201626279

(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 201626279 A

(43)公開日： 中華民國 105 (2016) 年 07 月 16 日

(21)申請案號：104100328 (22)申請日： 中華民國 104 (2015) 年 01 月 06 日

(51)Int. Cl.： *G06F21/56 (2013.01)* *G06N99/00 (2010.01)*

(71)申請人：緯創資通股份有限公司 (中華民國) WISTRON CORPORATION (TW)

新北市汐止區新台五路 1 段 88 號 21 樓

(72)發明人：陳志明 CHEN, CHIH MING (TW)

(74)代理人：吳豐任；戴俊彥

申請實體審查：有 申請專利範圍項數：16 項 圖式數：5 共 23 頁

(54)名稱

保護方法與其電腦系統

PROTECTION METHOD AND COMPUTER SYSTEM THEREOF

(57)摘要

一種保護方法，用以解除免於一惡意軟體於一終端裝置之攻擊，該保護方法包含接收一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；根據一轉導機器學習，轉換該觀測資料為一第一對應資料；根據一引導機器學習，切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及傳輸該特徵辨識結果至該終端裝置。

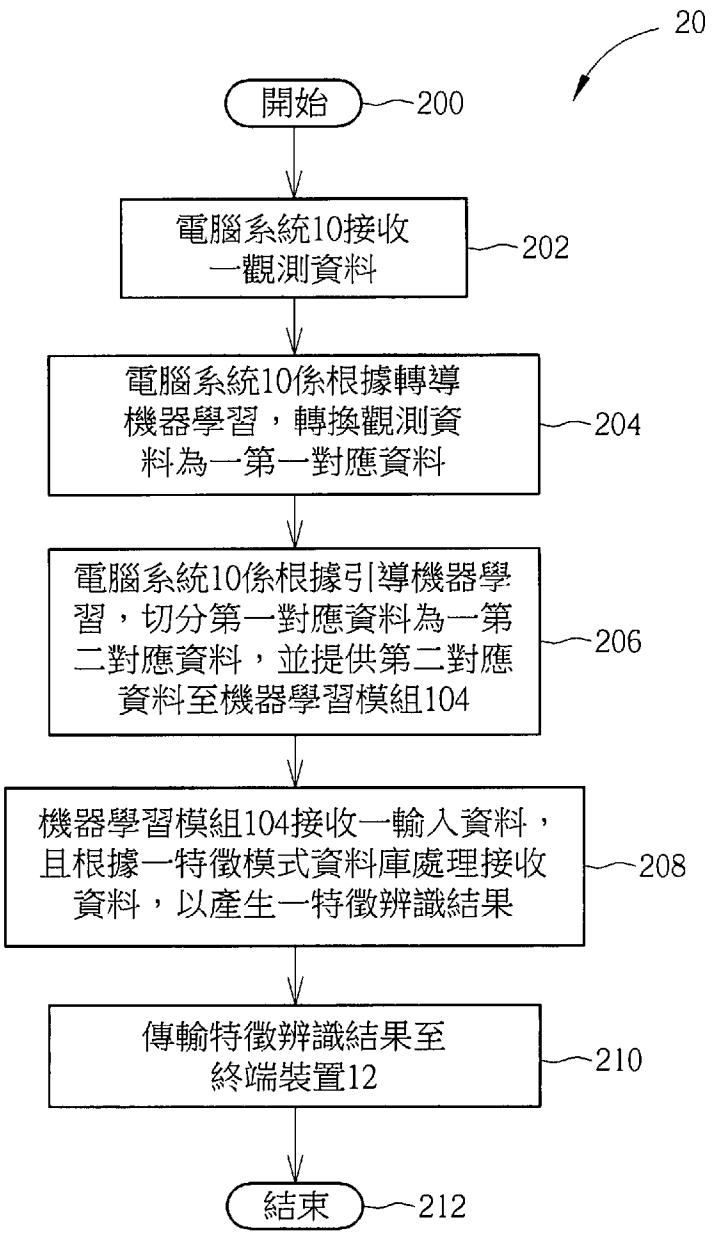
A protection method to be utilized for removing an attack of a malware inside a user equipment includes receiving an observed information including at least one of a sampled information and a labeled information; transforming the observed information to a first mapping information according to a transductive machine learning; splitting the first mapping information to form a second mapping information according to an inductive machine learning, and transmitting the second mapping information to a machine leaning module; the machine leaning module receiving an input information, and utilizing a pattern database to processing the input information for generating a pattern recognition result; and transmitting the pattern recognition result to the user equipment.

指定代表圖：

符號簡單說明：

20・・・保護流程

200、202、204、206、208、210・・・步驟



第2圖

201626279
201626279

發明摘要

※ 申請案號：104100328

※ 申請日：104. 1. 06　　※IPC 分類：G06F 21/56 (2013.01)
G06N 99/00 (2010.01)

【發明名稱】 保護方法與其電腦系統

Protection Method and Computer System thereof

【中文】

一種保護方法，用以解除免於一惡意軟體於一終端裝置之攻擊，該保護方法包含接收一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；根據一轉導機器學習，轉換該觀測資料為一第一對應資料；根據一引導機器學習，切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及傳輸該特徵辨識結果至該終端裝置。

【英文】

A protection method to be utilized for removing an attack of a malware inside a user equipment includes receiving an observed information including at least one of a sampled information and a labeled information; transforming the observed information to a first mapping information according to a transductive machine learning; splitting the first mapping information to form a second mapping information according to an inductive machine learning, and transmitting the second mapping information to a machine leaning module; the machine leaning module receiving an input information, and utilizing a pattern database to processing the input information for generating a pattern recognition result; and transmitting the pattern recognition result to the user equipment.

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

20	保護流程
200、202、204、206、208、210	步驟

【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

【發明名稱】保護方法與其電腦系統

Protection Method and Computer System thereof

【技術領域】

【0001】 本發明係指一種保護方法與其電腦系統，尤指一種保護終端裝置免於一惡意軟體之攻擊的保護方法與其電腦系統。

【先前技術】

【0002】 隨著網際網路的快速發展，一般人倚賴網路資訊的程度越來越普遍，隨之而來的惡意軟體如電腦病毒、間諜軟體、廣告軟體或垃圾郵件等，皆可大開門戶地通過網際網路之路徑，入侵或攻擊一般人所使用之電腦系統或行動裝置，或像是其他以連接網路並執行應用程式 APP 之電子裝置（如智慧型手錶)，病毒軟體惡意破壞上述電子裝置之軟、硬體功能，更甚者竊取其中的重要資訊。

【0003】 為了建立電腦系統或行動裝置的保護措施，通常係以安裝防毒軟體來辨識與隔離任何潛在之惡意軟體。傳統上，病毒辨識資料庫之更新與配置需透過人為操作，逐一比對該些病毒辨識是否與目前資料庫內的資料吻合，並合理地推測出潛在病毒辨識之樣態，進而提供電腦系統或行動裝置之使用者最有效且即時性的保護措施。然而，由於惡意軟體所對應之程式碼必然與時俱變，使得電腦系統或行動裝置之防毒軟體必須隨時進行更新以下載最新之病毒辨識資料庫，但病毒辨識資料庫中的資料數據往往過於龐大，加上人為操作的更新速度無法跟上惡意軟體程式碼的演變，而不利於所有電腦系統或行動裝置之保護操作，另外在一般電子裝置中，因不具有儲存大量病毒資訊之存儲空間，而導致中毒之後無法解決之困擾。

【0004】 因此，提供另一種保護終端裝置的保護方法與其電腦系統，來避免終端裝置受惡意軟體之攻擊，已成為本領域之重要課題。

【發明內容】

【0005】 因此，本發明之主要目的即在於提供一種保護終端裝置的保護方法與其電腦系統，來避免終端裝置受惡意軟體之攻擊。

【0006】 本發明揭露一種保護方法，用以解除一惡意軟體於一終端裝置之攻擊，該保護方法包含取得一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；根據一轉導機器學習，轉換該觀測資料為一第一對應資料；根據一引導機器學習，切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及傳輸該特徵辨識結果至該終端裝置。

【0007】 本發明另揭露一種電腦系統，耦接一終端裝置，並用以解除一惡意軟體於該終端裝置之攻擊，該電腦系統包含一中央處理器；以及一儲存裝置，耦接於該中央處理器，並儲存有一程式碼，該程式碼用來進行一保護方法，該保護方法包含接收一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；根據一轉導機器學習，轉換該觀測資料為一第一對應資料；根據一引導機器學習，切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及傳輸該特徵辨識結果至該終端裝置。

【圖式簡單說明】

【0008】

第 1 圖為本發明實施例一電腦系統耦接一終端裝置之示意圖。

第 2 圖為本發明實施例一保護流程之流程圖。

第 3 圖為本發明實施例一特徵模式資料樹圖之示意圖。

第 4 圖為本發明實施例一辨識流程之流程圖。

第 5 圖為本發明實施例一轉導機器學習與一引導機器學習之結果示意

圖。

【實施方式】

【0009】 在說明書及後續的申請專利範圍當中使用了某些詞彙來指稱特定的元件。所屬領域中具有通常知識者應可理解，製造商可能會用不同的名詞來稱呼同樣的元件。本說明書及後續的申請專利範圍並不以名稱的差異來作為區別元件的方式，而是以元件在功能上的差異來作為區別的基準。在通篇說明書及後續的請求項當中所提及的「包含」係為一開放式的用語，故應解釋成「包含但不限定於」。此外，「耦接」一詞在此係包含任何直接及間接的電氣連接手段。因此，若文中描述一第一裝置耦接於一第二裝置，則代表該第一裝置可直接連接於該第二裝置，或透過其他裝置或連接手段間接地連接至該第二裝置。

【0010】 請參考第 1 圖，第 1 圖為本發明實施例之一電腦系統 10 耦接一終端裝置 12 之示意圖。如第 1 圖所示，本實施例的電腦系統 10 基本架構包含如主機板、處理器、記憶體、硬碟、南橋模組、北橋模組等，其應係本領域所熟知，為求簡潔，第 1 圖僅繪示出電腦系統 10 之中央處理器 100、儲存裝置 102 與機器學習模組 104。儲存裝置 102 可以是唯讀記憶體、快閃記憶體、軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫，或是熟習本領域之通常知識者所熟知之任何其它儲存媒體等，用以儲存一程式碼，中央處理器 100 可執行程式碼來進終端裝置 12 所適用之一保護方法，而機器學習模組 104 係耦接中央處理器 100 與儲存裝置 102，並透過保護方法來產生一病毒特徵辨識結果且傳輸至終端裝置 12，以解除或避免終端裝置 12 遭受一惡意軟體（如電腦病毒、間諜軟體、廣告軟體或垃圾郵件等）之攻擊或入侵。當然，本實施例係直接繪出電腦系統 10 中的機器學習模組 104，來清楚標示本發明的主要技術特徵，於其他實施例中機器學習模組 104 的軟硬體操作機制，亦可由本實施例之中央處理器 100 與儲存裝置 102 彼此相互整合來提供相對應之軟硬體操作而取代之，非用以限制本發明的範疇。再者，本實施例

的電腦系統 10 於儲存裝置 102 中儲存有一轉導機器學習（Transductive machine learning）與一引導機器學習（Inductive machine learning）所對應之另一程式碼，且可透過中央處理器 100 之控制，進行另一訓練與學習操作，當然，本實施例中轉導機器學習與引導機器學習所對應之程式碼亦可獨立成為另一機器學習模組（未顯示於第 1 圖中），且耦接中央處理器 100 與儲存裝置 102，而非用以限制本發明的範疇。

【0011】 於本實施例中，電腦系統 10 與終端裝置 12 之間的傳輸方式可為一有線傳輸或一無線傳輸，非用以限制本發明的範疇。至於終端裝置 12 的實施態樣例如可為另一電腦系統、一行動裝置（如手機、平板、個人行動祕書裝置）、一筆記型電腦、一智慧型手錶、一可運算攜帶式電子產品或一多媒體電子裝置等，當然，本實施例中的終端裝置 12 亦可和電腦系統 10 間相互整合，來形成單一電腦系統 10 者，此亦屬於本發明的範疇之一。

【0012】 進一步，本實施例終端裝置 12 所適用之保護方法可歸納為一保護流程 20，且被編譯為程式碼而儲存於儲存裝置 102 中，如第 2 圖所示，保護流程 20 包含以下步驟。

【0013】 步驟 200：開始。

【0014】 步驟 202：電腦系統 10 接收一觀測資料。

【0015】 步驟 204：電腦系統 10 係根據轉導機器學習，轉換觀測資料為一第一對應資料。

【0016】 步驟 206：電腦系統 10 係根據引導機器學習，切分第一對應資料為一第二對應資料，並提供第二對應資料至機器學習模組 104。

【0017】 步驟 208：機器學習模組 104 接收一輸入資料，且根據一特徵模式資料庫處理輸入資料，以產生一特徵辨識結果。

【0018】 步驟 210：傳輸特徵辨識結果至終端裝置 12。

【0019】 步驟 212：結束。

【0020】 於步驟 202 中，本實施例中的電腦系統 10 適性地接收來自一可運

算裝置、一遠端儲存裝置、一應用程式或一網路資料所對應之一操作或一資料，例如傳輸/夾帶之電子檔案、安裝一特定程式之操作或開啟一網頁資料之瀏覽操作，並將該些操作或資料中至少一者當作本實施例的觀測資料，進而從該些觀測資料中檢測是否有存在最新或潛在之病毒特徵資料。較佳地，本實施例的觀測資料中包含有一未辨識資料與一已辨識資料中至少一者，其中已辨識資料係該筆資料所攜帶之至少一片段病毒特徵資料已可被辨識，而未辨識資料係該筆資料所攜帶之片段病毒特徵資料仍未可被辨識。

【0021】 於步驟 204 中，本實施例中的電腦系統 10 根據轉導機器學習所對應之程式碼的操作，轉換觀測資料來形成第一對應資料。較佳地，若觀測資料有潛在之片段病毒特徵資料，於電腦系統 10 接收至少一之未辨識資料及/或已辨識資料後，轉導機器學習可對應判斷是否存在有不同種類的惡意軟體，以將觀測資料進行一初步分類，進而產生第一對應資料。

【0022】 舉例來說，本實施例可包含有惡意軟體 V_1～V_4 等四種，且不同惡意軟體間係具備有不同之一可辨識特徵資料來分別代表電腦病毒 V_1、一間諜軟體 V_2、一廣告軟體 V_3 或一垃圾郵件 V_4，在此情況下，本實施例的轉導機器學習係參考觀測資料 Ob_1～Ob_N 每一者所包含之可辨識特徵資料，以將觀測資料 Ob_1～Ob_N 分為不同之群組資料 G_1～G_4。其中，每一群組資料被視為一特徵群聚（labeled cluster）且包含有相同之可辨識特徵資料，而本實施例中的群組資料 G_1～G_4 例如依序為一電腦病毒 V_1、一間諜軟體 V_2、一廣告軟體 V_3 或一垃圾郵件 V_4 等，非用以限制本發明之範疇。至於觀測資料 Ob_1～Ob_N 對應至群組資料 G_1～G_4 之對應結果，則為本實施例中的第一對應資料。因此，本實施例的轉導機器學習係判斷每一觀測資料（包含至少一未辨識資料及/或已辨識資料）是否屬於相同的惡意軟體，並將其對應結果傳輸至引導機器學習，來做為引導機器學習之輸入資料。

【0023】 於步驟 206 中，電腦系統 10 根據引導機器學習所對應之程式碼的

操作，轉換第一對應資料來形成第二對應資料，並傳輸第二對應資料至機器學習模組 104。較佳地，本實施例中的引導機器學習可將每一特徵群聚再分類為複數個特徵子群聚，以將初步對應後之觀測資料（包含未辨識資料與已辨識資料中至少一者）對應至複數個特徵子群聚，進而產生第二對應資料。

【0024】 舉例來說，本實施例的引導機器學習可將每一群組資料如 G_1 所對應之電腦病毒 V_1 分類為不同型號、版本或編碼之單一特定惡意軟體種類如 V_1_1～V_1_n，以將歸類為群組資料 G_1 之所有觀測資料（即相同種類之惡意軟體）再細分為不同之特定惡意軟體種類，進而得到每一群組資料（包含至少一未辨識資料及/或已辨識資料）對應至單一特徵群聚中所有特徵子群聚的對應結果，且形成第二對應資料來傳輸至機器學習模組 104。因此，本實施例的引導機器學習可將專屬不同惡意軟體之觀測資料（包含至少一未辨識資料及/或已辨識資料）再分類為不同型號、版本或編碼之單一特定惡意軟體種類，並將其對應結果傳輸至機器學習模組 104，來提供機器學習模組 104 之相關更新操作。

【0025】 較佳地，本實施例電腦系統 10 的機器學習模組 104 還包含有特徵模式資料庫，且特徵模式資料庫預設有複數個特徵模式資料，而每一特徵模式資料係為進行保護流程 20 之前已成功對應至一特徵子群聚之已辨識資料（即已辨識資料對應至一特徵子群聚之對應結果），且該些特徵模式資料可用來辨識潛在之片段病毒特徵資料。據此，本實施例的機器學習模組 104 係利用觀測資料（包含至少一未辨識資料及/或已辨識資料），並適性地透過轉導機器學習以及引導機器學習的兩階段操作，以完成針對每一筆觀測資料之有效率且精準的學習與訓練操作，進而將潛在之片段病毒特徵資料與其對應至複數個特定惡意軟體種類的對應結果（即第二對應資料）傳輸至機器學習模組 104，使得機器學習模組 104 之特徵模式資料庫可動態/即時地進行更新操作，相較於習知技術，本實施例所提供之轉導機器學習以及引導機器學習的訓練與學習操作，已無須透過人力操作來更新或配置特徵模式資料庫中的龐

大資料量，對應提高辨識各種類型之惡意軟體的處理效率。

【0026】 換言之，本實施例中的機器學習模組 104 可即時進行特徵模式資料庫之更新操作，同時對應儲存該些對應結果（即第二對應資料）。據此，於步驟 208 中，當機器學習模組 104 接收輸入資料後，機器學習模組 104 將進行輸入資料與特徵模式資料庫所儲存之對應結果間的一辨識操作，以產生特徵辨識結果，且於步驟 210 中，傳輸特徵辨識結果至終端裝置 12，進而提供終端裝置 12 處理不同惡意軟體之適性保護操作。較佳地，本實施例的輸入資料係為電腦系統 10 接收來自可運算裝置、遠端儲存裝置、應用程式或網路資料等處所對應之操作或資料，來代表各類型潛在之惡意軟體。至於本實施例所用的辨識操作，可理解為一分散（Separation）流程，例如透過一合併特徵方程式（Joint feature function），於輸入資料與特徵模式資料庫所儲存之對應結果間進行比對，來判斷該些輸入資料中有潛伏的惡意軟體。

【0027】 值得注意地，為了避免惡意軟體會輕易地被終端裝置之防毒軟體所偵測，惡意軟體之設計者常將惡意軟體的本體分解成複數個子體，且安插於一或多個電子檔案內的多個位元位置，而本實施例將透過特徵模式資料庫中之一或多個特徵模式資料樹圖，來辨識惡意軟體的本體及/或本體之複數個子體。請參考第 3 圖，第 3 圖為本發明實施例一特徵模式資料樹圖 30 之示意圖。如第 3 圖所示，本實施例的特徵模式資料樹圖 30 包含有複數個可辨識特徵資料，如第 3 圖中所圈示之一支幹 300，同時，支幹 300 可代表一電子檔案之結構特徵，並標示有惡意軟體之複數個子體的所在位置。其中，每一支幹皆包含有複數個標誌（token）來代表單一子體，每一子體間可串接形成一線狀實施態樣，每兩個標誌間的連接線係為該些標誌安插於電子檔案內所代表之偏移量（Offset），且每一可辨識特徵資料末端的標誌還耦接一治癒資料（script）。一旦惡意軟體之本體及/或複數個子體已被辨識時，治癒資料可對應進行終端裝置 12 的掃毒操作，例如刪除或隔離該些可辨識特徵資料，來免除惡意軟體對終端裝置 12 的入侵或攻擊。

【0028】 詳細來說，於辨識操作下，本實施例將進行一半監督特徵學習（Semi-supervised structured learning）操作，其將定義合併特徵方程式為Φ(x, y)，其中 x 代表一訓練後資料，而 y 代表一候選預測值，兩者係透過 Φ(x, y)對應至一向量，而該向量具有一長度 n，且 n 值係根據不同訓練模組而有不同，同時本實施例還定義另一方程式 GEN 來產生該候選預測值，並預設長度 n 對應一權重向量 w，以及預設一遞回操作之次數。據此，本實施利將進行 $\hat{y} = \arg\max\{y \in GEN(X)\}(W^T\Phi(x,y))$之遞回操作，且隨者時間 t 之演進，適性更新權重向量 w 之值，即進行$w = w + c(-\Phi(x,\hat{y}) + \Phi(x,t))$之操作，其中 c 代表一學習比率。據此，遞回操作結束後，本實施例所得之候選預測值可判斷輸入資料與特徵模式資料庫所儲存之對應結果間是否存在有相同之至少一可辨識特徵資料。

【0029】 於本實施例中，完成半監督特徵學習操作後，且機器學習模組 104 判斷複數個特徵模式資料與輸入資料間包含有相同之至少一可辨識特徵資料時（即輸入資料中包含或攜帶有潛在之惡意軟體），本實施例的機器學習模組 104 係將至少一可辨識特徵資料與其所耦接之治癒資料作為特徵辨識結果，並傳輸將特徵辨識結果至終端裝置 12 來進行其保護操作。較佳地，本實施例的電腦系統 10 可為一終端伺服器，且經由一有線傳輸或一無線傳輸來傳送特徵辨識結果（包含至少一可辨識特徵資料與其耦接之治癒資料）至終端裝置 12，以進行終端裝置的掃毒操作來刪除或隔離惡意軟體之本體或複數個子體，進而免除終端裝置 12 恐遭惡意軟體的入侵或攻擊。

【0030】 於另一實施例中，一旦判斷複數個特徵模式資料與輸入資料間並未包含有相同之至少一可辨識特徵資料時，本實施例將還進行一相似核心（Similarity kernels）操作，以產生一處方性分析（Prescriptive analytics）結果或一認知性分析（Cognitive analytics）結果來作為特徵辨識結果，並傳輸特徵辨識結果至終端裝置 12 來執行該其保護操作。

【0031】 舉例來說，於相似核心操作下，本實施例將定義一得分方程式

（Scoring function）為F: X × Y ↦ ℝ，其中 x 代表一輸入資料，而 y 代表特徵模式資料庫所儲存之對應結果，並進行$\hat{y}_i = arg\max_{y\in Y}(\Delta(y_i, y) + w^T\Psi(x_i, y))$之操作，或透過 Mercer kernel 的操作如$K\left((x_i, y_i), (x_j, y_j)\right) = \langle|\Psi(x_i, y_i), \Psi(x_j, y_j)|\rangle$，以取得本實施例的得分方程式為$F(x, y) = w^{*T}\Psi(x, y) = \sum_{\bar{y}\in W}\alpha^*_{\bar{y}}(\frac{1}{n}\sum_{i=1}^{n}[K\left((x, y), (x_i, y_i)\right) - K((x, y), (x_i, \overline{y_i}))])$，同時還結合$\hat{y}_i = arg\max_{y\in Y}(\Delta(y_i, y) + F(x, y))$之操作，來表達最有可能之潛在惡意軟體之組合為$\bar{y} = (\overline{y_1}, \ldots, \overline{y_n})$。另外，本實施例還利用$K\left((x_i, y_i), (x_j, y_j)\right) = \Lambda(x_i, x_j)\cdot\Omega(y_i, y_j; x_i, x_j)$之操作，來預測潛在之惡意軟體的來源或種類，其中$\Lambda(x_i, x_j)$代表輸入資料之相似度，而$\Omega(y_i, y_j)$代表特徵模式資料庫中不同可辨識特徵資料之相似度。再者，本實施例還選用 Gaussian kernel Λ來表示輸入資料之間的距離或離散程度，即$\Lambda(x_i, x_j) = \exp(-\frac{\left\|\phi(x_i)-\phi(x_j)\right\|^2}{2\sigma^2})$之操作，其中 ϕ: χ ↦ $\mathbb{R}^n$，並選用 n=4 來表示輸入資料係為可運算裝置、遠端儲存裝置、應用程式或網路資料等四種來源處所對應之各種操作或資料。此外，本實施例還透過$\Omega(y_i, y_j; x_i, x_j) = \sum_l^L \beta_l\Omega_l(y_i, y_j; x_i, x_j)$之操作來表示一特定可辨識特徵資料的相似度，其中包含有潛在惡意軟體之三種核心計算值，分別為 Node kernel 來代表位置（position）、Token kernel 來代表特徵（signature）以及 Script kernel 來代表治癒資料（script）。

【0032】 在此情況下，當取得相似核心操作之辨識結果，且查覺輸入資料中存在潛伏的惡意軟體之本體或複數個子體中一者時，本實施例的機器學習模組 104 將適性提供處方性分析結果至終端裝置 12，其中處方性分析結果包含有一或多種可選擇的掃毒方式，且可告知/建議終端裝置使用者複數種選擇/手段，以刪除或隔離夾帶惡意軟體的本體及/或複數個子體的電子檔案（即該些潛在之片段病毒特徵資料）。或者，本實施例的機器學習模組 104 另可提供

認知性分析結果，來告知終端裝置使用者，目前終端裝置 12 正遭受某一特定惡意軟體之攻擊或入侵，而應採用該某一特定惡意軟體所對應之特定掃毒操作，以預防性地清除或隔離該某一特定惡意軟體的入侵或攻擊，進而避免終端裝置 12 發生無法正常運作或檔案毀損之情形。

【0033】 進一步，於步驟 208 中機器學習模組 104 所適用之辨識操作，還可被歸納為一辨識流程 40，且被編譯為程式碼而儲存於儲存裝置 102 中，如第 4 圖所示，辨識流程 40 包含以下步驟。

【0034】 步驟 400：開始。

【0035】 步驟 402：透過半監督特徵學習操作，以判斷輸入資料與特徵模式資料庫所儲存之對應結果間是否存在有相同之至少一可辨識特徵資料。若兩者存在相同之可辨識特徵資料，進行步驟 404，否則進行步驟 406。

【0036】 步驟 404：機器學習模組 104 傳輸特徵辨識結果至終端裝置 12 來進行其保護操作。

【0037】 步驟 406：再透過相似核心操作，以對應產生處方性分析結果或認知性分析結果來執行終端裝置 12 之保護操作。

【0038】 由於第 4 圖所示辨識流程 40 之相關操作已於步驟 208 與步驟 210 的相關段落進行說明，為避免不必要的贅述，在此僅簡單圖示辨識流程 40 來茲說明。

【0039】 簡言之，本實施例中的終端裝置 12 並非直接儲存或預設有特徵模式資料庫，而係根據電腦系統 10 中機器學習模組 104 的辨識操作來對應接收特徵辨識結果，以進行相關之掃毒操作，相較於習知技術的終端裝置仍須安裝或預存有數據量龐大之病毒辨識資料庫，本實施例所提供之終端裝置 12 的硬體限制已大幅下降。此外，由於本實施例還利用轉導機器學習以及引導機器學習之兩階段訓練與學習操作，來動態地更新特徵模式資料庫，相較於習知技術仍須使用大量人力、時間成本來進行潛在片段病毒特徵資料之辨識操作或更新服務，本實施例之兩階段訓練與學習操作確實已可提高各種類型惡

意軟體的辨識效率，而增進終端裝置使用者的操作便利和應用範圍。

【0040】 值得注意地，本實施例並未限制電腦系統 10 與終端裝置 12 間的溝通與時機，使得本實施例的輸入資料可由電腦系統 10 與終端裝置 12 中任一者取得，並經電腦系統 10 之機器學習模組 104 的操作後，對應取得不同輸入資料之相關保護方法，以利於終端裝置 12 來進行各類型惡意軟體的掃毒操作。當然，本領域具通常知識者亦可加入不同之傳輸加解密操作或認證機制等，以搭配有本實施例中電腦系統 10 與終端裝置 12 間的傳輸操作，而非用以限制本發明的範疇。

【0041】 此外，請再參考第 5 圖，第 5 圖為本發明實施例一轉導機器學習與一引導機器學習之結果示意圖，其中，第 5 圖左邊係為轉導機器學習的結果示意圖，圖中僅列出單一已被分類為相同群組資料 G_1，且包含有觀測資料 Ob_1～Ob_3，同時群組資料 G_1 係對應為惡意軟體之中一者如電腦病毒 V_1。另外，第 5 圖右邊係為引導機器學習的結果示意圖，根據第 5 圖左邊所示之對應結果，觀測資料 Ob_1～Ob_3 還被操作來分別對應為電腦病毒 V_1 中特定電腦病毒種類如 V_1_1～V_1_3。雖然第 5 圖的實施例僅為示範性說明，轉導機器學習與引導機器學習係如何分別得到第一對應資料與第二對應資料，當然，本領域具通常知識者還可適性地結合或修改其他訓練與學習機器之設計模型，以實現本實施例中兩階段或多階段的受訓與學習操作，進而提供更精準之對應結果來動態更新特徵模式資料庫者，此亦屬於本發明的範疇之一。

【0042】 綜上所述，本發明實施例係提供一種包含有機器學習模組之電腦系統，可接收經由轉導機器學習與引導機器學習之受訓資料，來適性且即時地更新機器學習模組之特徵模式資料庫；此外，本實施例的終端裝置不儲存特徵模式資料庫之龐大資料，而僅接收機器學習模組辨識操作後的特徵辨識結果，以減少終端裝置需額外配置大量的儲存空間，進而降低生產成本並提高其應用範圍。

【0043】 以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【符號說明】

【0044】

10	電腦系統
100	中央處理器
102	儲存裝置
104	機器學習模組
12	終端裝置
20	保護流程
200、202、204、206、208、210、212、400、402、404、406	步驟
30	特徵模式資料樹圖
300	支幹
40	辨識流程
G_1	群組資料
Ob_1～Ob_3	觀測資料
V_1	電腦病毒
V_1_1～V_1_3	特定電腦病毒種類
Offset 1～ Offset 7	偏移量
Token A～Token F	標誌
Script 1～Script 3	治癒資料

申請專利範圍

1. 一種保護方法，用以解除一惡意軟體於一終端裝置之攻擊，該保護方法包含：

接收一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；

根據一轉導機器學習（Transductive machine learning），轉換該觀測資料為一第一對應資料；

根據一引導機器學習（Inductive machine learning），切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；

該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及

傳輸該特徵辨識結果至該終端裝置。

2. 如請求項 1 所述之保護方法，其中該輸入資料係來自一可運算裝置、一遠端儲存裝置、一應用程式或一網路資料所對應之一操作或一資料，而該觀測資料係為該輸入資料所對應之該操作或該資料中至少一者。

3. 如請求項 1 所述之保護方法，其中該轉導機器學習係根據一可辨識特徵資料，以將該觀測資料分類對應至複數個群組資料來形成該第一對應資料，其中每一該群組資料係對應為一特徵群聚（labeled cluster）。

4. 如請求項 3 所述之保護方法，其中該引導機器學習係接收該第一對應資料，且區分每一該特徵群聚為複數個特徵子群聚，以將對應後之每一群組資料之該觀測資料對應至該複數個特徵子群聚，進而得到該複數組群組資料中該未辨識資料與該已辨識資料中至少一者對應至該複數個特徵子群聚之對應結果且形成該第二對應資料。

5. 如請求項 4 所述之保護方法，其中該第二對應資料係用來更新該機器學習模組之該特徵模式資料庫，其中該特徵模式資料庫包含有複數個特徵

模式資料，而每一特徵模式資料係為一已辨識資料對應至一特徵子群聚之對應結果。

6. 如請求項 5 所述之保護方法，其中該機器學習模組係進行該複數個特徵模式資料與該輸入資料之一辨識操作，以產生該特徵辨識結果，進而進行該終端裝置之該保護操作。

7. 如請求項 6 所述之保護方法，其還包含進行一半監督特徵學習（Semi-supervised structured learning）操作，來判斷該複數個特徵模式資料與該輸入資料間是否包含有相同之至少一可辨識特徵資料，且當該複數個特徵模式資料與該輸入資料間包含有相同之至少一可辨識特徵資料時，將該至少一可辨識特徵資料與其所對應之一治癒資料（script）作為該特徵辨識結果，以傳輸該特徵辨識結果至該終端裝置來進行該保護操作，其中，該可辨識特徵資料係對應為一電子檔案之結構特徵。

8. 如請求項 7 所述之保護方法，其中若該複數個特徵模式資料與該輸入資料間未包含有相同之至少一可辨識特徵資料時，還進行一相似核心（Similarity kernels）操作，以產生一處方性分析（Prescriptive analytics）結果或一認知性分析（Cognitive analytics）結果為該特徵辨識結果，進而傳輸該特徵辨識結果至該終端裝置來執行該保護操作。

9. 一種電腦系統，耦接一終端裝置，並用以解除一惡意軟體於該終端裝置之攻擊，該電腦系統包含：

一中央處理器；以及

一儲存裝置，耦接於該中央處理器，並儲存有一程式碼，該程式碼用來進行一保護方法，該保護方法包含：

接收一觀測資料，其中該觀測資料包含有一未辨識資料與一已辨識資料中至少一者；

根據一轉導機器學習（Transductive machine learning），轉換該觀測資料為一第一對應資料；

根據一引導機器學習（Inductive machine learning），切分該第一對應資料為一第二對應資料，並提供該第二對應資料至一機器學習模組；

該機器學習模組接收一輸入資料，且根據一特徵模式資料庫處理該輸入資料，以產生一特徵辨識結果；以及

傳輸該特徵辨識結果至該終端裝置。

10. 如請求項 9 所述之電腦系統，其中該輸入資料係來自一可運算裝置、一遠端儲存裝置、一應用程式或一網路資料所對應之一操作或一資料，而該觀測資料係為該輸入資料所對應之該操作或該資料中至少一者。

11. 如請求項 9 所述之電腦系統，其中該保護方法還包含該轉導機器學習根據一可辨識特徵資料，以將該觀測資料分類對應至多個群組資料來形成該第一對應資料，其中每一該群組資料係對應為一特徵群聚（labeled cluster）。

12. 如請求項 11 所述之電腦系統，其中該保護方法還包含該引導機器學習接收該第一對應資料，且區分每一該特徵群聚為複數個特徵子群聚，以將對應後之每一群組資料之該觀測資料對應至該複數個特徵子群聚，進而得到該複數組群組資料中該未辨識資料與該已辨識資料中至少一者對應至該複數個特徵子群聚之對應結果且形成該第二對應資料。

13. 如請求項 12 所述之電腦系統，其中該保護方法還包含利用該第二對應資料來更新該機器學習模組之一特徵模式資料庫，其中，該特徵模式資料庫包含有複數個特徵模式資料，而每一特徵模式資料係為一已辨識資料對應至一特徵子群聚之對應結果。

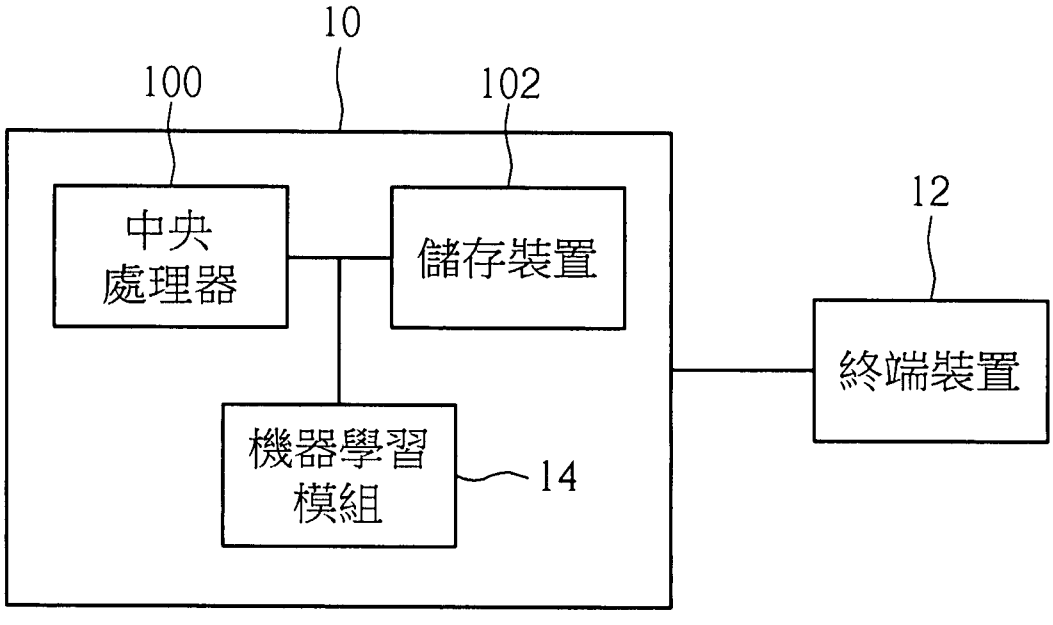
14. 如請求項 13 所述之電腦系統，其中該保護方法還包含該機器學習模組進行該複數個特徵模式資料與該輸入資料之一辨識操作，以產生該特徵辨識結果，進而進行該終端裝置之該保護操作。

15. 如請求項 14 所述之電腦系統，其中該保護方法還包含進行一半監督特徵

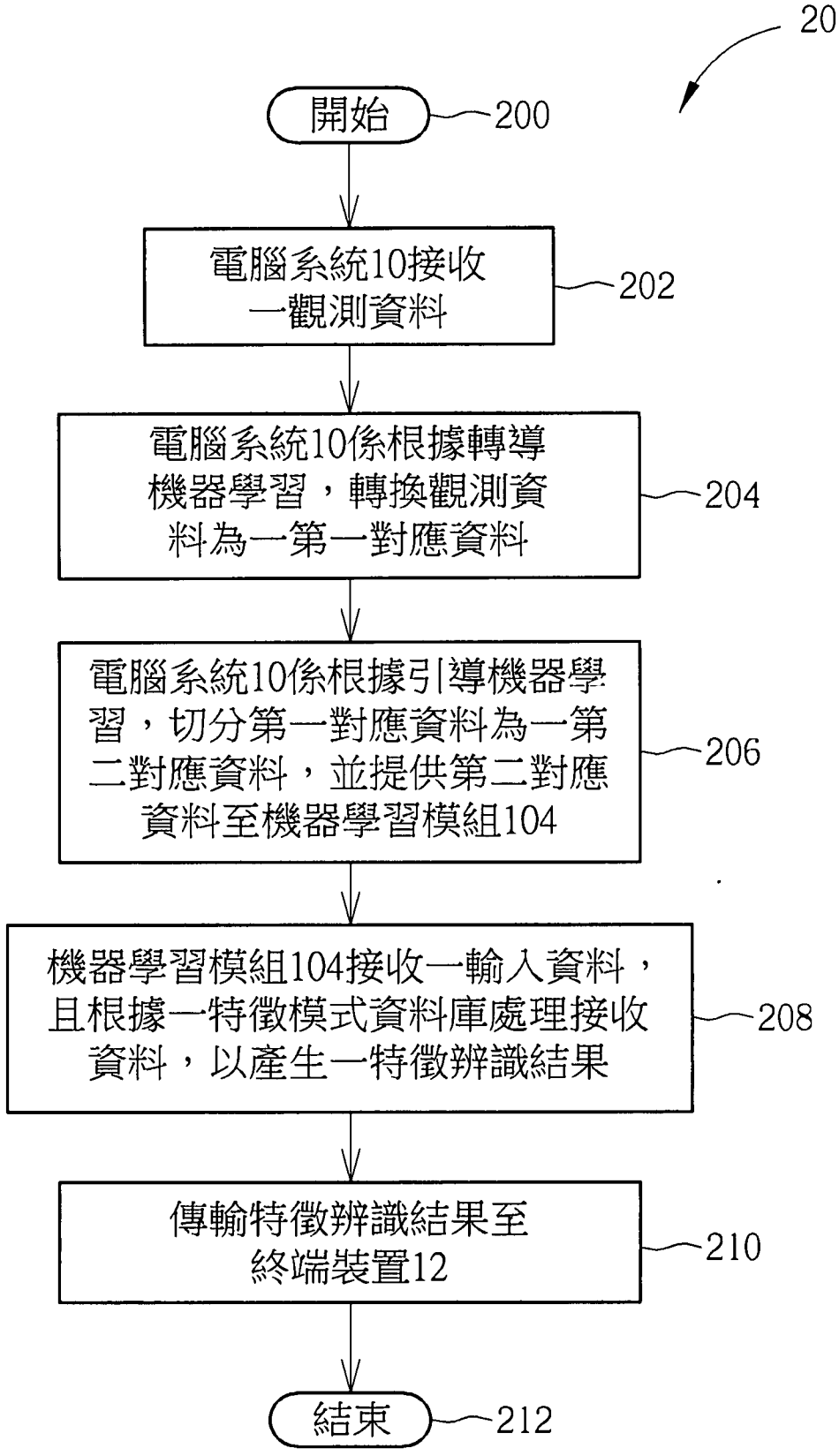
學習（Semi-supervised structured learning）操作，來判斷該複數個特徵模式資料與該輸入資料間是否包含有相同之至少一可辨識特徵資料，且當該複數個特徵模式資料與該輸入資料間包含有相同之至少一可辨識特徵資料時，將該至少一可辨識特徵資料與其所對應之一治癒資料（script）作為該特徵辨識結果，以傳輸該特徵辨識結果至該終端裝置來進行該保護操作，其中，該可辨識特徵資料係對應為一電子檔案之結構特徵。

16. 如請求項 15 所述之電腦系統，其中該保護方法還包含若該複數個特徵模式資料與該輸入資料間未包含有相同之至少一可辨識特徵資料時，進行一相似核心（Similarity kernels）操作，以產生一處方性分析（Prescriptive analytics）結果或一認知性分析（Cognitive analytics）結果為該特徵辨識結果，進而傳輸該特徵辨識結果至該終端裝置來執行該保護操作。

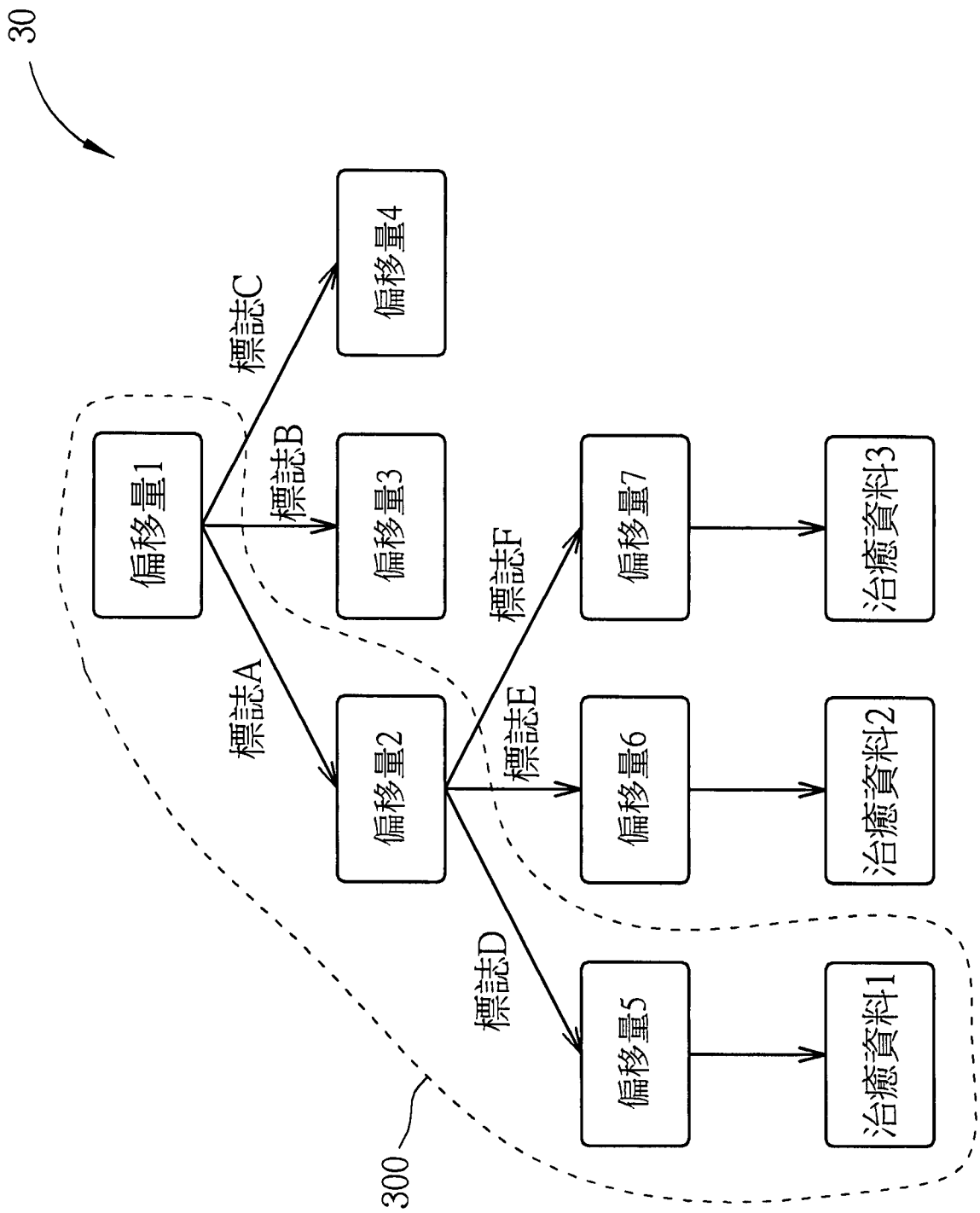
圖式



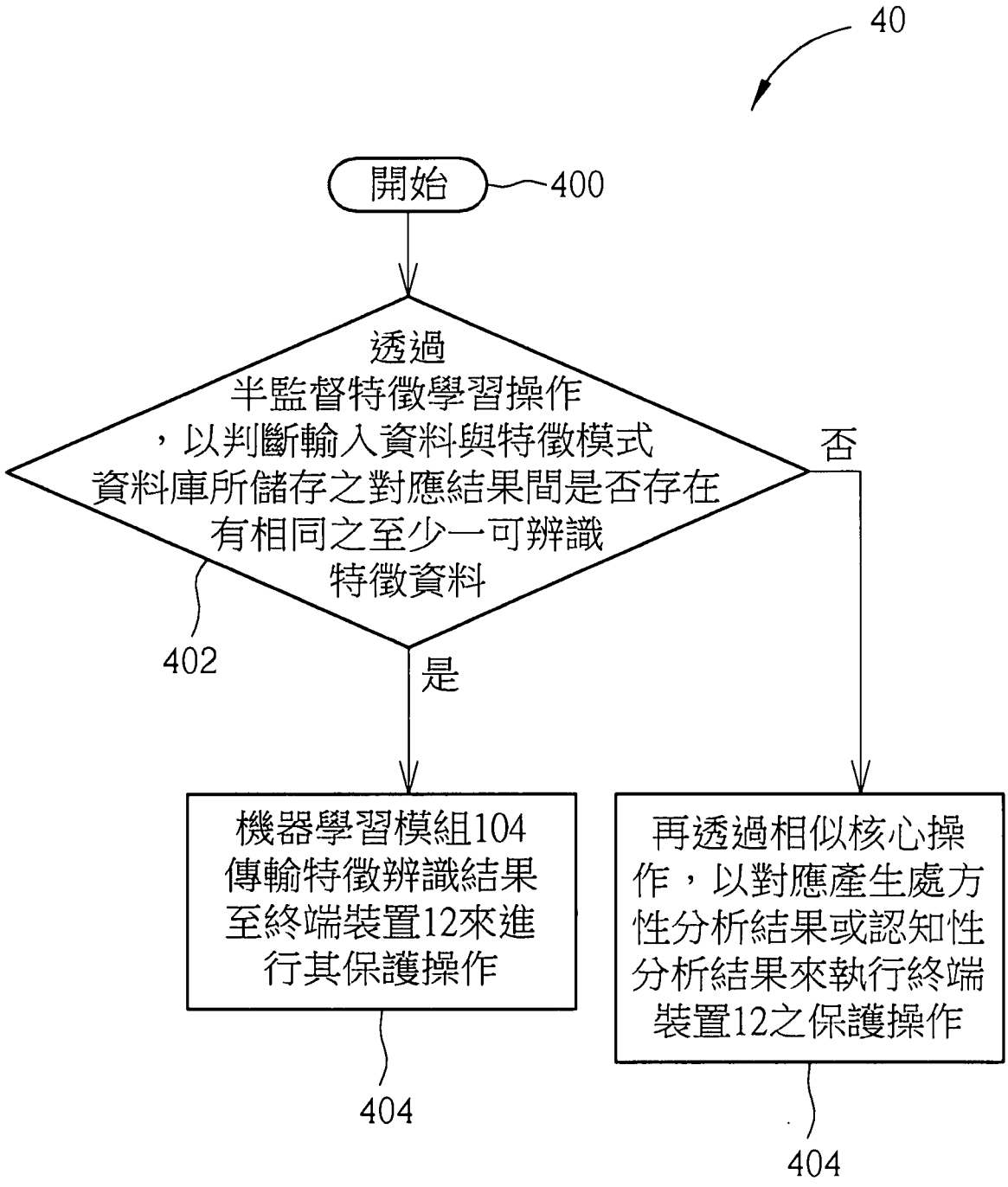
第1圖


20
開始
200
電腦系統10接收一觀測資料
202
電腦系統10係根據轉導機器學習，轉換觀測資料為一第一對應資料
204
電腦系統10係根據引導機器學習，切分第一對應資料為一第二對應資料，並提供第二對應資料至機器學習模組104
206
機器學習模組104接收一輸入資料，且根據一特徵模式資料庫處理接收資料，以產生一特徵辨識結果
208
傳輸特徵辨識結果至終端裝置12
210
結束
212

第2圖


30
偏移量1
標誌A
偏移量2
標誌B
偏移量3
標誌C
偏移量4
標誌D
偏移量5
標誌E
偏移量6
標誌F
偏移量7
治癒資料1
治癒資料2
治癒資料3
300

第3圖


40
開始
400
透過
半監督特徵學習操作
，以判斷輸入資料與特徵模式
資料庫所儲存之對應結果間是否存在
有相同之至少一可辨識
特徵資料
否
402
是
機器學習模組104
傳輸特徵辨識結果
至終端裝置12來進
行其保護操作
再透過相似核心操
作，以對應產生處方
性分析結果或認知性
分析結果來執行終端
裝置12之保護操作
404
404

第4圖

G_1
Ob_1
Ob_2
Ob_3
群組資料
對應
V_1
轉導機器學習
對應
對應
對應
V_1_1
V_1_2
V_1_3
V_1
G_1
Ob_1
Ob_2
Ob_3
群組資料
引導機器學習

第5圖