(30)優先權：2011/06/23 中國大陸 201110171086.0
(71)申請人：鴻海精密工業股份有限公司 (中華民國) HON HAI PRECISION INDUSTRY CO., LTD. (TW)
新北市土城區自由街 2 號
(72)發明人：鍾明導 CHUNG, MING TAW (TW) ；賓煒靈 BIN, WEI-LING (CN) ；陳枝地 CHEN, CHIH TI (TW)
申請實體審查：無 申請專利範圍項數：10 項 圖式數：5 共 30 頁

(54)名稱

資料庫資料管理方法及系統

DATABASE DATA MANAGEMENT METHOD AND SYSTEM

(57)摘要

一種資料庫資料管理方法及系統，該方法包括：接收用戶端電腦對主機中資料庫的訪問需求；驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，當用戶端電腦有訪問許可權時，則選擇用戶端電腦對主機的訪問需求，當用戶端電腦需要加密資料庫的資料時，則加密資料庫中的敏感資料，接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作；當用戶端電腦需要解密資料庫的資料時，則解密資料庫中的敏感資料。本發明可以對敏感資料進行保護，實現對資料庫資料安全的加密及解密過程。

201301077

智專收字第1002038887-0

DTD版本：1.0.2

專利案號：100122980

日期：100年06月30日

發明專利說明書

※申請案號：100122980 ※IPC分類：G06F 21/20 (2006.01)

※申請日：100.6.30 G06F 21/24 (2006.01)

一、發明名稱：

資料庫資料管理方法及系統

Database data management method and system

二、中文發明摘要：

一種資料庫資料管理方法及系統，該方法包括：接收用戶端電腦對主機中資料庫的訪問需求；驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，當用戶端電腦有訪問許可權時，則選擇用戶端電腦對主機的訪問需求，當用戶端電腦需要加密資料庫的資料時，則加密資料庫中的敏感資料，接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作；當用戶端電腦需要解密資料庫的資料時，則解密資料庫中的敏感資料。本發明可以對敏感資料進行保護，實現對資料庫資料安全的加密及解密過程。

三、英文發明摘要：

The present invention provides a database data management method and system. The method includes: receiving a client computer's needs to access the database in the host; verifying the client computer's permission, to determine whether the client computer has access permission, when the client computer has access license, selecting the client computer's needs, if the client computer want to encrypt the data in the database, then encrypting the sensitive database information, receiving the client computer's operation on the database and having the same data manipulation corresponding to the database; if the client computer

need to decrypt the data in the database, then decrypting the sensitive database information. The present invention can protect sensitive data, to achieve data security for database encryption and decryption process.

四、指定代表圖：

(一)本案指定代表圖為：圖 (3)

(二)本代表圖之元件符號簡單說明：

接收用戶端電腦對主機中資料庫的訪問需求 S100

驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權 S101

加密資料庫的資料還是解密資料庫的資料 S102

加密資料庫中的敏感資料 S103

解密資料庫中的敏感資料 S104

接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作 S105

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

[0001] 本發明涉及一種資料庫資料管理方法及系統。

【先前技術】

[0002] 目前電腦系統的維護主要有以下方式：(1)將其交給本公司內部的專業IT部門維護，(2)將其外包給公司以外的機構維護，(3)請專業的DBA進行維護，DBA全稱為Data-Base Administrator，指資料庫管理員。

[0003] 這三種維護方式都會帶來以下的缺點：

[0004] (1)對於一些存儲敏感資料的電腦系統，由於需要IT人員的維護，一些敏感資料容易被IT人員竊取並進行非法交易，這樣不僅洩漏了個人的隱私，同時也對公司的資訊安全帶來了嚴重的潛在威脅。

[0005] (2)資料庫的維護需要極高的系統許可權和資料庫許可權，這樣DBA就可以對敏感資料進行查看、修改甚至是刪除的動作，這樣對資料庫進行維護，IT人員可能會洩密資料，從而造成公司的財產損失。

【發明內容】

[0006] 鑒於以上內容，有必要提供一種資料庫資料管理方法及系統，可以對敏感資料進行保護，實現對資料庫資料安全的加密及解密過程。

[0007] 所述資料庫資料管理方法，應用於資料庫資料的管理，該方法包括以下步驟：接收步驟：接收用戶端電腦對主機中資料庫的訪問需求，所述用戶端電腦通過網路連接

至主機；驗證步驟：驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，當用戶端電腦有訪問許可權時，則執行選擇步驟，否則，直接結束流程，驗證過程中對用戶端電腦的電腦名稱、IP位址及用戶端密鑰進行驗證；選擇步驟：選擇用戶端電腦對主機的訪問需求，當用戶端電腦需要加密資料庫的資料時，則執行加密步驟，當用戶端電腦需要解密資料庫的資料時，則執行解密步驟；加密步驟：加密資料庫中的敏感資料；處理步驟：接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作，所述對資料庫的資料操作，為對資料庫中的資料進行增加、刪除、修改、查詢的操作；解密步驟：解密資料庫中的敏感資料。

[0008] 所述資料庫資料管理系統，運行於主機中，該系統包括：接收模組，用於接收用戶端電腦對主機中資料庫的訪問需求，所述用戶端電腦通過網路連接至主機；驗證模組，用於驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，驗證過程中對用戶端電腦的電腦名稱、IP位址及用戶端密鑰進行驗證；選擇模組，用於當用戶端電腦有訪問許可權時，選擇用戶端電腦對主機的訪問需求，判斷用戶端電腦是需要加密資料庫的資料，還是需要解密資料庫的資料；加密模組，用於當用戶端電腦需要加密資料庫的資料時，加密資料庫中的敏感資料；處理模組，用於接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作，所述對資料庫的資料操作，為對資料庫中的資料進行增加、刪除、

修改、查詢的操作；解密模組，用於當用戶端電腦需要解密資料庫的資料時，解密資料庫中的敏感資料。

[0009] 相較於習知技術，本發明所述之資料庫資料管理方法及系統，使具有維護許可權的工作人員也無法看到真實資料，可以對敏感資料進行保護，從而實現對資料庫資料安全的加密及解密過程。

【實施方式】

[0010] 如圖1所示，係為本發明資料庫資料管理系統較佳實施例之架構圖。

[0011] 資料庫資料管理系統10運行於主機1中，該主機1中還包括資料庫11，所述主機1通過網路2與用戶端電腦3連接。所述用戶端電腦3可有多個，圖1中僅畫出一個。所述網路2可以是企業內部網（Intranet）或乙太網（Ethernet），也可以是網際網路（Internet）或其他類型的通訊網路。

[0012] 如圖2所示，係為本發明資料庫資料管理系統較佳實施例之功能模組圖。

[0013] 所述資料庫資料管理系統10包括接收模組100、驗證模組101、選擇模組102、加密模組103、解密模組104、處理模組105。

[0014] 所述接收模組100用於接收用戶端電腦3對主機1中資料庫11的訪問需求。

[0015] 所述驗證模組101用於驗證用戶端電腦3的許可權，判斷用戶端電腦3是否有訪問許可權。驗證過程中對用戶端電

腦3的電腦名稱、IP位址及用戶端密鑰進行驗證，只有當所述三者完全正確時，才能證明用戶端電腦3是安全管理員添加了用戶信任憑證的用戶，才可以對資料庫11中的某些敏感資料進行加密及解密操作。所述用戶端密鑰是加密及解密用戶端電腦3的電腦名稱及IP位址的密鑰。

[0016] 安全管理員是資料庫11中的用戶，主要負責授權的工作，通過對資料庫資料管理系統10添加用戶信任憑證，將敏感資料的訪問許可權授權給某一用戶端電腦3。安全管理員擁有最大的許可權，只有安全管理員能直接查看到資料庫11中所有敏感資料的加密及解密的資訊。安全管理員可以對所有敏感資料進行加密及解密操作。

[0017] 主機1中安全管理員隨機產生一個主密鑰Master Key，所述Master Key是用於加密及解密資料庫11中的敏感資料的密鑰。Master Key在資料庫資料管理系統10中至關重要，如果有人拿到了Master Key，那麼就可以破解資料庫11中的所有加密資料，所以為了對Master Key進行保護，還需要對Master Key(其實就是一串字串)進行再次加密，這樣Master Key即使被人拿到了，也是一串密文。因此安全管理員會產生一個User Key，User Key存儲於主機1的系統檔案中，利用User Key作為密鑰對Master Key進行MD5不可逆加密，並將加密後密鑰Table Key存放在資料庫11中。綜上所述：對主密鑰Master Key的管理採取不可逆的MD5方式加密，這樣只有安全管理員知道密碼，增強了主密鑰Master Key的安全性。安全管理員可產生多個User Key，不同的User Key

可對應擁有對於資料庫11的不同敏感資料的訪問許可權。在主機1對用戶端電腦3添加用戶信任憑證時，對應不同的訪問許可權，將User Key賦予用戶端電腦3，所述User Key即為用戶端密鑰。即主機1中只有一個Master Key，但可同時存在多個User Key，不同的User Key對應不同敏感資料的訪問許可權，不同的User Key可以被賦予不同的用戶端電腦3，每個User Key均可與Master Key生成一個Table Key存儲於資料庫11中。

[0018] 所述選擇模組102用於當用戶端電腦3有訪問許可權時，選擇用戶端電腦3對主機1的訪問需求，判斷用戶端電腦3是需要加密資料庫11的資料，還是需要解密資料庫11的資料。

[0019] 所述加密模組103用於當用戶端電腦3需要加密資料庫11的資料時，加密資料庫11中的敏感資料。

[0020] 所述加密模組103通過下述步驟加密敏感資料：從ALL_TABLES中取得需加密欄位的資料類型，並根據不同的資料類型調用相應的處理方法，所述需加密欄位為敏感資料所在欄位，所述ALL_TABLES是資料庫11中所有表的一個集合，所述處理方法指對應不同的資料類型的不同的加密處理方法，如資料類型為字元或數值類型，則其所對應的加密處理方法不同；從資料庫11的資料字典中取得需加密欄位的相關資訊，並移除需加密欄位上的相關約束，所述相關資訊如預設值等，所述資料字典中存儲著需加密欄位的相關屬性資訊，如預設值、相關約束等，所述相關約束指需加密欄位上的約束條件，如欄

位為性別時，則其約束條件為只能輸入“男”或“女”；在需加密欄位所在表中添加臨時欄位，並將需加密欄位中資料複製至臨時欄位中；將需加密欄位清空，並將需加密欄位中資料類型轉變為RAW類型；將臨時欄位中資料進行加密，並將加密後資料複製至需加密欄位中，所述加密為利用主機1中安全管理員所產生的Master Key作為密鑰，採取加密演算法對臨時欄位中資料進行加密，所述加密演算法為AES256、AES、3DES-2KEY三種加密演算法其中之一；記錄加密的相關資訊至一個記錄表中，並刪除臨時欄位，所述記錄表中包括需加密欄位資料類型、需加密欄位上的相關約束、從資料字典中取得的需加密欄位的相關資訊以及採取的加密演算法。

[0021] 在加密前，敏感資料是可見的，在加密模組103對敏感資料進行加密後，該敏感資料所在表的名稱變更為“E$+原表名”，敏感資料是隱藏的，用戶端電腦3的用戶是見不到敏感資料的，此時在資料庫11中，產生一張和原表名名字相同的視圖供用戶端電腦3的用戶進行操作，此視圖中敏感資料是隱藏的。

[0022] 所述處理模組105用於接收用戶端電腦3對資料庫11的資料操作，並對應在資料庫11中進行相同的資料操作。所述對資料庫11的資料操作，為對資料庫11中的資料進行增加、刪除、修改、查詢的操作。

[0023] 當用戶端電腦3的用戶需要對資料庫11中的資料進行增加、刪除、修改和查詢的相關操作時，所述接收模組100接收用戶端電腦3輸入的User Key，並調用存儲在資料庫

11中對應的Table Key，之後用戶端電腦3的用戶在所述和原表名名字相同的視圖上進行資料操作，對應該在視圖上的資料操作，則處理模組105在資料庫11中對應進行同樣的資料操作。

[0024] 此時，如果用戶端電腦3的用戶輸入User Key直接去訪問“E$+原表名”這張表，則返回的是加密文本，同理用戶不輸入User Key而是直接去訪問和原表名名字相同的視圖，則會返回空文本。由此來實現用戶端電腦3對敏感資料的透明化操作，杜絕了用戶操作到敏感資料。

[0025] 所述解密模組104用於當用戶端電腦3需要對資料庫11的資料進行操作時，解密資料庫11中的敏感資料。

[0026] 所述解密模組104通過下述步驟解密敏感資料：從所述記錄表中取得需解密欄位資料，並在需解密欄位所在表中添加RAW類型臨時欄位，所述需解密欄位為敏感資料所在欄位；將需解密欄位複製至臨時欄位，並將需解密欄位清空；將需解密欄位資料類型轉換為原資料類型；將臨時欄位資料進行解密，並將解密後資料複製至需解密欄位，所述解密為由所述記錄表上得到需解密欄位的加密演算法，並利用所述Master Key做為密鑰，採取相關解密演算法進行逆向解密；恢復需解密欄位的預設值及欄位約束；將加密相關資訊從所述記錄表上移除，並刪除臨時欄位。所述原資料類型、需解密欄位的預設值及欄位約束由所述記錄表上得到。

[0027] 在解密過程中，首先需要接收模組100接收用戶端電腦3

的用戶端密鑰User Key，並調用存儲在資料庫11中對應的Table Key，解密模組104即可對相關敏感資料進行解密。

[0028] 本發明以保護敏感資料，讓維護人員也無法看到真實資料為目的，利用用戶端密鑰管理(加強對加密操作人員密碼的管理和保護)、IP和主機管控(限制加密操作人員登錄的用戶端電腦3以及唯一的IP位址)、操作流程日誌監控(為本發明中所述記錄表，對加密操作人員所作的任何一個動作都有詳盡的記錄)特性，從而形成了一個特有的資料加密及解密流程。

[0029] 如圖3所示，係為本發明資料庫資料管理方法較佳實施例之流程圖。

[0030] 步驟S100，所述接收模組100接收用戶端電腦3對主機1中資料庫11的訪問需求。

[0031] 步驟S101，所述驗證模組101驗證用戶端電腦3的許可權，判斷用戶端電腦3是否有訪問許可權。當用戶端電腦3有訪問許可權時，則執行步驟S102，否則，直接結束流程。

[0032] 驗證過程中對用戶端電腦3的電腦名稱、IP位址及用戶端密鑰進行驗證，只有當所述三者完全正確時，才能證明用戶端電腦3是安全管理員添加了用戶信任憑證的用戶，才可以對資料庫11中的敏感資料進行加密及解密操作。所述用戶端密鑰是加密及解密用戶端電腦3的電腦名稱及IP位址的密鑰。

[0033] 步驟S102，所述選擇模組102選擇用戶端電腦3對主機1的訪問需求，判斷用戶端電腦3是需要加密資料庫11的資料，還是需要解密資料庫11的資料。當用戶端電腦3需要加密資料庫11的資料時，則執行步驟S103，當用戶端電腦3需要解密資料庫11的資料時，則執行步驟S104。

[0034] 步驟S103，所述加密模組103加密資料庫11中的敏感資料。所述加密過程將在圖4中詳細介紹。

[0035] 在加密前，敏感資料時可見的，在加密模組103對敏感資料進行加密後，該敏感資料所在表的名稱變更為“E$+原表名”，用戶端電腦3的用戶是見不到敏感資料的，此時在資料庫11中，產生一張和原表名名字相同的視圖供用戶端電腦3的用戶進行操作，在該視圖中敏感資料也是隱藏的。

[0036] 步驟S105，所述處理模組105接收用戶端電腦3對資料庫11的資料操作。所述對資料庫11的資料操作，為對資料庫11中的資料進行增加、刪除、修改、查詢的操作。

[0037] 當用戶端電腦3的用戶需要對資料庫11中的資料進行增加、刪除、修改和查詢的相關操作時，所述接收模組100接收用戶端電腦3輸入的User Key，並調用存儲在資料庫11中對應的Table Key，之後用戶端電腦3的用戶在所述和原表名名字相同的視圖上進行資料操作，對應該在視圖上的資料操作，處理模組105在資料庫11進行同樣的資料操作。

[0038] 步驟S104，所述解密模組104解密資料庫11中的敏感資

料。所述解密過程將在圖5中詳細介紹。

[0039] 在解密過程中，首先接收模組100需要接收用戶端電腦3的用戶端密鑰User Key，並調用存儲在資料庫11中對應的Table Key，解密模組104即可對相關敏感資料進行解密。

[0040] 如圖4所示，係為本發明資料庫資料管理方法較佳實施例之加密子流程圖。

[0041] 步驟S1030，所述加密模組103從ALL_TABLES中取得需加密欄位的資料類型，並根據不同的資料類型調用相應的處理方法，所述需加密欄位為敏感資料所在欄位，所述ALL_TABLES是資料庫11中所有表的一個集合，所述處理方法指對應不同的資料類型的不同的加密處理方法，如資料類型為字元或數值類型，則其所對應的加密處理方法不同。

[0042] 步驟S1031，所述加密模組103從資料庫11的資料字典中取得需加密欄位的相關資訊，並移除需加密欄位上的相關約束，所述相關資訊如預設值等，所述資料字典中存儲著需加密欄位的相關屬性資訊，如預設值、相關約束等，所述相關約束指需加密欄位上的約束條件，如欄位為性別時，則其約束條件為只能輸入“男”或“女”。

[0043] 步驟S1032，所述加密模組103在需加密欄位所在表中添加臨時欄位，並將需加密欄位中資料複製至臨時欄位中。

[0044] 步驟S1033，所述加密模組103將需加密欄位清空，並將

需加密欄位中資料類型轉變為RAW類型。

[0045] 步驟S1034，所述加密模組103將臨時欄位中資料進行加密，並將加密後資料複製至需加密欄位中，所述加密為利用主機1中安全管理員所產生的Master Key作為密鑰，採取加密演算法對臨時欄位中資料進行加密，所述加密演算法為AES256、AES、3DES-2KEY三種加密演算法之一。

[0046] 步驟S1035，所述加密模組103記錄加密的相關資訊至一個記錄表中，並刪除臨時欄位，所述記錄表中包括需加密欄位資料類型、需加密欄位上的相關約束、從資料字典中取得需加密欄位的相關資訊以及採取的加密演算法。

[0047] 如圖5所示，係為本發明資料庫資料管理方法較佳實施例之解密子流程圖。

[0048] 步驟S1040，所述解密模組104從所述記錄表上取得需解密欄位資料，並在需解密欄位所在表中添加RAW類型臨時欄位，所述需解密欄位為敏感資料所在欄位。

[0049] 步驟S1041，所述解密模組104將需解密欄位複製至臨時欄位，並將需解密欄位清空。

[0050] 步驟S1042，所述解密模組104將需解密欄位資料類型轉換為原資料類型。所述原資料類型由所述記錄表上得到。

[0051] 步驟S1043，所述解密模組104將臨時欄位資料進行解密

，並將解密後資料複製至需解密欄位，所述解密為由所述記錄表上得到需解密欄位的加密演算法，並利用主機1中安全管理員所產生的Master Key做為密鑰，採取相關解密演算法進行逆向解密。

[0052] 步驟S1044，所述解密模組104恢復需解密欄位的預設值及欄位約束。所述需解密欄位的預設值及欄位約束由所述記錄表上得到。

[0053] 步驟S1045，所述解密模組104將加密相關資訊從所述記錄表上移除，並刪除臨時欄位。

[0054] 綜上所述，本發明符合發明專利要件，爰依法提出專利申請。惟，以上所述者僅爲本發明之較佳實施例，本發明之範圍並不以上述實施例爲限，舉凡熟悉本案技藝之人士援依本發明之精神所作之等效修飾或變化，皆應涵蓋於以下申請專利範圍內。

【圖式簡單說明】

[0055] 圖1係為本發明資料庫資料管理系統較佳實施例之架構圖。

[0056] 圖2係為本發明資料庫資料管理系統較佳實施例之功能模組圖。

[0057] 圖3係為本發明資料庫資料管理方法較佳實施例之流程圖。

[0058] 圖4係為本發明資料庫資料管理方法較佳實施例之加密子流程圖。

[0059] 圖5係為本發明資料庫資料管理方法較佳實施例之解密子流程圖。

【主要元件符號說明】

[0060] 主機 1

[0061] 資料庫資料管理系統 10

[0062] 資料庫 11

[0063] 網路 2

[0064] 用戶端電腦 3

[0065] 接收模組 100

[0066] 驗證模組 101

[0067] 選擇模組 102

[0068] 加密模組 103

[0069] 解密模組 104

[0070] 處理模組 105

[0071] 接收用戶端電腦對主機中資料庫的訪問需求 S100

[0072] 驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權 S101

[0073] 加密資料庫的資料還是解密資料庫的資料 S102

[0074] 加密資料庫中的敏感資料 S103

[0075] 解密資料庫中的敏感資料 S104

[0076] 接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作 S105

七、申請專利範圍：

1．一種資料庫資料管理方法，其中，該方法包括步驟：

接收步驟：接收用戶端電腦對主機中資料庫的訪問需求，所述用戶端電腦通過網路連接至主機；

驗證步驟：驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，當用戶端電腦有訪問許可權時，則執行選擇步驟，否則，直接結束流程，驗證過程中對用戶端電腦的電腦名稱、IP位址及用戶端密鑰進行驗證；

選擇步驟：選擇用戶端電腦對主機的訪問需求，當用戶端電腦需要加密資料庫的資料時，則執行加密步驟，當用戶端電腦需要解密資料庫的資料時，則執行解密步驟；

加密步驟：加密資料庫中的敏感資料；

處理步驟：接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作，所述對資料庫的資料操作為對資料庫中的資料進行增加、刪除、修改、查詢的操作；

解密步驟：解密資料庫中的敏感資料。

2．如申請專利範圍第1項所述之資料庫資料管理方法，其中，所述加密步驟包括：

從ALL_TABLES中取得需加密欄位的資料類型，並根據不同的資料類型調用相應的處理方法，所述需加密欄位為敏感資料所在欄位，所述ALL_TABLES是資料庫中所有表的一個集合；

從資料庫的資料字典中取得需加密欄位的屬性資訊，並移除需加密欄位上的約束條件；

在需加密欄位所在表中添加臨時欄位，並將需加密欄位中資料複製至臨時欄位中；

將需加密欄位清空，並將需加密欄位中資料類型轉變為RAW類型；

將臨時欄位中資料進行加密，並將加密後資料複製至需加密欄位中，所述加密為利用主機所產生的主密鑰，採取加密演算法對臨時欄位中資料進行加密，所述主密鑰是安全管理員所產生的，用於加密及解密資料庫中的敏感資料的密鑰，所述安全管理員為資料庫中的用戶；

記錄加密的相關資訊至一個記錄表中，並刪除臨時欄位，所述記錄表中包括需加密欄位資料類型、需加密欄位上的約束條件、從資料字典中取得需加密欄位的屬性資訊以及採取的加密演算法。

3．如申請專利範圍第2項所述之資料庫資料管理方法，其中，所述加密步驟還包括：

在資料庫中產生一張和原表名名字相同的視圖，供用戶端電腦的用戶進行資料操作。

4．如申請專利範圍第1項所述之資料庫資料管理方法，其中，所述解密步驟包括：

從所述記錄表上取得需解密欄位資料，並在需解密欄位所在表中添加RAW類型臨時欄位，所述需解密欄位為敏感資料所在欄位；

將需解密欄位複製至臨時欄位，並將需解密欄位清空；

將需解密欄位資料類型轉換為原資料類型，所述原資料類型由所述記錄表上得到；

將臨時欄位資料進行解密，並將解密後資料複製至需解密

欄位，所述解密為由所述記錄表上得到需解密欄位的加密演算法，並利用所述主密鑰，採取相關解密演算法進行逆向解密；

恢復需解密欄位的預設值及欄位約束條件，所述需解密欄位的預設值及欄位約束條件由所述記錄表上得到；

將加密相關資訊從所述記錄表上移除，並刪除臨時欄位。

5．如申請專利範圍第1項所述之資料庫資料管理方法，其中，在要進行解密步驟或處理步驟之前還包括：

接收用戶端電腦用戶輸入的用戶端密鑰，並調用儲存於資料庫中對應該用戶端密鑰的Table Key，所述Table Key為利用用戶端密鑰對主密鑰進行MD5不可逆加密所產生的密鑰。

6．一種資料庫資料管理系統，其中，該系統包括：

接收模組，用於接收用戶端電腦對主機中資料庫的訪問需求，所述用戶端電腦通過網路連接至主機；

驗證模組，用於驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權，驗證過程中對用戶端電腦的電腦名稱、IP位址及用戶端密鑰進行驗證；

選擇模組，用於當用戶端電腦有訪問許可權時，選擇用戶端電腦對主機的訪問需求，判斷用戶端電腦是需要加密資料庫的資料，還是需要解密資料庫的資料；

加密模組，用於當用戶端電腦需要加密資料庫的資料時，加密資料庫中的敏感資料；

處理模組，用於接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作，所述對資料庫的資料操作為對資料庫中的資料進行增加、刪除、修改、查詢

的操作；

解密模組，用於當用戶端電腦需要解密資料庫的資料時，解密資料庫中的敏感資料。

7．如申請專利範圍第6項所述之資料庫資料管理系統，其中，所述加密模組加密資料庫中的敏感資料包括：

從ALL_TABLES中取得需加密欄位的資料類型，並根據不同的資料類型調用相應的處理方法，所述需加密欄位為敏感資料所在欄位，所述ALL_TABLES是資料庫中所有表的一個集合；

從資料庫的資料字典中取得需加密欄位的屬性資訊，並移除需加密欄位上的約束條件；

在需加密欄位所在表中添加臨時欄位，並將需加密欄位中資料複製至臨時欄位中；

將需加密欄位清空，並將需加密欄位中資料類型轉變為RAW類型；

將臨時欄位中資料進行加密，並將加密後資料複製至需加密欄位中，所述加密為利用主機所產生的主密鑰，採取加密演算法對臨時欄位中資料進行加密，所述主密鑰是安全管理員所產生的，用於加密及解密資料庫中的敏感資料的密鑰，所述安全管理員為資料庫中的用戶；

記錄加密的相關資訊至一個記錄表中，並刪除臨時欄位，所述記錄表中包括需加密欄位資料類型、需加密欄位上的約束條件、從資料字典中取得需加密欄位的屬性資訊以及採取的加密演算法。

8．如申請專利範圍第7項所述之資料庫資料管理系統，其中，所述加密模組還用於：

在資料庫中產生一張和原表名名字相同的視圖，供用戶端電腦的用戶進行操作。

9．如申請專利範圍第6項所述之資料庫資料管理系統，其中，所述解密模組解密資料庫中的敏感資料包括：

從所述記錄表上取得需解密欄位資料，並在需解密欄位所在表中添加RAW類型臨時欄位，所述需解密欄位為敏感資料所在欄位；

將需解密欄位複製至臨時欄位，並將需解密欄位清空；

將需解密欄位資料類型轉換為原資料類型，所述原資料類型由所述記錄表上得到；

將臨時欄位資料進行解密，並將解密後資料複製至需解密欄位，所述解密為由所述記錄表上得到需解密欄位的加密演算法，並利用所述主密鑰，採取相關解密演算法進行逆向解密；

恢復需解密欄位的預設值及欄位約束條件，所述需解密欄位的預設值及欄位約束條件由所述記錄表上得到；

將加密相關資訊從所述記錄表上移除，並刪除臨時欄位。

10．如申請專利範圍第6項所述之資料庫資料管理系統，其中，所述接收模組還用於：

當處理模組需要進行資料操作或解密模組需要解密時，接收用戶端電腦用戶輸入的用戶端密鑰，並調用儲存於資料庫中對應該用戶端密鑰的Table Key，所述Table Key為利用用戶端密鑰對主密鑰進行MD5不可逆加密所產生的密鑰。

八、圖式：

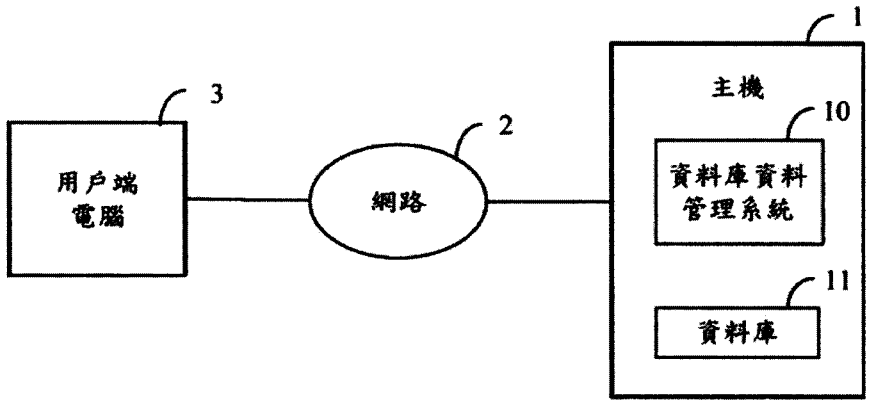


圖 1

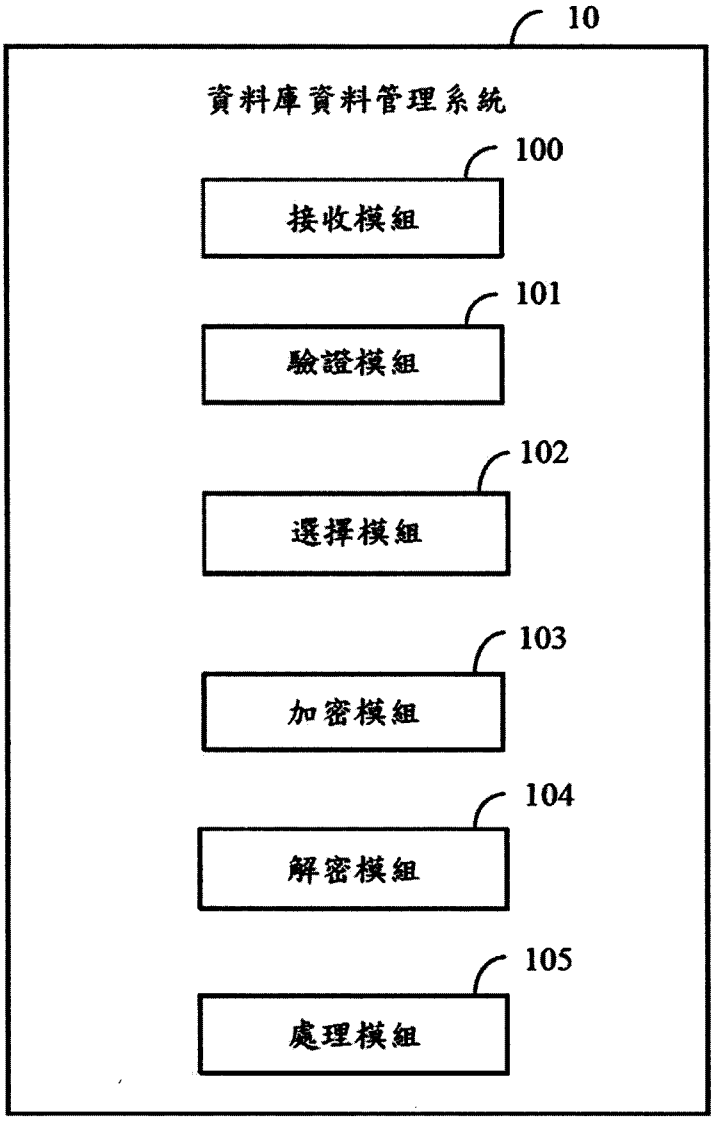

10
資料庫資料管理系統
100
接收模組
101
驗證模組
102
選擇模組
103
加密模組
104
解密模組
105
處理模組

圖 2

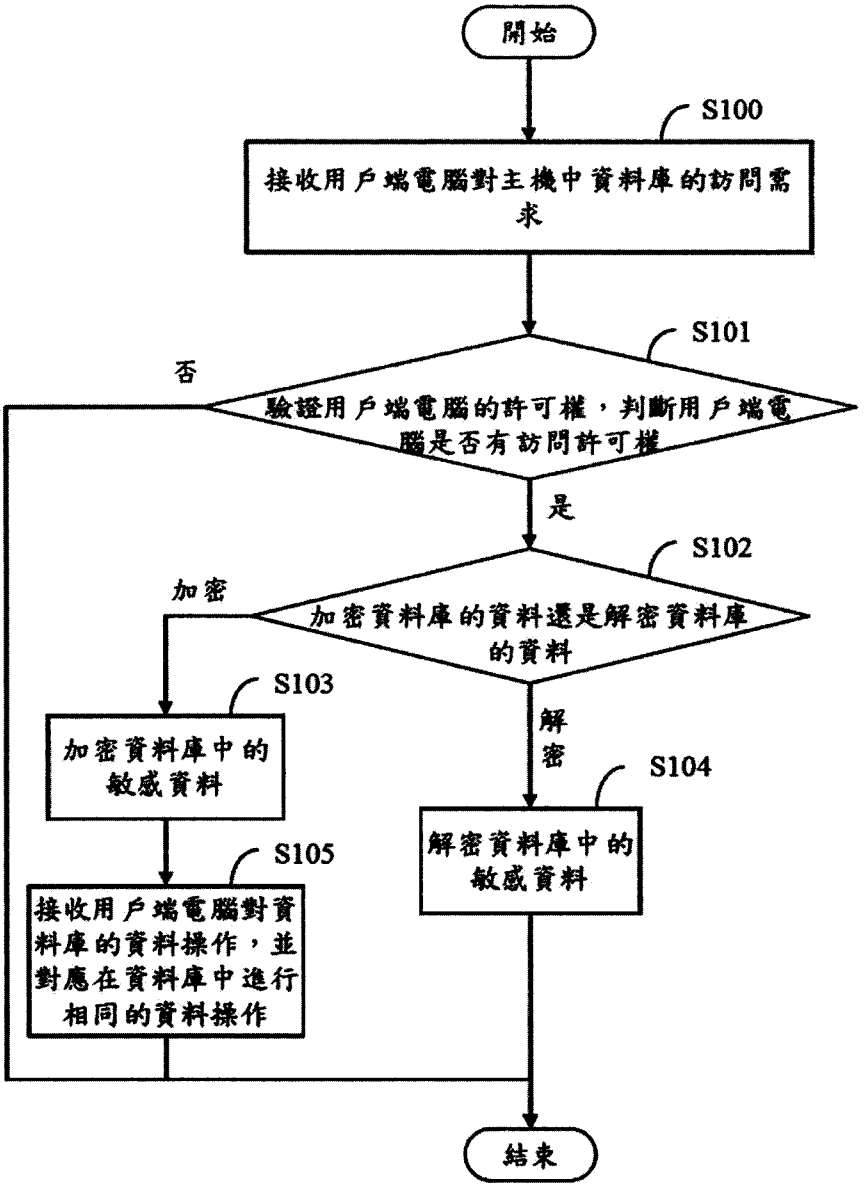

開始
S100
接收用戶端電腦對主機中資料庫的訪問需求
S101
驗證用戶端電腦的許可權，判斷用戶端電腦是否有訪問許可權
否
是
S102
加密資料庫的資料還是解密資料庫的資料
加密
解密
S103
加密資料庫中的敏感資料
S104
解密資料庫中的敏感資料
S105
接收用戶端電腦對資料庫的資料操作，並對應在資料庫中進行相同的資料操作
結束

圖 3

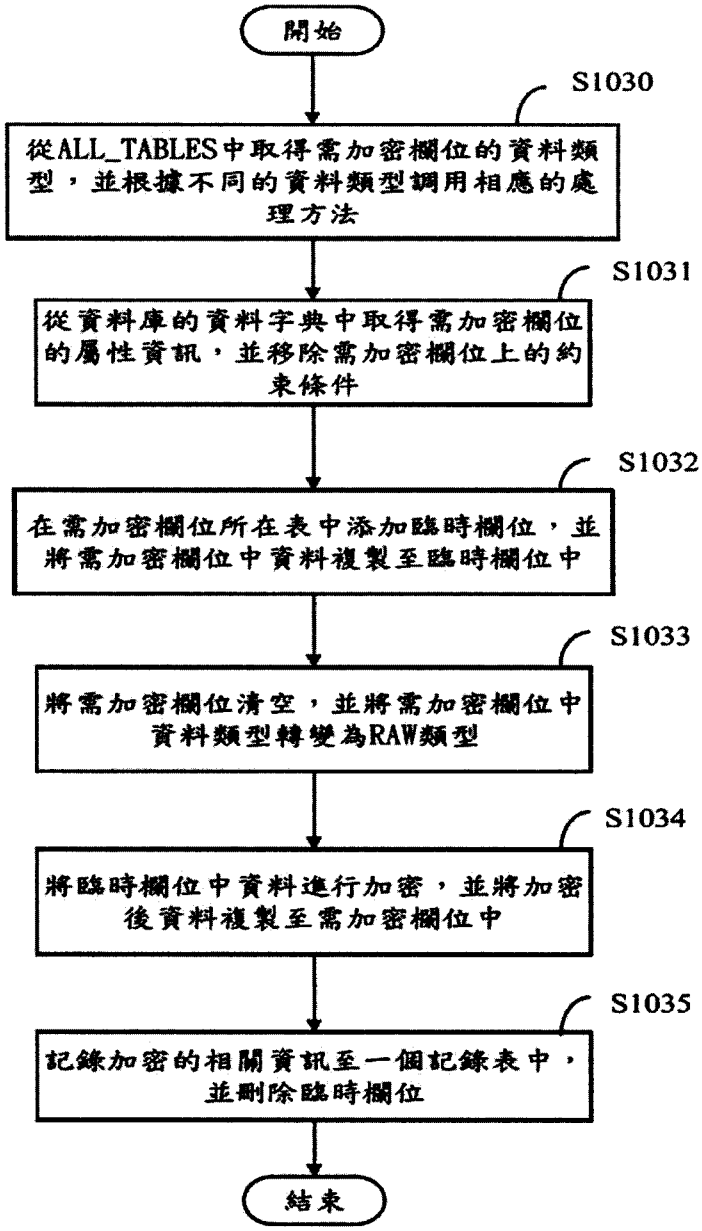

開始
S1030
從ALL_TABLES中取得需加密欄位的資料類型，並根據不同的資料類型調用相應的處理方法
S1031
從資料庫的資料字典中取得需加密欄位的屬性資訊，並移除需加密欄位上的約束條件
S1032
在需加密欄位所在表中添加臨時欄位，並將需加密欄位中資料複製至臨時欄位中
S1033
將需加密欄位清空，並將需加密欄位中資料類型轉變為RAW類型
S1034
將臨時欄位中資料進行加密，並將加密後資料複製至需加密欄位中
S1035
記錄加密的相關資訊至一個記錄表中，並刪除臨時欄位
結束

圖 4

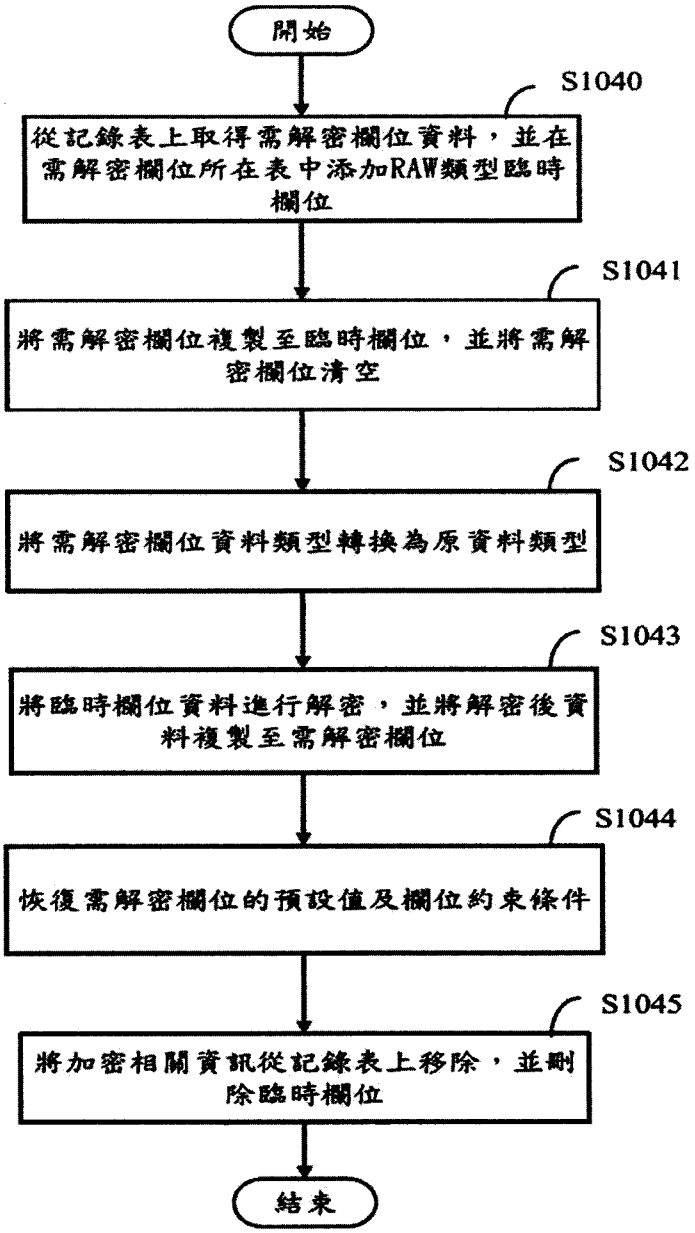

開始
S1040
從記錄表上取得需解密欄位資料，並在需解密欄位所在表中添加RAW類型臨時欄位
S1041
將需解密欄位複製至臨時欄位，並將需解密欄位清空
S1042
將需解密欄位資料類型轉換為原資料類型
S1043
將臨時欄位資料進行解密，並將解密後資料複製至需解密欄位
S1044
恢復需解密欄位的預設值及欄位約束條件
S1045
將加密相關資訊從記錄表上移除，並刪除臨時欄位
結束

圖 5