I883754

(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 I883754 B**

(45)公告日： 中華民國 114 (2025) 年 05 月 11 日

(21)申請案號：112151677 (22)申請日： 中華民國 112 (2023) 年 12 月 29 日

(51)Int. Cl.： ***H04L41/16 (2022.01)*** ***H04L43/16 (2022.01)***
H04L43/0876(2022.01) ***H04L41/28 (2022.01)***
H04L47/20 (2022.01)

(71)申請人：中華電信股份有限公司 (中華民國) CHUNGHWA TELECOM CO., LTD. (TW)
臺北市中正區信義路 1 段 21 之 3 號

(72)發明人：黃翰暉 HUANG, HAHN HUEI (TW)

(74)代理人：林長榮

(56)參考文獻：

TW	201036399A	US	2021/0105302A1
US	2021/0264004A1	US	2022/0263846A1
US	2023/0412640A1		

審查人員：謝紀明

申請專利範圍項數：11 項 圖式數：2 共 28 頁

(54)名稱

以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介

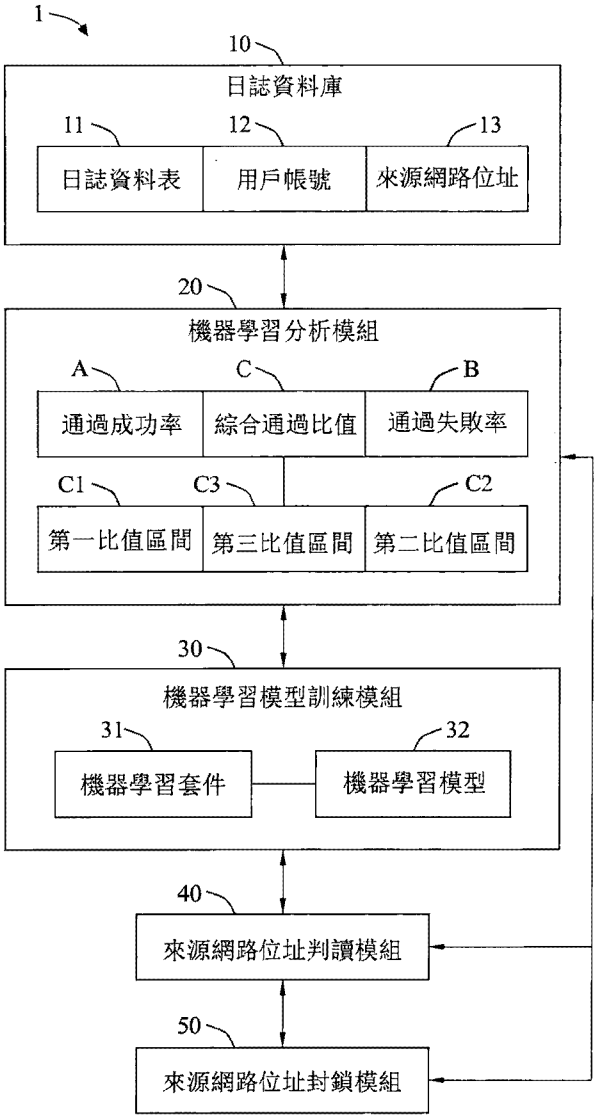
(57)摘要

本發明揭露一種以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介，係於同一用戶帳號之來源網路位址在一定時間區間內所嘗試之登入次數超過次數門檻值時，由機器學習分析模組分析用戶帳號之來源網路位址之通過狀態分別為成功與失敗之次數，再依據成功之次數與失敗之次數分析出通過成功率與通過失敗率，俾依據通過成功率與通過失敗率分析出綜合通過比值。再者，當綜合通過比值落在第一比值區間或第二比值區間時，由機器學習分析模組判定為正常用戶帳號之來源網路位址，而當綜合通過比值落在第三比值區間時，由機器學習分析模組判定為異常用戶帳號之來源網路位址，俾由來源網路位址封鎖模組針對異常用戶帳號之來源網路位址進行封鎖。

The invention discloses a system, method and computer readable medium for analyzing and blocking abnormal source network address using machine learning. When number of login attempts from a source network address of a same user account exceeds a number threshold within a time period, a machine learning analysis module analyzes pass status of the source network address of the user account as the number of successes and failures, and then analyzes a pass success rate and a pass failure rate based on the number of successes and the number of failures, so as to analyze a comprehensive passing ratio based on the pass success rate and the pass failure rate. Furthermore, when the comprehensive passing ratio falls within a first ratio range or a second ratio range, the machine learning analysis module determines as the source network address of a normal user account, and when the comprehensive passing ratio falls within a third ratio range, the machine learning analysis module determines as the source network address of an abnormal user account, so as to allow a source network address blocking module to block the source network address of abnormal user accounts.

TW I883754 B

指定代表圖：



【圖 1】

符號簡單說明：

1:以機器學習分析與封鎖異常來源網路位址之系統

10:日誌資料庫

11:日誌資料表

12:用戶帳號

13:來源網路位址

20:機器學習分析模組

30:機器學習模型訓練模組

31:機器學習套件

32:機器學習模型

40:來源網路位址判讀模組

50:來源網路位址封鎖模組

A:通過成功率

B:通過失敗率

C:綜合通過比值

C1:第一比值區間

C2:第二比值區間

C3:第三比值區間

【發明摘要】

【中文發明名稱】 以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介

【英文發明名稱】 SYSTEM, METHOD AND COMPUTER READABLE MEDIUM FOR ANALYZING AND BLOCKING ABNORMAL SOURCE NETWORK ADDRESS USING MACHINE LEARNING

【中文】

本發明揭露一種以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介，係於同一用戶帳號之來源網路位址在一定時間區間內所嘗試之登入次數超過次數門檻值時，由機器學習分析模組分析用戶帳號之來源網路位址之通過狀態分別為成功與失敗之次數，再依據成功之次數與失敗之次數分析出通過成功率與通過失敗率，俾依據通過成功率與通過失敗率分析出綜合通過比值。再者，當綜合通過比值落在第一比值區間或第二比值區間時，由機器學習分析模組判定為正常用戶帳號之來源網路位址，而當綜合通過比值落在第三比值區間時，由機器學習分析模組判定為異常用戶帳號之來源網路位址，俾由來源網路位址封鎖模組針對異常用戶帳號之來源網路位址進行封鎖。

【英文】

The invention discloses a system, method and computer readable medium for analyzing and blocking abnormal source network address using machine learning. When number of login attempts from a source network address of a same user account exceeds a number threshold within a time period, a machine learning analysis module analyzes pass status of the source network address of the user account as the number of successes and failures, and then analyzes a pass success rate and a pass failure rate based on the number of successes and the number of failures, so as to analyze a comprehensive passing ratio based on the pass success rate and the pass failure rate. Furthermore, when the comprehensive passing ratio falls within a first ratio range or a second ratio range, the machine learning analysis module determines as the source network address of a normal user account, and when the comprehensive passing ratio falls within a third ratio range, the machine learning analysis module determines as the source network address of an abnormal user account, so as to allow a source network address blocking module to block the source network address of abnormal user accounts.

【指定代表圖】　圖1

【代表圖之符號簡單說明】

1:以機器學習分析與封鎖異常來源網路位址之系統

10:日誌資料庫

11:日誌資料表

12:用戶帳號

13:來源網路位址

20:機器學習分析模組

30:機器學習模型訓練模組

31:機器學習套件

32:機器學習模型

40:來源網路位址判讀模組

50:來源網路位址封鎖模組

A:通過成功率

B:通過失敗率

C:綜合通過比值

C1:第一比值區間

C2:第二比值區間

C3:第三比值區間

【特徵化學式】 無。

【發明說明書】

【中文發明名稱】 以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介

【英文發明名稱】 SYSTEM, METHOD AND COMPUTER READABLE MEDIUM FOR ANALYZING AND BLOCKING ABNORMAL SOURCE NETWORK ADDRESS USING MACHINE LEARNING

【技術領域】

【0001】本發明係關於一種異常來源網路位址(如來源 IP 位址)之分析與封鎖技術，特別是指一種以機器學習(Machine Learning)分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介。

【先前技術】

【0002】目前在各種系統(如會員帳號系統)、電子裝置、應用程式(APP)、網頁瀏覽器或帳號登入介面中，經常需要用戶輸入正確之用戶帳號、密碼或驗證碼(如一次性密碼 OTP)等資訊，才能有效登入各種系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面中，以進一步使用相關之服務或功能。

【0003】惟，用戶可能為會員(如個人/公司/學校用戶等)，亦有可能為駭客(如惡意攻擊者/帳號盜取者等)，若用戶無法一次輸入正確之用戶帳號、密碼或驗證碼時，則大多會嘗試多次輸入不同或曾經使用之用戶帳號、

密碼或驗證碼，以嘗試或企圖登入各種系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面。

【0004】再者，各種系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在判斷用戶帳號之來源網路位址(如來源 IP 位址)時，通常難以有效區分用戶帳號之來源網路位址為正常用戶帳號(如會員/公司/學校用戶帳號)之來源網路位址或異常用戶帳號(如駭客用戶帳號)之來源網路位址，導致不易對異常用戶帳號之來源網路位址進行有效之防範措施。

【0005】現有技術之解決方式為同一用戶帳號之來源網路位址(如來源 IP 位址)針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間(如 5 分鐘)內所嘗試之登入次數超過次數門檻值(如 3 次或 10 次)後，便直接將此用戶帳號之來源網路位址進行封鎖。

【0006】然而，此種解決方式會造成若是用戶(如公司用戶)有使用網路代理(proxy)，且同時有用戶以多次嘗試錯誤來企圖登入各種系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面時，有可能將正常用戶帳號之來源網路位址誤判為異常用戶帳號之來源網路位址，導致錯誤地將正常用戶帳號之來源網路位址進行封鎖，從而造成用戶(如公司用戶)之不必要客訴。

【0007】因此，如何提供一種創新之異常來源網路位址(如來源 IP 位址)之分析與封鎖技術，以解決上述之任一問題並提供相關之系統或方法，已成為本領域技術人員之一大研究課題。

【發明內容】

【0008】本發明所述以機器學習分析與封鎖異常來源網路位址之系統包括：一機器學習分析模組，係於同一用戶帳號之來源網路位址針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由機器學習分析模組分析用戶帳號之來源網路位址之通過狀態分別為或以統計出成功與失敗之次數，再由機器學習分析模組依據成功之次數與失敗之次數分析出用戶帳號之來源網路位址之通過成功率與通過失敗率，俾由機器學習分析模組依據用戶帳號之來源網路位址之通過成功率與通過失敗率分析出用戶帳號之來源網路位址之綜合通過比值；以及一來源網路位址封鎖模組，係通訊連結機器學習分析模組；其中，當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在一第一比值區間或大於第一比值區間之一第二比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為正常用戶帳號之來源網路位址，而當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在第一比值區間與第二比值區間之間的一第三比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為異常用戶帳號之來源網路位址，俾由來源網路位址封鎖模組針對機器學習分析模組所判定之異常用戶帳號之來源網路位址進行封鎖。

【0009】本發明所述以機器學習分析與封鎖異常來源網路位址之方法，係由電腦或伺服器所執行，該方法包括：當同一用戶帳號之來源網路位址針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由一機器學習分析模組分析用戶帳號之來源網路位址之通過狀態分別為或以統計出成功與失

敗之次數，再由機器學習分析模組依據成功之次數與失敗之次數分析出用戶帳號之來源網路位址之通過成功率與通過失敗率，俾由機器學習分析模組依據用戶帳號之來源網路位址之通過成功率與通過失敗率分析出用戶帳號之來源網路位址之綜合通過比值；以及當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在一第一比值區間或大於第一比值區間之一第二比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為正常用戶帳號之來源網路位址，而當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在第一比值區間與第二比值區間之間的一第三比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為異常用戶帳號之來源網路位址，俾由一來源網路位址封鎖模組針對機器學習分析模組所判定之異常用戶帳號之來源網路位址進行封鎖。

【0010】本發明之電腦可讀媒介應用於計算裝置或電腦中，係儲存有指令，以執行上述以機器學習分析與封鎖異常來源網路位址之方法。

【0011】因此，本發明提供一種創新之以機器學習分析與封鎖異常來源網路位址之系統、方法及電腦可讀媒介，係能由機器學習分析模組採用「綜合通過比值」來判斷用戶帳號之來源網路位址為正常用戶帳號或異常用戶帳號之來源網路位址，以利快速得到較高的判斷精準度或正確性，俾使機器學習分析模組大幅降低對於正常用戶帳號或異常用戶帳號之來源網路位址之誤判機率。

【0012】或者，本發明之機器學習分析模組能自動地分析正常用戶帳號之來源網路位址之行為(如正常登入/驗證行為)與異常用戶帳號之來源網路位址之行為(如異常登入/嘗試行為)，亦能針對正常用戶帳號之來源網

路位址與異常用戶帳號之來源網路位址兩者之綜合通過比值進行比較或判讀，也能由機器學習分析模組有效地分辨正常用戶帳號之來源網路位址與異常用戶帳號之來源網路位址兩者之差異，有利於更精準地判斷正常用戶帳號(如一般用戶帳號)與異常用戶帳號(如大量攻擊/駭客用戶帳號)之行為。

【0013】亦或者，本發明之機器學習分析模組能分析或判斷異常用戶帳號(如可疑用戶帳號)之來源網路位址，以由來源網路位址封鎖模組針對異常用戶帳號之來源網路位址進行封鎖，藉此強化各種系統、電子裝置、應用程式(APP)、網頁瀏覽器或帳號登入介面等之資安防護力，亦能減少不必要之客訴產生，也能增加客戶之信賴度。

【0014】又或者，本發明可以具有[1]分辨能力：機器學習分析模組能依據綜合通過比值有效地分辨正常用戶帳號之來源網路位址與異常用戶帳號之來源網路位址兩者之差異。[2]即時性：毋須以人工方式辨別大量攻擊之異常用戶帳號之來源網路位址(如來源 IP 位址)，且每日全時(如 24 小時)皆能運作。[3]安全性：能安全保護各種系統(如會員帳號系統)之帳戶安全。[4]防護力：來源網路位址封鎖模組能針對暴力破解或異常攻擊之異常用戶帳號之來源網路位址(如來源 IP 位址)進行有效封鎖及防護。

【0015】為使本發明之上述特徵與優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明。在以下描述內容中將部分闡述本發明之額外特徵及優點，且此等特徵及優點將部分自所述描述內容可得而知，或可藉由對本發明之實踐習得。應理解，前文一般描述與以下詳細描述二者均為例示性及解釋性的，且不欲約束本發明所欲主張之範圍。

【圖式簡單說明】

【0016】圖 1 為本發明所述以機器學習分析與封鎖異常來源網路位址之系統之架構示意圖。

【0017】圖 2 為本發明所述以機器學習分析與封鎖異常來源網路位址之方法之流程示意圖。

【實施方式】

【0018】以下藉由特定的具體實施形態說明本發明之實施方式，熟悉此技術之人士可由本說明書所揭示之內容瞭解本發明之其他優點與功效，亦可因而藉由其他不同具體等同實施形態加以施行或運用。

【0019】圖 1 為本發明所述以機器學習分析與封鎖異常來源網路位址之系統 1 之架構示意圖。如圖 1 所示，以機器學習分析與封鎖異常來源網路位址之系統 1 可包括互相通訊連結之一日誌資料庫 10、一機器學習分析模組 20、一機器學習模型訓練模組 30、一來源網路位址判讀模組 40 以及一來源網路位址封鎖模組 50 等。日誌資料庫 10 可具有至少一(如複數)日誌資料表 11，且機器學習模型訓練模組 30 可具有一機器學習套件 31(如 python sklearn 套件)與一機器學習模型 32 等。

【0020】在一實施例中，機器學習分析模組 20 可分別通訊連結日誌資料庫 10、機器學習模型訓練模組 30、來源網路位址判讀模組 40 與來源網路位址封鎖模組 50，且來源網路位址判讀模組 40 亦可進一步通訊連結機器學習模型訓練模組 30 與來源網路位址封鎖模組 50。

【0021】在一實施例中，日誌資料庫 10 可為日誌資料儲存器、日誌資料伺服器、日誌資料硬碟等，機器學習分析模組 20 可為機器學習分析器(晶片/電路)、機器學習分析軟體(程式)等。機器學習模型訓練模組 30 可為機器學習模型訓練器(晶片/電路)、機器學習模型訓練軟體(程式)等，機器學習套件 31 可為機器學習軟體或機器學習應用程式(APP)等。來源網路位址判讀模組 40 可為來源網路位址判讀器(晶片/電路)、來源網路位址判讀軟體(程式)等，來源網路位址封鎖模組 50 可為來源網路位址封鎖器(晶片/電路)、來源網路位址封鎖軟體(程式)等。

【0022】本發明所述「至少一」代表一個以上(如一、二或三個以上)，「複數」代表二個以上(如二、三、四、十或百個以上)，「通訊連結」代表透過資料、訊號、電性、有線方式(如有線網路)或無線方式(如無線網路)等各種形式互相通訊或連結。「用戶帳號」可能為正常用戶帳號或異常用戶帳號，「網路位址」可為 IP(網際網路協定; Internet Protocol)位址，「來源網路位址」可為來源 IP 位址等，「一定時間區間」可為預定或設定之時間區間(如 5 分鐘、1 小時、1 日等)，「次數門檻值」可為預定或設定之次數(如 5 次、20 次、100 次等)。但是，本發明並不以各實施例所提及者為限。

【0023】首先，日誌資料庫 10 可具有至少一(如複數)日誌資料表 11 以記錄有關用戶帳號 12 之來源網路位址 13 與登入資訊(使用行為)之日誌(log)資料，且用戶帳號 12 之登入資訊可包括用戶帳號 12 之來源網路位址 13 之通過狀態(如帳號登入狀態)為成功(如登入成功)或失敗(如登入失敗)等資訊。

【0024】其次，機器學習分析模組 20 可統整(如統計/整合/分析)日誌資料庫 10 之日誌資料表 11 所記錄之日誌資料以取得用戶帳號 12(如可疑用戶帳號)之來源網路位址 13 之登入資訊(使用行為)，且機器學習分析模組 20 亦能以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之通過成功率 A(如登入成功率)與通過失敗率 B(如登入失敗率)。

【0025】舉例而言，日誌資料庫 10 之日誌資料表 11 中之通過狀態(status)或狀態欄位，可以記錄用戶帳號 12 之來源網路位址 13(如來源 IP 位址)每次之通過狀態(登入結果)為成功(如登入成功)或失敗(如登入失敗)之資訊。當機器學習分析模組 20 分析出同一用戶帳號 12 之來源網路位址 13 針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面等，在一定時間區間(如 5 分鐘)內所嘗試之登入次數超過次數門檻值(如 100 次)時，由機器學習分析模組 20 以機器學習技術或機器學習方式分析(計算)日誌資料庫 10 之日誌資料表 11 中有關用戶帳號 12 之來源網路位址 13 之通過狀態(status)或狀態欄位分別為成功(success)之次數與失敗(fail)之次數，再由機器學習分析模組 20 以機器學習技術或機器學習方式依據成功之次數與失敗之次數分析(計算)出用戶帳號 12 之來源網路位址 13 之[1]通過成功率 A 與[2]通過失敗率 B，俾由機器學習分析模組 20 依據通過成功率 A 與通過失敗率 B 分析(計算)出用戶帳號 12 之來源網路位址 13 之[3]綜合通過比值 C。

【0026】在一實施例中，前述系統可為會員帳號系統、帳號登入系統或其他系統，電子裝置可為電腦、智慧型手機或其他電子裝置，應用程式

可為帳號登入軟體、帳號登入程式、應用軟體或其他應用程式，但不以此為限。

【0027】[1]通過成功率 A：機器學習分析模組 20 能以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之通過成功率 A 等於「日誌資料庫 10 之日誌資料表 11 中有關用戶帳號 12 之來源網路位址 13 之通過狀態(status)或狀態欄位為成功(success)之次數除以一定時間區間之次數門檻值再乘以 100%」，亦即通過成功率=成功之次數/一定時間區間之次數門檻值*100%。

【0028】[2]通過失敗率 B：機器學習分析模組 20 能以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之通過失敗率 B 等於「日誌資料庫 10 之日誌資料表 11 中有關用戶帳號 12 之來源網路位址 13 之通過狀態(status)或狀態欄位為失敗(fail)之次數除以一定時間區間之次數門檻值再乘以 100%」，亦即通過失敗率=通過失敗之次數/一定時間區間之次數門檻值*100%。

【0029】[3]綜合通過比值 C：機器學習分析模組 20 可先比較用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之通過成功率 A 與通過失敗率 B 兩者之大小，再由機器學習分析模組 20 以機器學習技術或機器學習方式依據通過成功率 A 與通過失敗率 B 兩者之大小比較結果分析(計算)出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C：(1)等於較小之通過失敗率 B 除以較大之通過成功率 A、(2)或者等於較小之通過成功率 A 除以較大之通過失敗率 B、(3)或者等於相同之通過成功率 A 除以通過失敗率 B，俾使用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 介於 0 至 1 之間。亦即，

綜合通過比值=(1)較小之通過失敗率/較大之通過成功率、(2)或者較小之通過成功率/較大之通過失敗率、(3)或者相同之通過成功率/通過失敗率，以使綜合通過比值=0-1。

【0030】當機器學習分析模組 20 分析(計算)出用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之綜合通過比值 C 落在一第一比值區間 C1(如 0-0.33)或大於第一比值區間 C1 之一第二比值區間 C2(如 0.67-1)時，機器學習分析模組 20 可初步判定用戶帳號 12 之來源網路位址 13 為正常用戶帳號之來源網路位址 13。

【0031】當機器學習分析模組 20 以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之綜合通過比值 C 落在第一比值區間 C1(如 0-0.33)與第二比值區間 C2(如 0.67-1)之間的一第三比值區間 C3(如 0.34-0.66)時，機器學習分析模組 20 可初步判定用戶帳號 12 之來源網路位址 13 為異常用戶帳號之來源網路位址 13。

【0032】在一實施例中，綜合通過比值 C 可為 0 至 1 之間，第一比值區間 C1 可為 0 至 0.33 之間，第二比值區間 C2 可為 0.67 至 1 之間，而第三比值區間 C3 可為 0.34 至 0.66 之間，但不以此為限。此外，上述比值區間可依不同系統、電子裝置、應用程式而變動，亦可透過機器學習分析模組 20 分析後產生上述比值區間。

【0033】[1]正常用戶帳號之來源網路位址 13：在本實施例中，例如機器學習分析模組 20 以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13 之通過成功率 A 等於 80%至 100%之任一者(如 80%)且通過失敗率 B 等於 0%至 20%之任一者(如 20%)，則機器學習分析

模組 20 可比較出用戶帳號 12 之來源網路位址 13 之通過失敗率 B(如 20%)小於通過成功率 A(如 80%)。因此，機器學習分析模組 20 可分析(計算)出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 為較小之通過失敗率 B(如 20%)除以較大之通過成功率 A(如 80%)等於 0.25，即綜合通過比值 C = 20% / 80% = 0.25，故機器學習分析模組 20 能以機器學習技術或機器學習方式分析(計算)出綜合通過比值 C(如 0.25)落在第一比值區間 C1(如 0-0.33)，以由機器學習分析模組 20 依據落在第一比值區間 C1 之綜合通過比值 C 初步判定用戶帳號 12 之來源網路位址 13 為正常用戶帳號之來源網路位址 13。

【0034】[2]異常用戶帳號之來源網路位址 13：在本實施例中，例如機器學習分析模組 20 分析(計算)出用戶帳號 12 之來源網路位址 13 之通過成功率 A 等於 30%至 40%之任一者(如 30%)且通過失敗率 B 等於 60%至 70%之任一者(如 70%)，則機器學習分析模組 20 可比較出用戶帳號 12 之來源網路位址 13 之通過成功率 A(如 30%)小於通過失敗率 B(如 70%)。因此，機器學習分析模組 20 可分析(計算)出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 為較小之通過成功率 A(如 30%)除以較大之通過失敗率 B(如 70%)等於 0.43，即綜合通過比值 C = 30% / 70% = 0.43，故機器學習分析模組 20 可分析(計算)出綜合通過比值 C(如 0.43)落在第三比值區間 C3(如 0.34-0.66)，以由機器學習分析模組 20 依據落在第三比值區間 C3 之綜合通過比值 C 初步判定用戶帳號 12 之來源網路位址 13 為異常用戶帳號之來源網路位址 13。

【0035】再者，機器學習模型訓練模組 30 可將機器學習分析模組 20

所初步判定之正常用戶帳號之來源網路位址 13(如來源 IP 位址)與異常用戶帳號之來源網路位址 13(如來源 IP 位址)進行統整，以由機器學習模型訓練模組 30 使用機器學習套件 31(如 python sklearn 套件)對機器學習分析模組 20 所初步判定之正常用戶帳號之來源網路位址 13 與異常用戶帳號之來源網路位址 13 進行線性回歸(Linear Regression)處理，且由機器學習模型訓練模組 30 將正常用戶帳號與異常用戶帳號兩者之來源網路位址 13 之通過成功率 A、通過失敗率 B 及相關聯之損失函數(Loss Function)與擬合函數(Fitting Function)等各種資訊導入機器學習套件 31 中，再由機器學習模型訓練模組 30 之機器學習套件 31 利用正常用戶帳號與異常用戶帳號兩者之來源網路位址 13 之通過成功率 A、通過失敗率 B 及相關聯之損失函數與擬合函數等各種資訊訓練機器學習模型 32，俾供機器學習模型訓練模組 30 之機器學習模型 32 能依據正常用戶帳號與異常用戶帳號兩者之來源網路位址 13 之通過成功率 A、通過失敗率 B 及相關聯之損失函數與擬合函數等各種資訊較精準或正確地輸出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C。

【0036】另外，來源網路位址判讀模組 40 可利用機器學習分析模組 20 或機器學習模型訓練模組 30 之機器學習模型 32 所分析或輸出之用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 落在第一比值區間 C1(如 0-0.33)或第二比值區間 C2(如 0.67-1)時，由來源網路位址判讀模組 40 最終判定或再次確認用戶帳號 12 之來源網路位址 13 為正常用戶帳號之來源網路位址 13，亦可利用機器學習分析模組 20 或機器學習模型訓練模組 30 之機器學習模型 32 所分析或輸出之用戶帳號 12 之來源網路位址 13 之綜

合通過比值 C 落在第三比值區間 C3(如 0.34-0.66)時，由來源網路位址判讀模組 40 最終判定或再次確認用戶帳號 12 之來源網路位址 13 為異常用戶帳號之來源網路位址 13。

【0037】最後，來源網路位址封鎖模組 50 可針對機器學習分析模組 20 或來源網路位址判讀模組 40 所判定之異常用戶帳號之來源網路位址 13 進行封鎖(如拒絕登入/限制存取權限/放入黑名單)，以強化系統之資安防護力，並減少不必要之客訴產生及增加客戶之信賴度。

【0038】圖 2 為本發明所述以機器學習分析與封鎖異常來源網路位址之方法之流程示意圖，並參閱圖 1 一併說明。同時，以機器學習分析與封鎖異常來源網路位址之方法主要包括下列步驟 S1 至步驟 S2 之技術內容，其餘內容相同於上述圖 1 之詳細說明，於此不再重覆敘述。

【0039】在步驟 S1 中，當同一用戶帳號 12 之來源網路位址 13 針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由機器學習分析模組 20 分析用戶帳號 12 之來源網路位址 13 之通過狀態分別為或以統計出成功與失敗之次數，再由機器學習分析模組 20 依據成功之次數與失敗之次數分析出用戶帳號 12 之來源網路位址 13 之通過成功率 A 與通過失敗率 B，俾由機器學習分析模組 20 依據用戶帳號 12 之來源網路位址 13 之通過成功率 A 與通過失敗率 B 分析出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C。

【0040】在步驟 S2 中，當機器學習分析模組 20 分析出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 落在一第一比值區間 C1 或大於第一比值區間 C1 之一第二比值區間 C2 時，由機器學習分析模組 20 初步判定

用戶帳號 12 之來源網路位址 13 為正常用戶帳號之來源網路位址 13，而當機器學習分析模組 20 分析出用戶帳號 12 之來源網路位址 13 之綜合通過比值 C 落在第一比值區間 C1 與第二比值區間 C2 之間的一第三比值區間 C3 時，由機器學習分析模組 20 初步判定用戶帳號 12 之來源網路位址 13 為異常用戶帳號之來源網路位址 13，俾由來源網路位址封鎖模組 50 針對機器學習分析模組 20 所初步判定之異常用戶帳號之來源網路位址 13 進行封鎖(如拒絕登入/限制存取權限/放入黑名單)。

【0041】因此，倘若單純以「通過成功率 A」及/或「通過失敗率 B」來判斷用戶帳號 12 之來源網路位址 13 為正常用戶帳號或異常用戶帳號之來源網路位址 13，會導致得到較低的判斷精準度或正確性，從而大幅提高對於正常用戶帳號或異常用戶帳號之來源網路位址 13 之誤判機率。所以，本發明之機器學習分析模組 20 或來源網路位址判讀模組 40 採用「綜合通過比值 C」來判斷用戶帳號 12 之來源網路位址 13 為正常用戶帳號或異常用戶帳號之來源網路位址 13，以利得到較高的判斷精準度或正確性，俾使機器學習分析模組 20 或來源網路位址判讀模組 40 大幅降低對於正常用戶帳號或異常用戶帳號之來源網路位址 13 之誤判機率。

【0042】換言之，本發明並非單純只採用「通過成功率 A」及/或「通過失敗率 B」來判斷正常用戶帳號或異常用戶帳號之來源網路位址 13，而是採用「綜合通過比值 C」來判斷正常用戶帳號或異常用戶帳號之來源網路位址 13，故能將更多的日誌資料(可記錄用戶帳號 12 之來源網路位址 13 及相關之登入資訊)輸入機器學習模型訓練模組 30 之機器學習模型 32 中進行學習，以利機器學習模型訓練模組 30 所訓練出之機器學習模型 32 能具

有更高的判斷精準度或正確性，俾使來源網路位址判讀模組 40 能大幅降低對於正常用戶帳號或異常用戶帳號之來源網路位址 13 之誤判機率。

【0043】本發明之機器學習分析模組 20 能自動地分析正常用戶帳號之來源網路位址 13 之行為(如正常登入/驗證行為)與異常用戶帳號之來源網路位址 13 之行為(如異常登入/嘗試行為)，亦能針對正常用戶帳號之來源網路位址 13 與異常用戶帳號之來源網路位址 13 兩者之綜合通過比值 C 進行比較或判讀，也能由機器學習分析模組 20 有效地分辨正常用戶帳號之來源網路位址 13 與異常用戶帳號之來源網路位址 13 兩者之差異，有利於更精準地判斷正常用戶帳號(如一般用戶帳號)與異常用戶帳號(如大量攻擊/駭客用戶帳號)之行為。

【0044】本發明之機器學習分析模組 20 或來源網路位址判讀模組 40 能分析或判斷異常用戶帳號(如可疑用戶帳號)之來源網路位址 13，以由來源網路位址封鎖模組 50 針對異常用戶帳號之來源網路位址 13 進行封鎖(如拒絕登入/限制存取權限/放入黑名單)，藉此強化各種系統(如會員帳號系統)、電子裝置、應用程式(APP)、網頁瀏覽器或帳號登入介面等之資安防護力，亦能減少不必要之客訴產生，也能增加客戶之信賴度。

【0045】本發明之機器學習分析模組 20 能於每次驗證用戶帳號 12 時，以機器學習技術或機器學習方式分析(計算)出用戶帳號 12 之來源網路位址 13 之通過成功率 A(如登入成功率)與通過失敗率 B(如登入失敗率)，以由機器學習分析模組 20 依據用戶帳號 12 之來源網路位址 13 之通過成功率 A 與通過失敗率 B 分析(計算)出正常用戶帳號或異常用戶帳號之來源網路位址 13 之綜合通過比值 C，俾由機器學習模型訓練模組 30 之機器學

習模型 32 以機器學習技術或機器學習方式有效率地學習正常用戶帳號與異常用戶帳號之來源網路位址 13 兩者之綜合通過比值 C 之差異。

【0046】本發明之機器學習分析模組 20、機器學習模型訓練模組 30 之機器學習模型 32 或來源網路位址判讀模組 40 能有效區分大量登入之正常用戶帳號(如個人/公司/行號/學校之用戶帳號)之來源網路位址 13 與異常用戶帳號(如駭客/暴力破解之用戶帳號)之來源網路位址 13，亦能解決難以採用人工方式分辨用戶帳號 12 之來源網路位址 13(如來源 IP 位址)之問題。

【0047】本發明至少具有下列優點：

【0048】[1]快速分辨能力：機器學習分析模組 20 能依據綜合通過比值 C 快速且有效地分辨正常用戶帳號之來源網路位址 13 與異常用戶帳號之來源網路位址 13 兩者之差異。

【0049】[2]即時性：毋須以人工方式辨別大量攻擊之異常用戶帳號之來源網路位址 13(如來源 IP 位址)，且每日全時(如 24 小時)皆能運作。

【0050】[3]安全性：能安全保護各種系統(如會員帳號系統)之帳戶安全。

【0051】[4]防護力：來源網路位址封鎖模組 50 能針對暴力破解或異常攻擊之異常用戶帳號之來源網路位址 13(如來源 IP 位址)進行有效封鎖及防護。

【0052】此外，本發明還提供一種針對以機器學習分析與封鎖異常來源網路位址之方法之電腦可讀媒介，係應用於具有處理器與記憶體之計算裝置或電腦中，且電腦可讀媒介儲存有指令，並可利用計算裝置或電腦透

過處理器與記憶體執行電腦可讀媒介，以於執行電腦可讀媒介時執行上述內容。在另一實施例中，此電腦可讀媒介係非暫時性(non-transitory)之電腦可讀儲存媒介。

【0053】在一實施例中，處理器可為中央處理器(CPU)、圖形處理器(GPU)、微處理器(MPU)、微控制器(MCU)、人工智慧(AI)處理器等，記憶體可為隨機存取記憶體(RAM)、唯讀記憶體(ROM)、快閃(Flash)記憶體、記憶卡、硬碟(如雲端/網路/外接式硬碟)、光碟、隨身碟、資料庫等，且計算裝置或電腦可為計算機、智慧型手機、平板電腦、個人電腦、筆記型電腦、桌上型電腦、伺服器(如雲端/遠端/網路伺服器)等。在另一實施例中，上述模組均可為軟體、硬體或韌體；若為硬體，則可為具有資料處理與運算能力之處理單元、處理器、或電腦主機；若為軟體或韌體，則可包括處理單元、處理器、電腦或電腦主機可執行之指令，且可安裝於同一硬體裝置或分布於不同的複數硬體裝置。

【0054】上述實施形態僅例示性說明本發明之原理、特點及其功效，並非用以限制本發明之可實施範疇，任何熟習此項技藝之人士均能在不違背本發明之精神及範疇下，對上述實施形態進行修飾與改變。任何使用本發明所揭示內容而完成之等效改變及修飾，均仍應為申請專利範圍所涵蓋。因此，本發明之權利保護範圍應如申請專利範圍所列。

【符號說明】

【0055】

1:以機器學習分析與封鎖異常來源網路位址之系統

10:日誌資料庫

11:日誌資料表

12:用戶帳號

13:來源網路位址

20:機器學習分析模組

30:機器學習模型訓練模組

31:機器學習套件

32:機器學習模型

40:來源網路位址判讀模組

50:來源網路位址封鎖模組

A:通過成功率

B:通過失敗率

C:綜合通過比值

C1:第一比值區間

C2:第二比值區間

C3:第三比值區間

S1 至 S2:步驟

第 112151677 號專利申請案
114 年 2 月 17 日修正替換頁

【發明申請專利範圍】

【請求項1】一種以機器學習分析與封鎖異常來源網路位址之系統，包括：

一機器學習分析模組，係於同一用戶帳號之來源網路位址針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由該機器學習分析模組分析該用戶帳號之來源網路位址之通過狀態分別為或以統計出成功與失敗之次數，再由該機器學習分析模組依據該成功之次數與該失敗之次數分析出該用戶帳號之來源網路位址之通過成功率與通過失敗率，俾依據該用戶帳號之來源網路位址之通過成功率與通過失敗率分析出該用戶帳號之來源網路位址之綜合通過比值；以及

一來源網路位址封鎖模組，係通訊連結該機器學習分析模組；

其中，當該機器學習分析模組分析出該用戶帳號之來源網路位址之該綜合通過比值落在一第一比值區間或大於該第一比值區間之一第二比值區間時，由該機器學習分析模組判定該用戶帳號之來源網路位址為正常用戶帳號之來源網路位址，而當該機器學習分析模組分析出該用戶帳號之來源網路位址之該綜合通過比值落在該第一比值區間與該第二比值區間之間的一第三比值區間時，由該機器學習分析模組判定該用戶帳號之來源網路位址為異常用戶帳號之來源網路位址，俾由該來源網路位址封鎖模組針對該機器學習分析模組所判定之該異常用戶帳號之來源網路位址進行封鎖。

【請求項2】如請求項 1 所述之系統，其中，該機器學習分析模組係利用機器學習分析出該用戶帳號之來源網路位址之通過成功率等於該用戶帳

號之來源網路位址之通過狀態為該成功之次數除以一定時間區間之次數門檻值再乘以 100%，且利用該機器學習分析出該用戶帳號之來源網路位址之通過失敗率等於該用戶帳號之來源網路位址之通過狀態為該失敗之次數除以該一定時間區間之次數門檻值再乘以 100%。

【請求項3】如請求項 1 所述之系統，其中，該機器學習分析模組係比較該用戶帳號之來源網路位址之通過成功率與通過失敗率，再由該機器學習分析模組依據該通過成功率與該通過失敗率之比較結果分析出該用戶帳號之來源網路位址之綜合通過比值等於較小之通過失敗率除以較大之通過成功率、或者等於較小之通過成功率除以較大之通過失敗率、或者等於相同之通過成功率除以通過失敗率，俾使該用戶帳號之來源網路位址之綜合通過比值介於 0 至 1 之間。

【請求項4】如請求項 1 所述之系統，更包括一具有機器學習套件與機器學習模型之機器學習模型訓練模組，係使用該機器學習套件對該機器學習分析模組所判定之該正常用戶帳號之來源網路位址與該異常用戶帳號之來源網路位址進行線性回歸處理，且由該機器學習模型訓練模組將該正常用戶帳號與該異常用戶帳號兩者之來源網路位址之通過成功率、通過失敗率及相關聯之損失函數與擬合函數導入該機器學習套件中，俾由該機器學習套件利用該正常用戶帳號與該異常用戶帳號兩者之來源網路位址之通過成功率、通過失敗率及相關聯之損失函數與擬合函數訓練該機器學習模型。

【請求項5】如請求項 1 所述之系統，更包括一具有機器學習模型之機器學習模型訓練模組與一來源網路位址判讀模組，其中，當該機器學習模型訓練模組之該機器學習模型所輸出之該用戶帳號之來源網路位址之綜合

通過比值落在該第一比值區間或該第二比值區間時，由該來源網路位址判讀模組最終判定或再次確認該用戶帳號之來源網路位址為該正常用戶帳號之來源網路位址，而當該機器學習模型訓練模組之該機器學習模型所輸出之該用戶帳號之來源網路位址之綜合通過比值落在該第三比值區間時，由該來源網路位址判讀模組最終判定或再次確認該用戶帳號之來源網路位址為該異常用戶帳號之來源網路位址。

【請求項6】一種以機器學習分析與封鎖異常來源網路位址之方法，包括：

當同一用戶帳號之來源網路位址針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由一機器學習分析模組分析該用戶帳號之來源網路位址之通過狀態分別為或以統計出成功與失敗之次數，再由該機器學習分析模組依據該成功之次數與該失敗之次數分析出該用戶帳號之來源網路位址之通過成功率與通過失敗率，俾由該機器學習分析模組依據該用戶帳號之來源網路位址之通過成功率與通過失敗率分析出該用戶帳號之來源網路位址之綜合通過比值；以及

當該機器學習分析模組分析出該用戶帳號之來源網路位址之該綜合通過比值落在一第一比值區間或大於該第一比值區間之一第二比值區間時，由該機器學習分析模組判定該用戶帳號之來源網路位址為正常用戶帳號之來源網路位址，而當該機器學習分析模組分析出該用戶帳號之來源網路位址之該綜合通過比值落在該第一比值區間與該第二比值區間之間的一第三比值區間時，由該機器學習分析模組判定該用戶帳號之來源網路位址為異

常用戶帳號之來源網路位址，俾由一來源網路位址封鎖模組針對該機器學習分析模組所判定之該異常用戶帳號之來源網路位址進行封鎖。

【請求項7】如請求項 6 所述之方法，更包括由該機器學習分析模組利用機器學習分析出該用戶帳號之來源網路位址之通過成功率等於該用戶帳號之來源網路位址之通過狀態為該成功之次數除以一定時間區間之次數門檻值再乘以 100%，且利用該機器學習分析出該用戶帳號之來源網路位址之通過失敗率等於該用戶帳號之來源網路位址之通過狀態為該失敗之次數除以該一定時間區間之次數門檻值再乘以 100%。

【請求項8】如請求項 6 所述之方法，更包括由該機器學習分析模組比較該用戶帳號之來源網路位址之通過成功率與通過失敗率，再由該機器學習分析模組依據該通過成功率與該通過失敗率之比較結果分析出該用戶帳號之來源網路位址之綜合通過比值等於較小之通過失敗率除以較大之通過成功率、或者等於較小之通過成功率除以較大之通過失敗率、或者等於相同之通過成功率除以通過失敗率，俾使該用戶帳號之來源網路位址之綜合通過比值介於 0 至 1 之間。

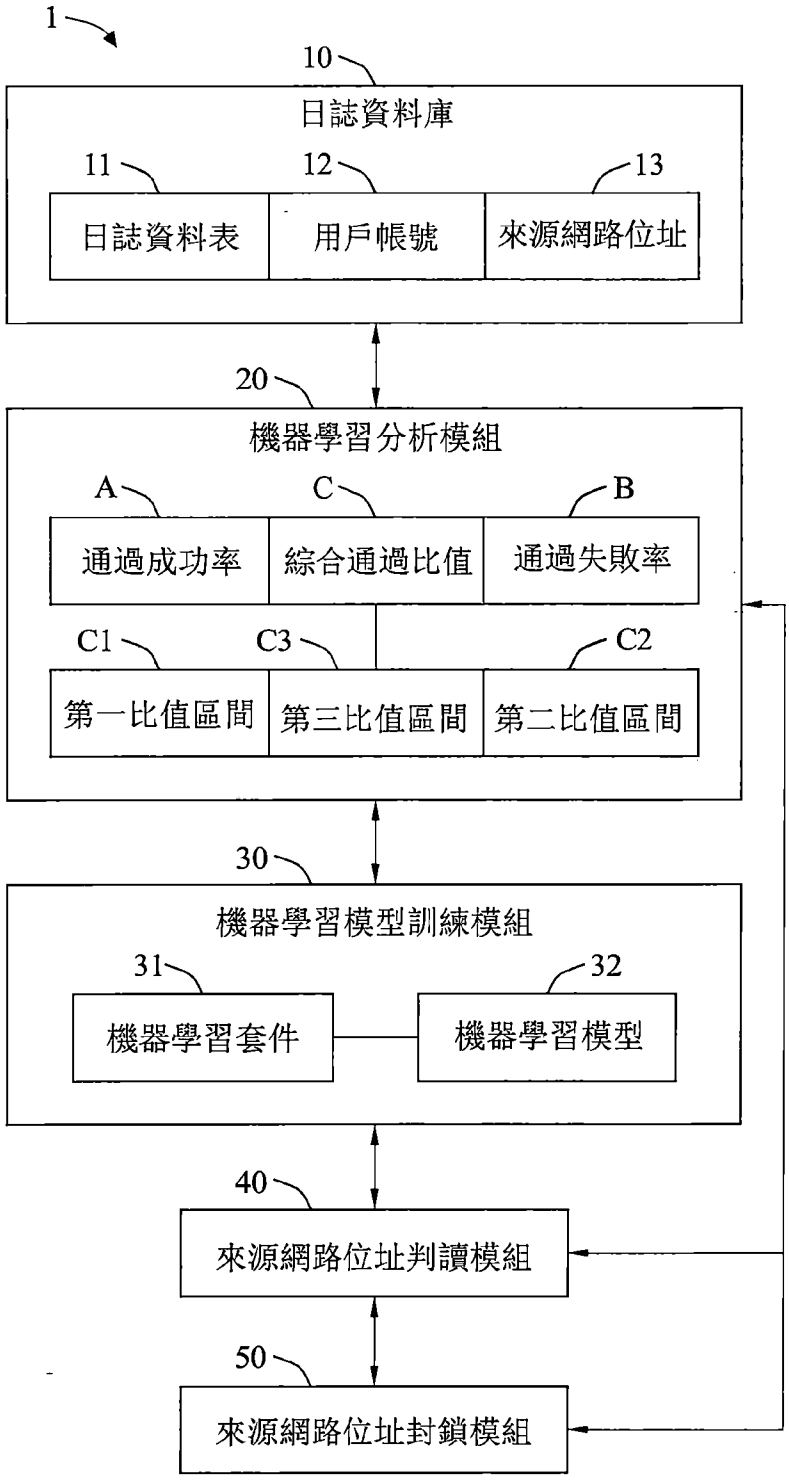
【請求項9】如請求項 6 所述之方法，更包括由一機器學習模型訓練模組使用機器學習套件對該機器學習分析模組所判定之該正常用戶帳號之來源網路位址與該異常用戶帳號之來源網路位址進行線性回歸處理，且由該機器學習模型訓練模組將該正常用戶帳號與該異常用戶帳號兩者之來源網路位址之通過成功率、通過失敗率及相關聯之損失函數與擬合函數導入該機器學習套件中，俾由該機器學習套件利用該正常用戶帳號與該異常用戶

帳號兩者之來源網路位址之通過成功率、通過失敗率及相關聯之損失函數與擬合函數訓練機器學習模型。

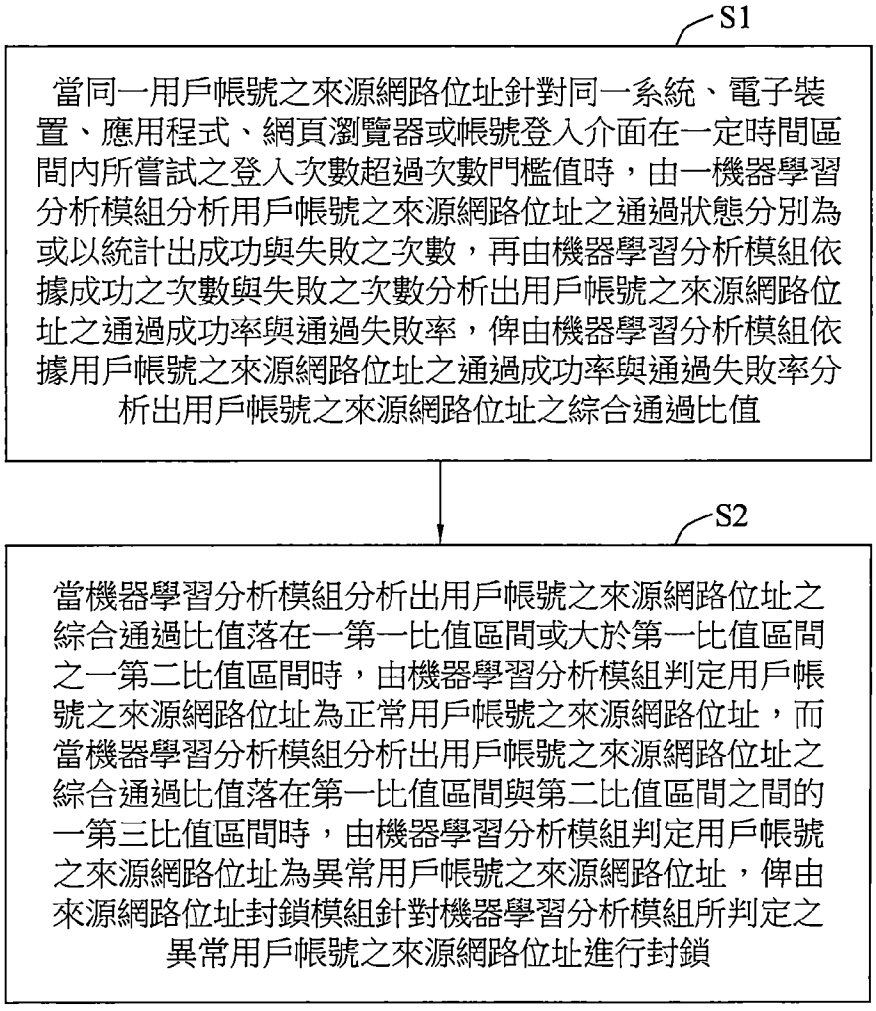
【請求項10】如請求項 6 所述之方法，更包括當一機器學習模型訓練模組之機器學習模型所輸出之該用戶帳號之來源網路位址之綜合通過比值落在該第一比值區間或該第二比值區間時，由一來源網路位址判讀模組最終判定或再次確認該用戶帳號之來源網路位址為該正常用戶帳號之來源網路位址，而當該機器學習模型訓練模組之該機器學習模型所輸出之該用戶帳號之來源網路位址之綜合通過比值落在該第三比值區間時，由該來源網路位址判讀模組最終判定或再次確認該用戶帳號之來源網路位址為該異常用戶帳號之來源網路位址。

【請求項11】一種電腦可讀媒介，應用於計算裝置或電腦中，係儲存有指令，以執行如請求項 6 至 10 之其中一者所述以機器學習分析與封鎖異常來源網路位址之方法。

【發明圖式】


1
10
日誌資料庫
11
日誌資料表
12
用戶帳號
13
來源網路位址
20
機器學習分析模組
A
通過成功率
C
綜合通過比值
B
通過失敗率
C1
第一比值區間
C3
第三比值區間
C2
第二比值區間
30
機器學習模型訓練模組
31
機器學習套件
32
機器學習模型
40
來源網路位址判讀模組
50
來源網路位址封鎖模組

【圖 1】


S1
當同一用戶帳號之來源網路位址針對同一系統、電子裝置、應用程式、網頁瀏覽器或帳號登入介面在一定時間區間內所嘗試之登入次數超過次數門檻值時，由一機器學習分析模組分析用戶帳號之來源網路位址之通過狀態分別為或以統計出成功與失敗之次數，再由機器學習分析模組依據成功之次數與失敗之次數分析出用戶帳號之來源網路位址之通過成功率與通過失敗率，俾由機器學習分析模組依據用戶帳號之來源網路位址之通過成功率與通過失敗率分析出用戶帳號之來源網路位址之綜合通過比值
S2
當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在一第一比值區間或大於第一比值區間之一第二比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為正常用戶帳號之來源網路位址，而當機器學習分析模組分析出用戶帳號之來源網路位址之綜合通過比值落在第一比值區間與第二比值區間之間的一第三比值區間時，由機器學習分析模組判定用戶帳號之來源網路位址為異常用戶帳號之來源網路位址，俾由來源網路位址封鎖模組針對機器學習分析模組所判定之異常用戶帳號之來源網路位址進行封鎖

【圖 2】