科技部補助專題研究計畫成果報告
期末報告

運用資訊融合與模型融合發展穩定高效能之電子商務詐騙偵測架構

計 畫 類 別 ： 個別型計畫
計 畫 編 號 ： MOST 105-2410-H-032-042-
執 行 期 間 ： 105年08月01日至106年07月31日
執 行 單 位 ： 淡江大學資訊管理學系

計 畫 主 持 人： 張昭憲

計畫參與人員： 碩士班研究生-兼任助理：周書任
碩士班研究生-兼任助理：李佳蓉
碩士班研究生-兼任助理：陳世軒

中 華 民 國 106 年 10 月 28 日

中 文 摘 要 ： 電子商務的蓬勃發展有目共睹，但也引起有心人士的注意，在各種交易平台中進行詐騙。由於網路的隱蔽性與便利性，讓這些不法行為在短期內便快速成長，若不加以抑制，將嚴重影響其未來發展。電子商務的詐騙偵測雖已獲得高度關注，亦有許多方法被提出，但仍面臨諸多挑戰。為此，本計畫運用資訊融合與模型融合概念，發展有效的預測方法，以提供更穩定、準確的偵測結果。有關資訊融合，本研究提出了一套動態資料融合方法，先將訓練集依照類別分成多個群聚，再根據待測帳號的特性，選擇適合的群聚資料進行塑模，以提升模型的偵測效果。對於模型融合，本研究則以線性迴歸組合多種不同模型，以提供更穩定的預測結果。考量蒐集資料對於預測值的影響延遲效果，除一般模型外，我們亦將各種延遲模型納入融合過程。為驗證提出方法之有效性，我們針對上述方法分別進行實驗。結果顯示，在不同資料分割方式設定下，使用動態資料融合方法確有機會能提供更佳的偵測結果。當透過模型融合進行數值預測時，在僅考慮訓練集的狀況下，其預測關聯度可達0.910。當實際進行預測時，其關聯度仍亦達0.844，與單一模型相較，確可提供了良好的預測穩定性。

中 文 關 鍵 詞 ： 模型融合、資訊融合、詐騙偵測、電子商務

英 文 摘 要 ： The fast development of e-Commerce is obvious to see. However, this also attract the attention of fraudsters who are trying to defraud in various trade platforms. Because e-Commerce has good privacy protection and convenient user interface, the number of fraudster has increased fast in the past few years. If the situation is not considered seriously, it would affect the long term development of e-Commerce. Though a lot of fraud detection methods have been proposed, however, there are still many challenges remained. To this end, the project focused on developing more effective method to deal with fraud detection problem in e-Commerce. Particularly, we use information fusion and model fusion to promote the accuracy and stability of detection. For information fusion, this work developed a dynamic data fusion method. At first, the training set is divided into several clusters. Then, according the characteristics of account under test, the most proper clusters are chosen to build the detection model. The effectiveness of detection would increase by such a fine-grained data fusion. For model fusion, this research first construct several kinds of prediction models, then gathering them by linear regression to build a more stable fusion model. Considering the delay effect of gathering data, delay models are also included in the fusion process. The experimental results show that, in different experimental setting, the dynamic data fusion method could obtain better detection result. When predicting the numerical data by model fusion, the correlation will be up

to 0.910 in the case of the training set considered only. If the test set is used the input, then the correlation is 0.844 that is still acceptable. In addition, in comparison with the results of applying single models, our method did provide more stable prediction results.

英文關鍵詞：Model Fusion, Information Fusion, Fraud Detection, Electronic Commerce

運用資訊融合與模型融合發展穩定高效能之電子商務詐騙偵測架構

MOST 105-2410-H-032-042 -

摘要

電子商務的蓬勃發展有目共睹，但也引起有心人士的注意，在各種交易平台中進行詐騙。由於網路的隱蔽性與便利性，讓這些不法行為在短期內便快速成長，若不加以抑制，將嚴重影響其未來發展。電子商務的詐騙偵測雖已獲得高度關注，亦有許多方法被提出，但仍面臨諸多挑戰。為此，本計畫運用資訊融合與模型融合概念，發展有效的預測方法，以提供更穩定、準確的偵測結果。有關資訊融合，本研究提出了一套動態資料融合方法，先將訓練集依照類別分成多個群聚，再根據待測帳號的特性，選擇適合的群聚資料進行塑模，以提升模型的偵測效果。對於模型融合，本研究則以線性迴歸組合多種不同模型，以提供更穩定的預測結果。考量蒐集資料對於預測值的影響延遲效果，除一般模型外，我們亦將各種延遲模型納入融合過程。為驗證提出方法之有效性，我們針對上述方法分別進行實驗。結果顯示，在不同資料分割方式設定下，使用動態資料融合方法確有機會能提供更佳的偵測結果。當透過模型融合進行數值預測時，在僅考慮訓練集的狀況下，其預測關聯度可達0.910。當實際進行預測時，其關聯度仍亦達0.844，與單一模型相較，確可提供了良好的預測穩定性。

關鍵詞: 模型融合、資訊融合、詐騙偵測、電子商務

Constructing effective e-commerce fraud detection framework based on information fusion and model fusion

Abstract

The fast development of e-Commerce is obvious to see. However, this also attract the attention of fraudsters who are trying to defraud in various trade platforms. Because e-Commerce has good privacy protection and convenient user interface, the number of fraudster has increased fast in the past few years. If the situation is not considered seriously, it would affect the long term development of e-Commerce. Though a lot of fraud detection methods have been proposed, however, there are still many challenges remained. To this end, the project focused on developing more effective method to deal with fraud detection problem in e-Commerce. Particularly, we use information fusion and model fusion to promote the accuracy and stability of detection. For information fusion, this work developed a dynamic data fusion method. At first, the training set is divided into several clusters. Then, according the characteristics of account under test, the most proper clusters are chosen to build the detection model. The effectiveness of detection would increase by such a fine-grained data fusion. For model fusion, this research first construct several kinds of prediction models, then gathering them by linear regression to build a more stable fusion model. Considering the delay effect of gathering data, delay models are also included in the fusion process. The experimental results show that, in different experimental setting, the dynamic data fusion method could obtain better detection result. When predicting the numerical data by model fusion, the correlation will be up to 0.910 in the case of the training set considered only. If the test set is used the input, then the correlation is 0.844 that is still acceptable. In addition, in comparison with the results of applying single models, our method did provide more stable prediction results.

Keywords: Model Fusion, Information Fusion, Fraud Detection, Electronic Commerce

1. 前言

隨著網路與行動裝置的普及，電子商務的蓬勃發展有目共睹，交易金額也逐年攀升。如此龐大的金流，引起許多不肖人士的注意，在電子商務平台中進行詐騙。常見的詐騙行為有商品敘述不實、販賣偽劣品、收到貨款不出貨、進行假交易等(NW3C, 2013; Gavish & Tucci, 2008; Chua, 2004)。但詐騙者不限於扮演賣方，當扮演買方時，亦可進行付款詐欺、異常退款，甚至洗錢等不法行為(Chen et al., 2015)。Kim et al., (2013)更提到線上購物經常出現價格詐欺(price fraud)手法，詐騙者以低於市價販售商品，巧妙隱藏商品規格細節，吸引消費者下單。由於網路的隱蔽性與便利性，讓這些不法行為在短期內便快速成長，若不加以抑制，將嚴重影響其未來發展。

電子商務的詐騙偵測雖已獲得學界與業界的高度關注，亦有許多方法被提出，但仍面臨諸多挑戰(Ahmed et al., 2016; West & Bhattacharya, 2016)。首先，傳統分類技術(classification)面臨的準確率與運算效能問題，也出現於詐騙偵測中。其次，詐騙類型會隨時間演化，偵測方法須能隨之調整。此外，許多機構基於隱私考量，無法提供詐騙相關資料，影響研究的實用性，如分類錯誤，在不同領域需付出不同代價。最後，應嘗試發展通用偵測架構，進行跨領域的詐騙偵測。由上述討論可知，為維護電子商務的長遠發展，不法的詐騙行為確實需要被抑制，但總體而言，仍有很大的發展空間。

因此，本計畫將針對電子商務詐騙偵測發展更有效的方法，以維護整體的交易安全。首先，身處大數據時代，網路上的資訊來源眾多，若能運用資訊融合(Information Fusion)技術加以整合，將有助於提升異常偵測所需資料集之品質(Balazs & Velasquez, 2016)。資訊融合為將不同來源的資訊轉換成為具有一致性(coherent)的單一表示方式，期能提供更有效的決策支援(Bostrom, et al., 2007)。上述所指的決策支援，可以是自動化、或半自動化(人類參與)。早期的資訊融合通常較著重於資料融合(data fusion)，將各種硬體感測器(GPS定位系統、移動感測器等)測得的資料結合，產生一致性的融合資料，以備後續的分析。但時至今日，由於各類型網路社群的興盛，使用者在其上的網路足跡(Internet Footprint)，成為另一種類型資料來源。例如，在Chen等人(2013)的研究中，為進行網路媒體語意分析，對於圖片的可見屬性(visual features)與標籤屬性(tag features)進行融合，做為多媒體語意分析的根據。又如，Huang等人(2015)則針對推薦系統的Collaborative Filtering流程進行資訊融合，結合了使用者資訊、社會網路與商品知識庫等訊息，期能產生更高品質的分群結果。因此，對詐騙偵測而言，若能蒐集各面向的資料加以融合，將有助於建立更有效的偵測模型。

其次，各種詐騙偵測模型均有其特質，偵測效能也有所差異。當利用多種模型進行預測時，模型融合(Model Fusion)是一種從這些模型中擷取有利於預測效能增益(gain)的流程。Alford (2013)比較了類神經網路與貝氏方法在詐騙偵測上的效能，認為不論在推理透明度(transparency of reasoning)、訓練資料集大小、訓練

時間、學習速度等指標上，貝氏方法均優於類神經網路。Chen等人(2013)則利用貝氏方法進行模型融合，以提升網路媒體語意擷取的正確性。Huang等人(2015)以加權平均方式融合各模型預測結果，並透過學習法調整各模型的權重，以產生精確商品推薦名單。Li等人(2012)則同時使用貝式分類法與關聯規則探勘，歸納觀察詐騙者樣式，以利專家判讀。Chen等人(2015)利用多種模型偵測電子商務詐騙，利用logistic regression組合各種模型產生的可疑分數，並發現決策樹與Random Forest能獲得較佳的偵測效能。根據上述文獻資料顯示，若能有效整合各種模型的特點，對於偵測的即時性與準確性將有很大助益。

綜合上述討論，為提升電子商務詐騙偵測之準確率與穩定性，本計畫運用資訊融合與模型融合概念，發展有效的預測方法。有關資訊融合，本研究發展了一套動態資料融合方法，以提升偵測的準確性。首先，我們將訓練集依照類別分成多個群聚，再根據待測帳號的特性，選擇適合的群聚資料進行組合。最後，利用選定的學習演算法(如分類樹)動態建立之偵測模型，以提升模型的效能穩定性與準確率。對於模型融合，本研究則針對數值資料預測，以線性迴歸組合多種不同模型。建立模型所需的資料集分別取自網路社群與關鍵字熱門搜尋，網路社群發言資料更經過關鍵字切割與字頻計算。考量社群發言與關鍵字熱度對於預測值的延遲效果，除正常模型外，我們亦產生各種不同的延遲模型，以提升整體的偵測效能。根據實驗結果，在不同資料分割方式設定下，使用動態資料融合方法確有機會能提供更佳的偵測結果。對於透過模型融合進行數值預測，在僅考慮訓練集的狀況下，其預測關聯度達0.910。若以訓練資料塑模對測試資料進行預測，其關聯度仍亦達0.844，與單一模型相較，確可提供良好的預測準確性與穩定度。

2. 文獻探討

本節介紹與本研究相關之文獻、背景知識與術語，以利後續章節之討論。

2.1 電子商務詐騙

針對電子商務詐騙偵測，學界與業界莫不給予高度關注，並投注大量心力(West & Bhattacharya, 2016)。Alford (2013)更認為現代企業都應發展智慧型詐騙偵測系統，檢視每日進行的所有交易，以維護電子商務的交易安全。針對線上購物的價格詐欺，Kim et al. (2013)使用有限混合模型(finite mixture model)進行線上購物的價格詐欺偵測。先將商品描述資料(關鍵字)與商品價格資料分別進行分群，再對待測商品進行群組歸屬計算，最後配合條件機率理論產生決策函數，以判定商品是否有詐欺的可能。對於線上商店的付款詐欺，Valsselaer等人(2015)將交易屬性分為Intrinsic features與network-based features，並透過滑動視窗概念(sliding windows)，產生與時間相關的可疑指數。電子商務詐騙的手法部分來自於線上購物興盛後所發展的新伎倆(如以多重帳號進行假交易)，其他則與傳統的財務詐欺(financial fraud)多有重疊。例如，財務詐欺中常見的信用卡付款詐騙、保險理賠詐騙、洗錢等(Ahmed et al., 2016)，也經常出現在電子商務的詐騙劇本(scenario)

中。因此，許多財務詐騙偵測方法亦與電子商務詐騙偵測有關。Carminati等人(2015)針對信用卡線上交易詐欺發展分析方法，利用Correlation進行偵測屬性相關性分析，以挑選合適的屬性集，再透過群聚分析，決定可疑帳號是否為詐騙者之可能性。同樣針對信用卡詐欺，Zareapoor等人(2015)則利用常見的資料探勘演算法配合Bagging Ensemble Classifier，強化總體偵測效能。Ahmed等人(2016)探討如何將分群方法妥善應用至財務詐欺偵測(financial fraud detection)，透過階層式分群與不同的歸類準則，期能提供更佳的偵測結果。Li等人(2012)則針對ATM電話轉帳詐欺進行偵測，配合貝氏機率方法與關聯規則，檢視詐欺帳號的特質。

除線上購物外，線上拍賣(online auctions)也是電子商務中的重要交易平台，詐騙者經常在其中找尋受害者。為避免消費者受損失，學者也紛紛提出各種詐騙偵測方法。Chau等人(2006)利用價格異常做為偵測基礎，以分類樹方式建立偵測模型。Chang&Chang(2011, 2012)則提出詐騙預警概念，以階段切割法(phased-profiling)切割交易者生命週期，產生具有早期偵測效能偵測模型。Pandit等人(2007)則提出二階段偵測概念，利用分類樹與Markov Random Field標示詐騙正犯與共犯，期能找出詐騙共犯集團。Tsang等人(2014)持續改進Pandit等人的方法，以更精細的學習方法調整帳號詐騙機率的計算，期能更精確地標示出詐騙共犯集團。

除了學界外，業界對於詐騙偵測的投入也不遺餘力。為抑制詐騙猖獗，中國的阿里巴巴集團發展了一套即時的詐騙防範與監控系統-CTU(Counter Terrorist Centre)，監控的行為涵蓋不正常退款、多重帳號、盜取帳號，甚至洗錢等複雜的犯罪行為(Chen et al., 2015)。對於詐騙偵測，CTU採用5層的過濾機制，通過者才能順利進行交易付款。透過大數據分析，檢視客戶帳號，連線裝置與交易流程等資訊，建立偵測的規則(Rule)與偵測模型(分類樹)。對於詐騙監控，CTU則利用多屬性加權分數判別用戶的風險分數，並製作詐騙儀表板(Dashboard)供觀察者使用。由阿里巴巴願投注大量心力在詐騙偵測可知，若能有效控制詐騙行為，對於電子商務平台的長遠發展具有指標性意義。

2.2 詐騙偵測

詐騙偵測也是異常偵測(anomaly detection)的一種，所謂的異常可分為(a) Point anomaly: 若待測樣本與其他樣本明顯不同，便視為異常。此種異常偵測相對簡單，但容易造成誤判。例如，購買大型家電時，支付大筆金額，雖異於平時消費金額，但絕非異常。(b) Contextual anomaly: 若樣本在特定狀況下呈現異常，才被稱為異常。例如，在運動時心跳超過140，不應被視為異常，但若在辦公時發生，便需提出警告。(c) Collective anomaly: 若有多個不同的事件同時(或依序)發生，才被視為異常，但若只有個別事件發生，則非異常。考量實作的困難度，前人研究經常使用Point anomaly或Contextual anomaly做為偵測基礎。理論上，若能將方法延伸至Collective anomaly的偵測，對於詐騙行為演化必能有更深刻的了解，有助於早期發現、遏止詐騙行為。

在偵測詐騙過程中，偵測屬性集扮演舉足輕重的地位。屬性集若確能與詐騙特徵緊密相關，則可發揮良好的偵測效果。反之，若屬性集挑選不佳，關聯度過低，則不論如何改變塑模學習方法，都可能無法使準確率達到所需水準。為此，本研究共蒐集了以下三種屬性集，期能截長補短，提升整體偵測準確性，其特性分述如下:

(1) Chang & Chang(2009)提出之屬性集以評價為基礎(編號1-7)，因為交易前絕大多數的交易者均會參考買(賣)家的正評與負評記錄，來決定是否要繼續進行交易。此系列之屬性非常簡單易懂，文獻中之實驗結果也證實，具有良好的偵測效果。

(2) Chau等人(2006)發現詐騙者的交易金額會隨著生命週期而產生變動，而且詐騙者在買、賣次數的比例可能會相當懸殊。因此，他們設計了與一系列與價格、交易次數相關的偵測屬性(編號8-24)。例如，詐騙者在開始要進行詐騙時，會突然密集貼出多筆交易，或是大幅提高每筆交易的金額，為的就是在被發覺前的短時間內，盡可能詐得更多的款項。所以，利用特定時間內，交易金額或單價的變化來判斷是否有詐騙可能，是一種可行的做法。

(3) 鄭孝儒(2011)參考前人研究，在多方考量各種情況後，分別對價格、評價、時間、交易次數等特徵，提出了一套對應的複合式屬性集(編號31-52)。以價格而言，他所提出的屬性集考慮賣家的在此特徵上是否有劇烈改變(如最後15天與最後30天的平均售價的差)。此外，由於詐騙者會在爆發初期，密集貼出多筆交易，因此他的屬性集也考慮了時間因素，希望偵測出短期間內所產生的不合理交易。

2.3 資訊融合(Information Fusion)

為偵測電子商務詐騙，除了分析使用者除了在購物網站之交易資料外，他在網路上留下的任何數位足跡，均可透過融合技術，產生更有價值的資料集。資料的來源可以是電子商務網站公開資料或社群網路公開資料，資料的類型可以是文字、圖片、影片等。基本融合步驟(Dasarathy, 1997; Balazs & Velasquez, 2016)為將各類型資料來源進行整併，產生高品質的資料來源:

(1) Data In-Data Out Fusion – 依資料類型精煉(Data Refinement): 此步驟的要點為過濾、校正各類型資料的內容，過濾掉無法對分析結果造成加值(value added)的資料。

(2) Data In-Feature Out Fusion – 依物件類型精煉(Object Refinement): 本步驟的要點為將上一步驟的資料，依照詐騙偵測目的，產生以屬性(features)為基礎的資料表。這些屬性值可能融合自不同類型的資料表，被用來描述分析中的物件(Object)。

(3) Feature In-Feature Out Fusion – 依情境精煉(Situation Refinement): 以物件精煉後的結果為輸入，根據特定觀測行為，本步驟將產生抽象化更高的資料集。

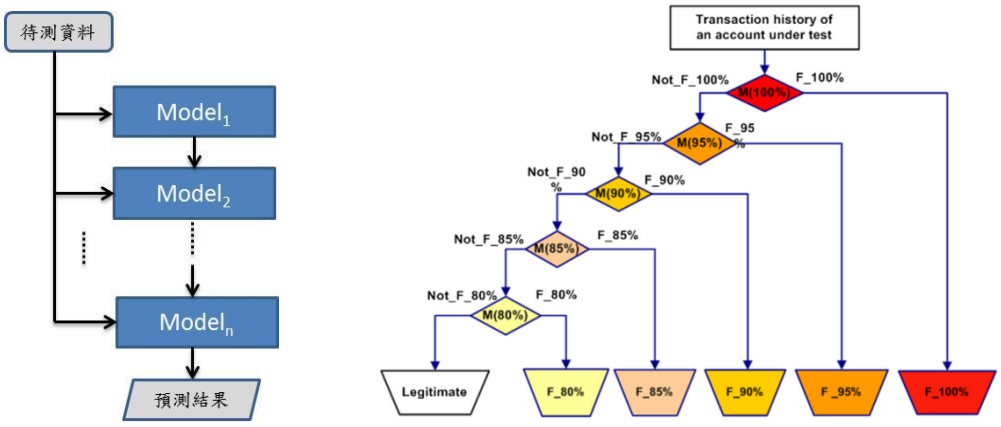
(4) Feature In - Decision Out Fusion – 威脅評估(Threat Assessment): 本步驟將根據上述資訊融合結果，進行自動化或半自動化威脅評估。若由電腦決策支援系統進行評估，則可進一步利用分類樹、類神經網路、貝氏推理方法等工具來協助判定威脅的程度。

2.4 偵測模型融合(Detection Model Fusion)

如前所述，各種偵測模型在不同狀況下，有不同的偵測效能。因此，很少有一種單一模型能適用各種不同場景或不同類型的待測資料。有鑒於此，融合多種模型的預測結果，截長補短以產生更準確的偵測結果，便成為可行之道。偵測模型融合流程的要點為如何擷取各種模型的長處，融合其預測結果，產生更有效的偵測結果。此外，融合流程亦須有學習過程，但需避免對訓練資料過度學習造成overfit現象。以下介紹各種可行的融合流程:

(1) 多階段融合流程:

參考 Fig. 2-1(a)，此種做法相當直覺，將待測資料逐一輸入各種模型($Model_1$~$Model_n$)，並將上一階段($Model_i$)模型偵測結果，做為下一階段模型($Model_{i+1}$)的參考依據，最後再產出偵測結果。應用類似概念，Chang&Chang(2011)亦發展出連續過濾式(successive filtering)的線上拍賣詐騙偵測方法(Fig. 2-1(b))，特點是偵測過程中若有決定性的結果，偵測步驟便可中斷。此種作法的優點為簡單、直覺，缺點為不同待測樣本可能需使用不同的模型排序，才能被有效偵測，因此可能較難獲得一致性、可接受的偵測準確率。



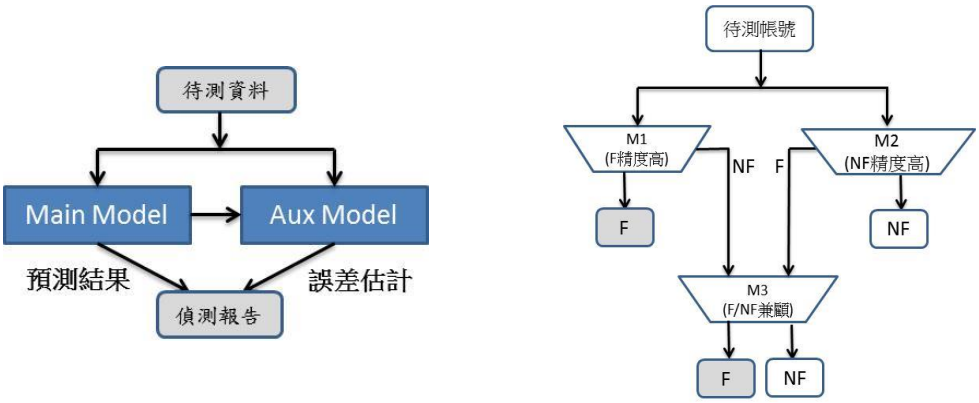
(a) 多層偵測概念 (Darudi et al., 2015)　　(b) 應用多階段偵測之研究 (Chang & Chang, 2011)

Fig. 2-1 多階段模型融合流程

(2) 互補式融合流程

參考 Fig. 2-2 (a)，此類型的融合流程基本上由一個主模型(main model)配合一個輔助模型(Aux Model)來進行。主模型提供主要的偵測結果，輔助模型則

估計主模型的偵測誤差，之後共同產生偵測報告。Fig. 2-2(b)所示為利用此概念所建構的線上拍賣詐騙偵測流程，其中的模型 M1 與 M2 具有互補特質(M1 擅長偵測詐騙者，M2 擅長偵測正常者)，之後再將所有難以決定的待測帳號以第三個模型 M3 進行綜合偵測。互補式融合方式較多階段融合更複雜，理論上也較可能將各模型截長補短。



(a) 基本互補式融合流程(Darudi et al., 2015)　　(b) 應用互補融合流程之研究 (Chang & Liu, 2014)

Fig. 2-2 互補式融合流程及其應用

3. 研究方法

以下各節將依序介紹本計畫提出之資訊融合與模型融合方法，並分別對於類別型資料(categorical data)與數值資料(numeric data)進行分類與預測。

3.1 運用動態資料融合進行詐騙偵測

詐騙偵測常見的方式為透過偵測模型，將待測帳號分為詐騙(Fraud)與非詐騙(Non-Fraud)二類(之後將以 F, NF 稱之)。傳統的模型融合偵測會先建立多個模型，並以特定方式加以組合。本研究則提出一種新的塑模方法，首先對訓練集進行分群，再根據待測樣本的特性，選用適當的資料群聚，以建立更合適的偵測模型。以本質而言，這是一種動態的資訊融合，與傳統使用固定資料集塑模方式，有基本上的差異。

本研究提出方法之細節請參閱表列 3-1 之虛擬碼，以下說明其主要流程:

(1) 利用訓練集，建立多種不同的資料群聚:

(a) 將訓練集分為 Train_F 與 Train_NF 二個子集合，分別儲存詐騙者與正常者之資料。

(b) 再利用分群演算法，將 Train_F 分為數個群聚，儲存於 CF；同樣將 Train_NF 分群，儲存於 CNF。

k-means 演算法為常見的分群演算法，但需事先指定 k 值。因此，本研究將在使群聚元素不至太少的狀況下，嘗試各種不同 k 值組合，找出最準確的塑模方式。除 k-means 外，另外一種可行的方法為使用 x-means 分群演算法，則無須事

先設定群數，由演算法自動決定最佳群數。

(2) 依照測試集中待測帳號(*aut*)的特性，動態產生偵測模型，並進行偵測:

(a) 將 *aut* 與 CF 與 CNF 中群聚之群心進行比對，分別找出最匹配之群聚，並分別存於 *cf* 與 *cnf* 中。

(b) 以 *cf* 與 *cnf* 之聯集做為訓練資料，利用使用指定之學習演算法 L(如 C4.5 分類樹演算法)，建立偵測模型 M。

(c) 利用 M 對帳號 *aut* 進行詐騙偵測，並將結果存於 result。

雖然上述方法的精神為動態選取資料集並塑模，但實際上可事先預備所有可能的偵測模型。若詐騙與非詐騙的分群數量(|CF|與|CNF|)分別為 *m*, *n*，則可能使用的偵測模型則有 *m*×*n* 種。圖 3-1 所示為 *m*=2, *n*=3 之狀況，共可產生 6 種不同的偵測模型。在實務上，這些偵測模型可事先產生備用，而非動態產生，以節省運算時間。

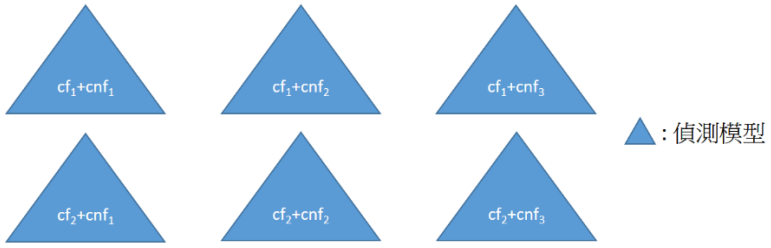


圖 3-1 當|CF|=2, |CNF|=3 時，可產生的偵測模型個數(2x3)

(3) 最後，當完成所有待測帳號之偵測後，統計偵測結果之精度(precision)、召回率(recall)等指標。

```
1   procedure FraudDetectionWithDynamicModel
2   input       Train_F: 僅含詐騙者(Fraud)之訓練集
3               Train_NF: 僅含正常者(Non-Fraud)之訓練集
4               TestSet: 待測帳號集合
5               L: 建立偵測模型之學習演算法
6   output      Metric: 儲存對 TestSet 之偵測結果
7       // CF 與 CNF 均為一集合，儲存 Train_F 與 Train_NF 的分群結果
8       CF = Clustering(Train_F);
9       CNF= Clustering(Train_NF) ;
10      for each account aut in TestSet do
11              // cf 為 CF 中各分群與 aut 最為匹配之分群
12              cf = BestFitCluster(CF, aut)
13              // cnf 為 CNF 中各分群中與 aut 最為匹配之分群
14              cnf = BestFit(CNF, aut) ;
15              //  以 cf 與 cnf 之聯集做為訓練資料，利用學習演算法 L 建立偵測模型 M
16              M = buildDetectionModel(cf ∪ cnf, L) ;
17              result = classify(M, aut)
18              add result to Metric
```

19	endfor
20	**end procedure**

表列 3-1：本研究提出之動態資訊融合詐騙偵測演算法

傳統詐騙偵測為將待測資料輸入預先建立的偵測模型中，再產生測試結果。然而，偵測模型乃根據訓練資料建造而成，學習演算法經常只為提升訓練資料集合的偵測準確率，犧牲少數較不典型之正常或異常資料，造成過度適配(overfitting)。此外，若測試資料可能與訓練資料性質不同，更導致模型偵測準確率不佳。為此，本研究事先將待測帳號與分群結果 CF, CNF 進行匹配，再將匹配所得做為塑模之訓練資料。事先分群不僅減少分類器所需的訓練時間，且由於是根據資料本身的相似度來分類，所以不會受到訓練資料的好壞而影響，還可將類型相似或屬性接近的詐騙者、正常使用者分為同一群。如此一來，在分類待測帳號時，便可動態產生更合適的偵測模型。

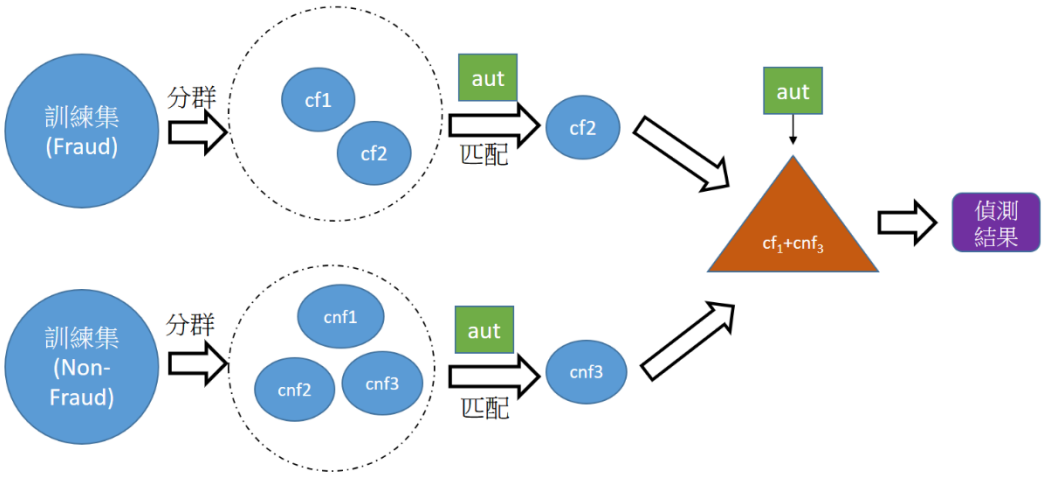


圖 3-2：動態資料融合與塑模之詐騙偵測流程範例

為更清楚呈現本研究提出之方法，以下將以圖 3-2 之範例來進行說明:

(1) 首先，將訓練資料集中的詐騙者(F)與正常交易者(NF)資料進行分群，假設 F 被分為 2 群、NF 分為 3 群，令 CF={cf1,cf2 }，CNF={cnf1,cnf2,cnf3 }，另個群的群心為 SCF = {cf1C, cf2C }，SCNF = {cnf1C, cnf2C, cnf3C}。

(2) 將待測帳號 *aut* 與 CF、CNF 各群群心進行歐基里德公式計算距離，依照設定的最適原則(如 Best-Fit、Second-Fit、Worst-Fit)，即得到 cnf = Match(CNF,aut)與 cf=Macth(CF,aut)。

(3) 若 *aut* 分別與 cf2C、cnf3C 最為接近，則將 cf2、cnf3 結合後進行塑模，再利用建立的模型來測試 *aut*。

以上為針對單一待測帳號之測試流程，若對象為一個測試集，可將其中每個帳號重複上述步驟，最後統計其偵測結果。

3.2 數值資料預測之資料融合與模型融合

3.1 節所述透過資料融合進行詐騙預測，為將帳號分為 Fraud 與 Non-Fraud。在實際應用時，有時也需進行數值資料的預測。例如，預測社群中每週的詐騙人數變化，用評估平台的交易安全性，讓平台管理者得以提早因應。有鑑於此，本研究將以不同資料來源做為輸入，並透過模型融合，發展有效的數值資料預測方法。對於模型融合，本計畫採用演算法融合(Fusion by Algorithm)方式來進行(參考圖 3-4)，先產生多個預測模型，之後再透過線性迴歸方式加以組合，以產生最後的融合模型。

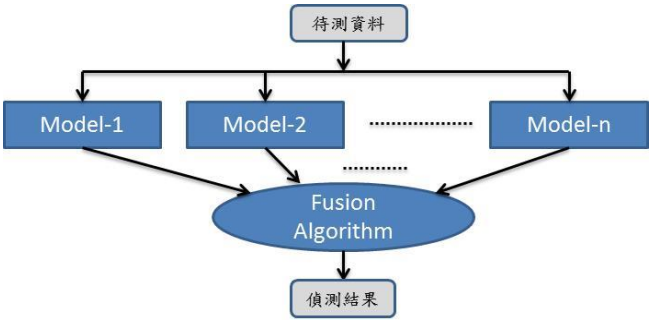


Fig. 3-4 使用融合演算法進行模型融合

3.2.1 資料來源

資料融合的精神為擷取性質不同資料來源，再透過不同方式整合，期待產生更好的預測效果。為此，本研究將使用以下二種不同來源的資料來進行預測:

(1) 蒐集網路社群 Tweeter 上之發言(Tweets): 透過呼叫 Twitter Streaming API，利用程式取得每日特定地區之發文(如圖 3-5 所示)，蒐集每日 Tweets 約有 3 千筆，每便可蒐集到約 2 萬餘筆。

```
Date:Sat Jun 11 13:00:16 CST 2016
User: Andrew Atterwill
Text: : Latest data Wind 0.0mph E Press 1011.6mb Steady Temp 12.3°C Rain today 0
.0mm Humidity 89% Fine, possible showers
Country: United Kingdom
Language: en
```

圖 **錯誤! 所指定的樣式的文字不存在文件中。**-5：每日蒐集之單則 Tweets

由 Twitter 蒐集之發文經過以下整理後，產生分析建模所需之資料集。我們計算每週所有關鍵詞出現在發文中的次數，並加以正規化:

$$s(k_i) = \frac{t(k_i)}{m \times n} \qquad (1)$$

其中$t(k_i)$為關鍵字k_i出現在當週所有發文中之頻率，m為關鍵字之總數，n為當周所有發文之總數。例如，關鍵字 k 在當週所有發文中共出現了 894 次，則 $t(k)$=894。假設關鍵字總數 m 為 74 個，當週發文總數 n 為 2000，則 k 在本週之正規化頻率為

$$s(k) = \frac{t(k)}{m \cdot n} = \frac{894}{74 \cdot 2000} = 0.0604$$

根據上述分析整理，每週之資料記錄便可用如下向量來表示(令 $K=\{k_0, k_1, k_2,\ldots, k_n\}$為分析時所用之關鍵字集)：

$$week_j(K) =< s(k_0), s(k_1), s(k_2) \ldots s(k_n), V_j > \qquad (2)$$

$week_j$為第 j 週之資料，V_j為所預測值之實際值(答案)。

(2) 蒐集 Google 關鍵字搜尋趨勢: 透過 Google 網站取得與 Twitter 相同時間點之關鍵字搜尋熱度，數字代表與圖表中特定區域和時間內最高點相對的搜尋熱門度(如圖 3-6 所示)。最高熱門程度的字詞將有 100 分，50 分為 100 分熱門程度的一半，而 0 分則表示熱門程度不到 100 分的 1%。

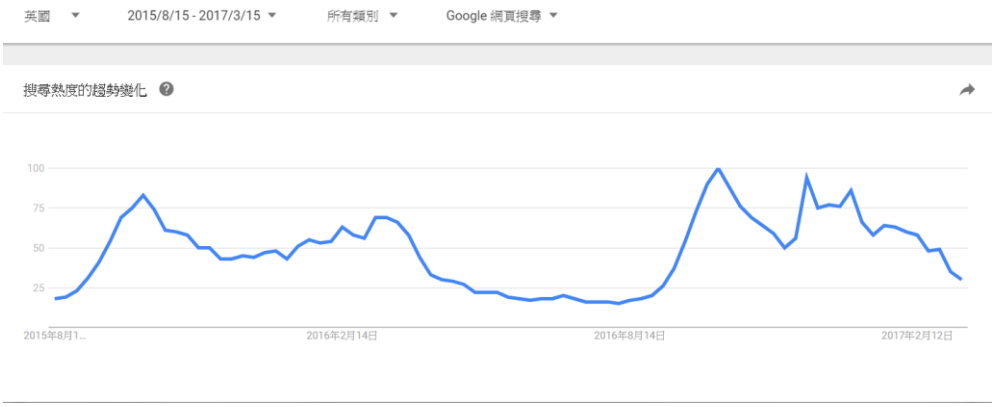


圖 3-6：某關鍵字在時間內的搜尋熱度
(資料來源: https://trends.google.com/trends)

3.2.2 以網路社群資料建立預測模型

本研究使用線性迴歸做為預測之基礎，為建立預測模型，使用者在網路社群(此處為 tweeter)發言需先經過整理，統計關鍵詞的出現頻率(本研究使用不同的關鍵詞集做為分析依據)。根據上述說明，本研究將依照回溯週數建立迴歸模型：

若預測時間點為第 t 週之數值，依照回溯週數 b，由資料集中取出 $week_{t-1}$, $week_{t-2}$, ..$week_{t-b}$，以便計算如下預測模型之係數 w_{k_i}：

$$V'(K) = w_{k_0} * s(k_0) + w_{k_1} * s(k_1) + \cdots + w_{k_i} * s(k_i) + c \qquad (3)$$

其中，V'為模型產生之預測值，w_{k_0}為迴歸模型為關鍵詞k_0所產生之權重，c 為迴歸模型之常數。

3.2.3 以 Google 關鍵字搜尋熱度建立預測模型

在預測時，若僅由單一資料來源(如 Twitter)建立模型，可能因某時時期資料代表性不足，無法準確預測結果。因此，本研究另外採用 Google 關鍵字搜尋熱度做為資料集來塑模，除與 Twitter 資料個別運用外，之後也希望透過模型融合，產生更佳的預測結果。

假設與研究相關之主要關鍵詞集為 G={g_0, g_1, g_2, …, g_m}，透過 Google 蒐集這些關鍵字之在特定時間內搜尋熱度。完成蒐集後，便以這些關鍵詞的搜尋熱度做為自變數，透過線性迴歸分析，建立流感預測模型，步驟如下:

(1) 將每週蒐集的關鍵字搜尋熱度資料轉換成如下之向量：

$$week_j(G) =< h(g_0), h(g_1), h(g_2) \ldots, h(g_m), V_j > \quad (4)$$

$week_j$為第 j 週之資料紀錄，$h(g_i)$為關鍵詞g_i在$week_j$的熱門程度，V_j為所預測值之實際值(答案)。

(2) 依照回溯週數建立預測模型：

若預測時間點為第 t 週之數值，依照回溯週數 b，由資料集中取出 $week_{t-1}$, $week_{t-2}$, ..$week_{t-b}$，以便計算如下預測模型之係數 w_{k_i}：

$$\text{Rate}'(G) = w_{g_0} * h(g_0) + w_{g_1} * h(g_1) + \cdots + w_{g_i} * h(g_i) + c \quad (5)$$

其中，V′為模型產生之預測值，w_{g_0}為迴歸模型為關鍵詞g_0所產生之權重，c為迴歸模型之常數。

3.2.4 延遲模型

考量發文或關鍵字搜尋可能具有延遲反映實際狀況的現象，導致當週所蒐集資料必能反應至當週之數值預測。為此，本研究考量延遲因素，以如下方式建立延遲迴歸模型：

(1) 將每週之資料向量修改為如下形式：

$$week_j\ (K) =< s(k_0), s(k_1), s(k_2) \ldots s\left(k_{|K|}\right), V_{j+d} > \quad (6)$$

$$week_j\ (G) =< h(g_0), h(g_1), h(g_2) \ldots h\left(g_{|G|}\right), V_{j+d} > \quad (7)$$

考量延遲因素，當週之 Twitter 發文頻率與搜尋熱度可能反應在 d 週後的實際值上(而非當週之實際值)。根據上述修改，建立延遲模型之訓練資料。

(2) 依照回溯週數建立預測模型：

若預測時間點為第 t 週之流感就診率，依照回溯週數 b，由資料集中取出 $week_{t-1-d}$, $week_{t-2-d}$, ..$week_{t-b-d}$，再帶入公式(3)或公式(5)，以便計算如下預測模型之係數。以下舉例如說明延遲模型之資料集建立方式: 若本周為第 6 週 $week_6$，回溯週數 b=4，延遲週數 d=1，則塑模時將採用 $week_{6-1-1}$, $week_{6-2-1}$, ..$week_{6-4-1}$，也就是取出第 1 週至第 4 週的資料進行訓練。此外，由於延遲因素，第 j 週之資料向量會採用第 $j+1$ 週之實際值做為其最後一個元素。

本研究以滑動視窗(sliding windows)概念建立迴歸公式，參考以下聯立公式: 假設時間單位為週，回溯週數為 bw，$y(t)$為第 t 週之實際發文量，$x_i(t)$為第 i 個自變數在第 t 週的值。為顧及實用性，本週發文量應不可使用本週之資料來進行塑模預測，否則便無參考價值。因此，本研究使用以下方式建立聯立公式集，再進行迴歸分析，以求得係數:

$$y(t-1) = w_1(t)x_1(t-2) + w_2(t)x_2(t-2) + \cdots + w_n(t)x_n(t-2) + \varepsilon(t)$$
$$y(t-2) = w_1(t)x_1(t-3) + w_2(t)x_2(t-3) + \cdots + w_n(t)x_n(t-3) + \varepsilon(t)$$
……
$$y(t-bw) = w_1(t)x_1(t-bw-1) + w_2(t)x_2(t-bw-1) + \cdots + w_n(t)x_n(t-bw-1) + \varepsilon(t)$$

根據求得之 w_i 與ε值，則本週之發文量 y'(t)則可以如下公式來求得:

$$y'(\mathrm{t}) = w_1(t)x_1(t-1) + w_2(t)x_2(t-1) + \cdots + w_n(t)x_n(t-n) + \varepsilon(t)$$

據此，當欲預測第 t+1 週之發文量時，依照滑動資料視窗概念，完成另一組 w_i 與ε值的計算如下:

$$y'(\mathrm{t}+1) = w_1(t+1)x_1(t) + w_2(t+1)x_2(t) + \cdots + w_n(t+1)x_n(t) + \varepsilon(\mathrm{t}+1)$$

假設預測週數由第 t 週至 t+r 週，則可產生(y'(t), y'(t+1),…,y'(t+r))，再與實際發文量向量((y(t), y(t+1),…,y(t+r))進行關聯度分析(如使用皮爾森相關係數)，即可了解預測結果與實際值之相關程度。

3.2.5 模型融合

使用單一模型進行預測，因資料集或學習演算法之特性，其效能可能受到限制。因此，本研究將使用模型融合(Model Fusion)方式，整合多種預測模型，將其預測結果以線性方式加以組合，並透過迴歸分析，找出其最佳的組合係數，相關做法將詳述如下。

(1) 將多種模型的預測結果做為資料集：本研究將融合以下六種預測模型來進行預測:

(a) MT: 使用 3-2 節介紹之方法，以 Twitter 資料集合，配合迴歸所建立之模型(回溯週數 b=4, 延遲週數 d=0)。
(b) $\mathrm{MT_{d1}}$: 同(a)，但延遲週數 d=1。
(c) $\mathrm{MT_{d2}}$: 同(a)，但延遲週數 d=2。
(d) MG: 使用之前介紹之方法，以關鍵字搜尋熱度做為資料集合，配合迴歸所建立之模型(回溯週數 b=4, 延遲週數 d=0)。
(e) $\mathrm{MG_{d1}}$: 同(d)，但延遲週數 d=1。
(f) $\mathrm{MG_{d2}}$: 同(d)，但延遲週數 d=2。

綜合以上六種模型之預測結果，配合實際值產生每週之資料向量如下：

$$week_j(MF) = < t\ , t_d\ , t_{d2}\ , g\ , g_d\ , g_{d2}\ , V_j > \qquad (8)$$

其中 MF={MT, $\mathrm{MT_{d1}}$, $\mathrm{MT_{d2}}$, MG, $\mathrm{MG_{d1}}$, $\mathrm{MG_{d2}}$}, 而$(t\ , t_d\ , t_{d2}\ , g\ , g_d\ , g_{d2})$分別對應前述六種模型在第 j 週之預測結果。

(2) 依照回溯週數建立預測模型：

若預測時間點為第 t 週之數值，依照回溯週數 b，由資料集中取出 $week_{t-1}(MF)$, $week_{t-2}(MF)$, ..$week_{t-b}(MF)$，以便計算如下預測模型各項之係數：

$$\mathrm{Rate}' = w_t * t + w_{t_d} * t_d + \cdots + w_{g_{d2}} * g_{d2} + c \qquad (9)$$

其中，Rate′為模型產生之預測值，w_t為迴歸模型為 Twitter 預測模型預測數值 t 所產生之權重，其餘模型常數依此類推，c為迴歸模型之常數。

4. 結果與討論

為驗證提出方法之有效性，本節將透過不同實驗，對於預測結果進行效能評估。

4.1 運用動態資訊融合進行線上拍賣詐騙偵測

本研究實驗採用因不誠實交易而被停權者作為訓練集 F，資料總筆數為正常者(NF): 246 筆，詐欺者(F): 296 筆，採用 18 個屬性之屬性集；訓練集測試集比例 7:3，詐欺者(F)與正常者(NF)資料筆數比例 1:2，各屬性值正規化後剔除 4 倍標準差資料。使用 k-means 進行分群時，最大 k 值設為 5，使用 x-means 時，分群上限設定為 10。計算待測帳號之最適群組時預設採用與測試集最近群心之訓練集資料(best-fit)進行匹配運算(其餘兩種為 second-fit 與 worst-fit)，且所有數據均為 10 次實驗之平均結果(亂數選取訓練集與測試集)，在比較測試集與訓練集之分群群心時，採用歐基里德距離公式。

在實驗過程中，若訓練集太小容易導致訓練不足，使分類效果不佳。但若訓練集比例過大，又會導致訓練集過度優化，導致學習演算法在訓練過程過於樂觀估計，造成 Over-fitting。因此本研究在多方嘗試後，依經驗法則使用訓練集測試集比例 7:3 的設定。有關詐騙者(F)與正常者(NF)資料筆數比例 1:2 的設定上，則依照 Chang&Chang(2009)在研究中所使用之比例。

依照上述實驗設定，本研究提出之動態塑模詐騙偵測方法之實驗結果如表 4-1 所示。其中，使用 1x1 分群建立模型等同於傳統單一分類樹塑模。以精度而言，以 4x1 之組合最佳，準確率(Accuracy)為 0.806，優於 1x1 單一分類樹之 0.738，驗證了本研究提出之方法之有效性。表 4-3 則為使用 x-means 分群之偵測結果，準確率僅為 0.69。顯示使用 x-means 演算法時，可能需有更精細之考慮，而非完全依賴演算法預測特質來分群。

接下來實驗嘗試調整各項實驗參數，以了解這些設定對於偵測結果的影響。為使實驗結果更精簡，以下實驗僅使用 x-means 做為分群方法。首先，表 4-2 顯示使用不同倍率標準差進行資料篩選之偵測結果，"n 倍標準差"之列表示該列之資料集已將超過平均值±n 倍標準差之樣本刪除。實驗結果顯示，使用 3 倍標準差進行資料過濾之結果最佳。倍率越高結果越差，原因可能為資料欄位歧異度若變大，偵測準確率越差。

在實驗過程中，若訓練集比例大小影響層面如實驗設定時所說，故本實驗進行多方嘗試，試驗不同比例狀況下之偵測結果。表 4-3 測試使用不同訓練集與測試集比例之偵測結果，實驗顯示 Train:Test=9:1 具有最佳結果。顯示在資料充足狀況下，可採用較高比例之訓練集，以獲得較佳之偵測模型。表 4-4 則為待測帳號使用三種不同方式，進行最適群聚匹配之偵測結果。結果顯示 Best Fit 具有最

佳之偵測準確率，Worst Fit 最差，此結果或可做為分群時之根據，以產生較佳辨識效果之群聚。

表 4-1：使用 k-means 分群不誠實交易者資料集進行動態塑模之偵測結果

分群數 |CF|x|CNF|	Recall	Precision	F-Measure	Accuracy
1X1	0.786	0.837	0.810	0.738
1X2	0.774	0.801	0.788	0.710
1X3	0.775	0.811	0.793	0.716
1X4	0.770	0.793	0.781	0.703
1X5	0.767	0.755	0.761	0.682
2X1	0.763	0.859	0.808	0.727
2X2	0.772	0.832	0.801	0.723
2X3	0.761	0.803	0.781	0.699
2X4	0.762	0.790	0.776	0.694
2X5	0.759	0.773	0.766	0.684
3X1	0.770	0.882	0.822	0.744
3X2	0.770	0.831	0.799	0.721
3X3	0.771	0.801	0.786	0.708
3X4	0.756	0.796	0.776	0.692
3X5	0.756	0.773	0.765	0.681
4X1	0.754	0.862	0.719	0.804
4X2	0.764	0.848	0.804	0.723
4X3	0.760	0.811	0.785	0.702
4X4	0.765	0.787	0.776	0.695
4X5	0.756	0.758	0.757	0.674
5X1	0.744	0.863	0.799	0.709
5X2	0.758	0.841	0.797	0.713
5X3	0.763	0.815	0.788	0.707
5X4	0.745	0.789	0.766	0.677
5X5	0.740	0.799	0.768	0.677

表 4-2：x-means 分群不誠實交易者資料集進行不同倍率標準差之偵測結果

X-Means	Recall	Precision	F-Measure	Accuracy
3 倍標準差	0.778	0.776	0.777	0.703
4 倍標準差	0.760	0.790	0.775	0.692
5 倍標準差	0.774	0.782	0.778	0.703
6 倍標準差	0.764	0.781	0.772	0.693
7 倍標準差	0.773	0.739	0.756	0.681

表 4-3：x-means 分群不誠實交易者資料集改變訓練測試集比例之偵測結果

使用 X-Means 分群	Recall	Precision	F-Measure	Accuracy
Train：Test = 7：3	0.760	0.790	0.775	0.692
Train：Test = 8：2	0.779	0.740	0.759	0.684
Train：Test = 9：1	0.814	0.777	0.795	0.733

表 4-4：x-means 分群不誠實交易者資料集且待測帳號使用不同匹配之結果

使用 X-Means 分群	Recall	Precision	F-Measure	Accuracy
Best Fit	0.760	0.790	0.775	0.692
Second Fit	0.732	0.807	0.768	0.673
Worst Fit	0.698	0.531	0.603	0.532

我們從實驗結果可推測出動態塑模詐騙偵測方法，能根據待測帳號的特性，動態建立有效的偵測模型，確實有助於偵測準確率的提升。其次，改變訓練與測試資料比例，亦有助於效能的提升。此外，不同的資料篩選方式，亦可影響最後偵測結果。

4.2 資訊融合與模型融合對於數值型預測之效能

有關運用資訊融合與模型融合進行詐騙人數預測，由於國內拍賣網站(如露天拍賣、Yahoo 拍賣)均已不再公告詐騙者，因此無法順利進行實驗。為此，本計畫採用流感就診率做為類比的實驗平台，將所發展之方法，運用於流感就診率之偵測上。

為進行實驗，我們選用英國地區做為流感就診率的標的。首先，下載英國官方(Public Health England)每周流感監測數據做為實際值，再配合由 Twitter 與 Google 關鍵字熱度搜尋下載之資料，進行模型融合預測。由於官方數據是以週為基礎，因此本研究將 Twitter 上每日發文合併成與官方數據日期相符之週數。上述資料經過一年多的蒐集，共蒐集約有 80 週的 Tweets 與官方統計數據(2015/8/13 – 2017/3/15)。Google 關鍵字熱度搜尋部分，本研究採用流感可能出現的八個主要症狀做為關鍵詞(發燒、咳嗽、頭痛、疲倦、喉嚨痛、畏寒、肌肉痠痛、打噴嚏)，之後統計這些關鍵字之在特定時間內搜尋熱度。圖 4-5 為將所有資料集均做為訓練資料，運用 3-2 節模型融合方法之預測統計結果。由圖中可知，預測值與實際值之相關係數高達 0.91，此結果顯示提出方法之有效性。若能運用各種模型的特質，確可效提升預測準確率。

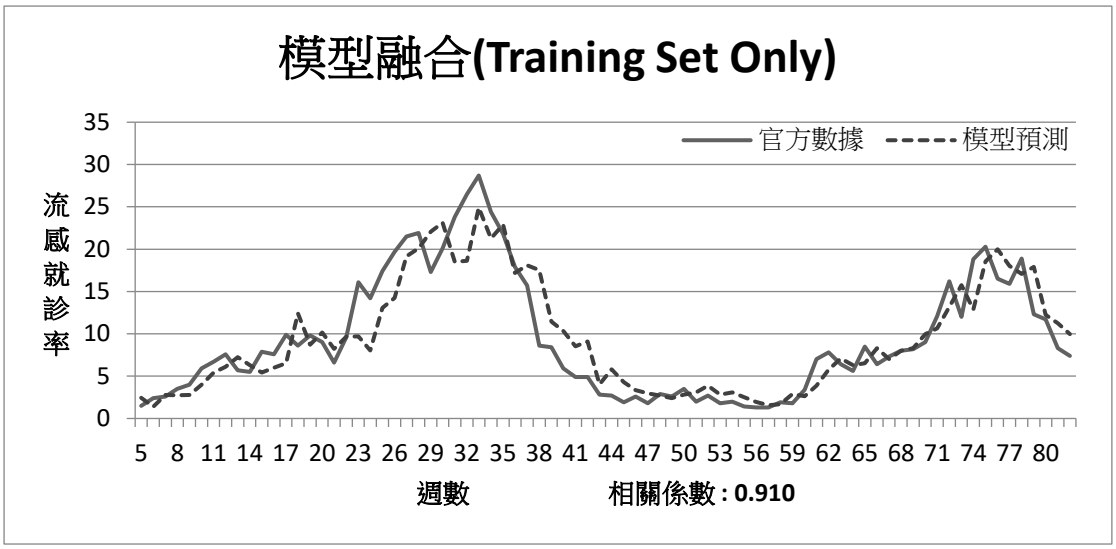


圖 4-5: 模型融合(Using Training Set)

圖 4-6 為運用前 52 週作為訓練資料，使用 52 至 82 週做為測試之資料之預測結果，結果顯示相關係數亦可達 0.844，顯示本研究提出方法之有效性。實際觀察波形變化，可發現模型融合在預測上仍有延遲現象(如 72, 73, 78 週等)，顯見如何選擇合適的模型來進行融合，是另一項重要課題。

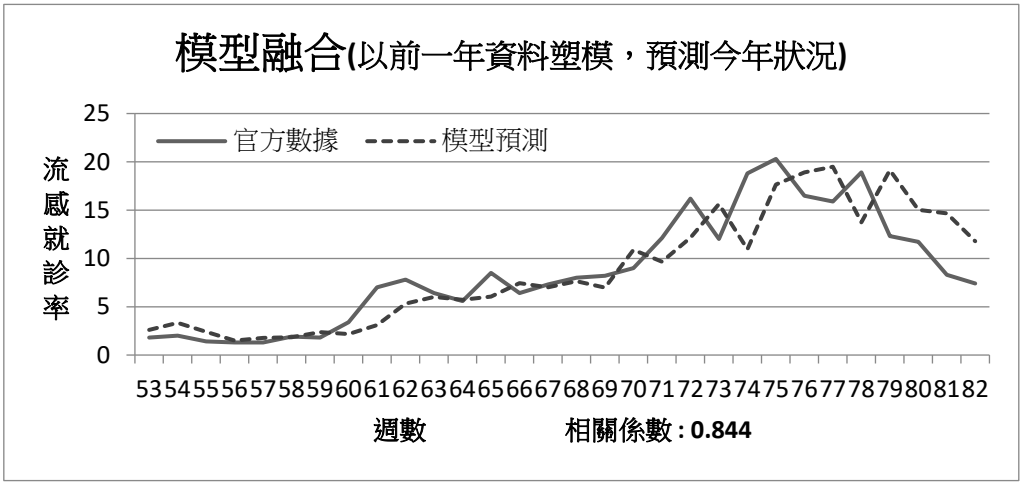


圖 4-6 : 模型融合(前一年預測今年)

表 4-5 為各種單一模型之偵測結果，仍使用前 52 週作為訓練資料，使用 52 至 82 週做為測試之資料之預測結果。由表中可知，使用模型融合與其他單一模型相較(只比較 53-82 週)，其效能僅次於 Google_lag2 模型。相較之下，模型融合之預測結果更具有穩定性，也顯示模型融合之優點。

53-82週各模型相關係數比較								
	Twitter	Twitter_L	Twitter_L	Google	Google_L	Google_L	trainset	test
相關係數	0.804	0.693	0.774	0.798	0.705	0.944	0.918	0.844

表 4-5: 第 53-82 週各模型相關係數比較

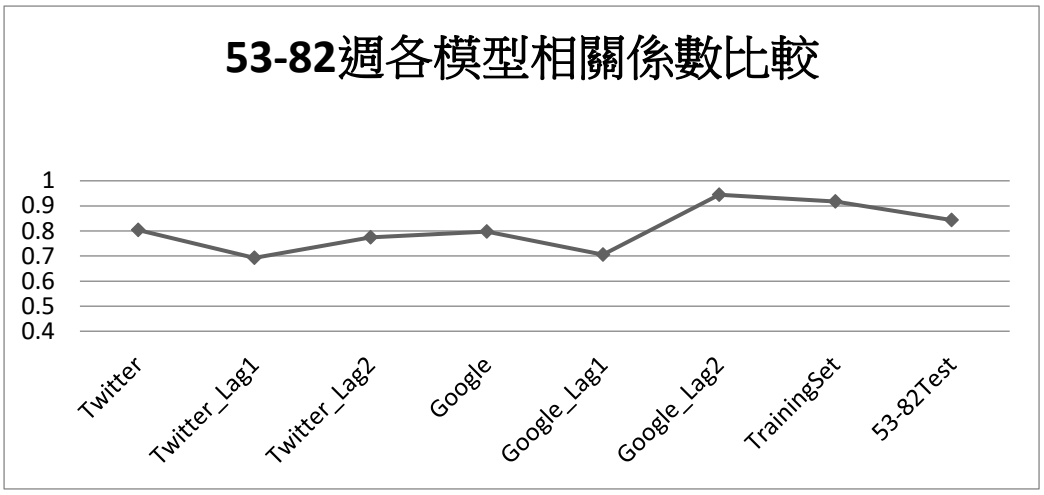


圖 4-7 : 53-82 週各模型相關係數比較

5. 結論與建議

近年來，在網路、資訊安全、金流、物流等基礎建設的配合下，電子商務已發展成足以威脅實體通路的經濟模式，並成為世界各國經濟發展新動能。電子商務讓交易行為隨時隨地發生，不受時間、地點的限制，除有效提升營業額外，也落實全球化經濟之理想。然而，由於網路的隱蔽性與便利性，也引起詐騙者的關注，運用詐術獲取不法收益。這些不法行為在短期內便快速成長，若不加以抑制，將嚴重影響其未來發展。

爲解決上述問題，本計畫運用資訊融合與模型融合概念，發展有效的預測方法。有關資訊融合，本研究發展了一套動態資料融合方法，以提升偵測的準確性。首先，我們將訓練集依照類別分成多個群聚，再根據待測帳號的特性，選擇適合的群聚資料進行組合。最後，利用選定的學習演算法(如分類樹)動態建立之偵測模型，以提升模型的效能穩定性與準確率。對於模型融合，本研究則針對數值資料預測，以線性迴歸組合多種不同模型。建立模型所需的資料集分別取自網路社群與關鍵字熱門搜尋，網路社群發言資料更經過關鍵字切割與字頻計算。考量社群發言與關鍵字熱度對於預測值的延遲效果，除正常模型外，我們亦產生各種不同的延遲模型，以提升整體的偵測效能。根據實驗結果，使用動態資料融合方法，在不同資料分割方式設定下，確有機會能提供更佳的偵測結果。對於透過模型融合進行數值預測，在僅考慮訓練集的狀況下，其預測值關聯性達 0.910。若以訓練資料塑模對測試資料進行預測，其關聯度仍亦可達 0.844，與單一模型相較，確提供了良好的預測準確性與穩定度。

根據本計畫之執行成果，我們有以下建議:

(1) 隨著詐騙偵測方式的發展，詐騙的方法也日新月異，因此對於新型態詐騙的產生應更有警覺。為此，往後可在建立偵測模型時，增加新的詐騙型態的權重，讓偵測模型能快速適應這些以往未曾出現之樣式。

(2) 模型融合的方式可更為多樣化，例如使用多階段互補式融合。然而，更多的偵測模型並非一定更有效，可將深度學習概念引入，讓模型的組合方式更為

適切。

(3) 在之前實驗中，將多個資訊進行融合可能有助於預測結果的改善。然而，資料若未經清洗，則將產生更多干擾與變因。因此，未來對於資訊融合時，應配合有效的資料清洗，以干擾最後偵測模型的穩定性。

參考文獻

1. Ahmed M. (2016), Mahmood A. N., and Islam M. R., "A survey of anomaly detection techniques in financial domain," Future Generation Computer Systems 55 (2016) 278-288.
2. Alford M. (2013), "Intelligent fraud detection: a comparison of neural and Bayesian methods," Computer Fraud & Security, pp. 14-16
3. Balazs, Jorge A., Juan D. Velásquez (2016), "Opinion Mining and Information Fusion: A survey," Volume 27, January 2016, Pages 95–110.
4. Carminati, M., et al. (2015), "BankSealer: A Decision support system for online banking fraud analysis and investigation," Computers & Security 53 (2015) 175-186.
5. Chang, W., and Chang, J. (2011), 'A Novel Two-Stage Phased Modeling Framework for Early Fraud Detection in Online Auctions', Expert System with Applications, vol.38, no.9 , pp. 11244-11260.
6. Chang, J.-S., Chang W.-H. (2014). Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters. Electronic Commerce Research and Applications, 13(2), pp. 79-97.
7. Chang, W.-H., Chang, J.-S. (2012). An effective early fraud detection method for online auctions. Electronic Commerce Research and Applications, 11(4), pp. 346-360.
8. Chang, Jau-Shien and Yu-Hung Liu, "Developing Cost-effective Methods for Identifying Online Auction Fraud," Electronic Commerce Research, Springer. (審稿中)
9. Chau, D. H. (2005). Fraud detection in electronic auction. European Web Mining Forum at ECML/PKDD, (pp. 87-97).
10. Chau, D. H. (2006). Detecting fraudulent personalities in networks of online auctioneers. Knowledge Discovery in Databases: PKDD (pp. 103-114). Springer.
11. Chen C., et al. (2013), "Web Media Semantic Concept Retrieval via Tag Removal and Model Fusion," ACM Trans. on Intelligent Systems and Technology, Vol. 4, No. 4, Sep. 2013.
12. Chen, J., et al. (2015), "Big Data based fraud risk management at Alibaba," The Journal of Finance and Data Science 1 (2015) 1-10.
13. Chua, C. E. and Wareham, J. (2004), 'Fighting Internet Auction Fraud: An Assessment and Proposal', Computer, vol. 37, no. 10 , pp. 31-37.
14. Dasarathy (1997), “Sensor fusion potential exploitation – innovative architectures and illustrative applications,” Proceedings of the IEEE, Vol. 85 (1), Jan. 1997, pp. 24-38.

15. Darudi, A., Bashari, M., and Javidi H. (2015), "Electricity price forecasting using a new data fusion algorithm," IET Generation, Transmission & Distribution, 2015, Vol. 9, pp. 1382-1390.
16. Dilla, N. W., Raschke, R. L. (2015), "Data Visualization for fraud detection: Practice implications and a call for future research," International Journal of Accounting Information Systems 16 (2015) 1-22.
17. eBay. (2013). eBay 交易安全 網上拍賣自保招數—詐騙賣家的特徵. 擷取自 eBay 台灣: http://pages.ebay.com.hk/securitycenter/education/fraud_traits.html
18. Gavish, B., and Tucci, C. (2008), 'Reducing Internet Auction Fraud', Communications of the ACM, vo. 51, no. 5 , pp. 89-97.
19. Halvaiee, N. S., and Akbari, M. K. (2014), "A novel model for credit card fraud detection using artificial immune systems," Applied Soft Computing 24 (2014) 40-49
20. Huang, S., et al. (2015), "A Hybrid Multigroup Coclustering Recommendation Framework Based on Information Fusion," ACM Trans. on Intelligent Systems and Technology, Vol. 6, No. 2, Mar. 2015.
21. Kim, K., Choi Y., and Park J. (2013), "Price fraud detection in online shopping malls using a finite mixture model," Electronic Commerce Research and Applications 12 (2013) 195-207.
22. Kohavi, Ron and John, H.George (1997), "Wrappers for feature subset selection", Artificial Intelligence 97 (1997), pp. 273-324
23. Kose, I., Gokturk, M., Kilic K. (2015), "An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance," Applied Soft Computing 36 (2015) 283-299.
24. Liu, S., Chen L., and Ni, L. (2014), "Anomaly Detection from Incomplete Data," ACM Trans. on Knowledge Discovery form Data, Vol. 9, No. 2, Sep. 2014.
25. National White Collar Crime Center(NW3C). (2013). 2011 Internet Crime Report. Retrieved on Dec 1, 2015, from Internet Crime Complaint Center: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf
26. Pandit, S. et al., (2007). Netprobe: a fast and scalable system for fraud detection in online auction networks. Proceedings of the 16th international conference on World Wide Web (pp. 201-210). ACM.
27. Russell, S., & Norvig P. , Artificial Intelligence-A Modern Approach (2/e). Prentice Hall (December 30, 2002)
28. Smith, M. G. and L. Bull (2005), "Genetic programming with a genetic algorithm for feature construction and selection," Genet. Program. Evol. Mach., vol. 6, no. 3, pp. 265-281, Sep. 2005.
29. Tang, L., and Liu, H. (2014), "Feature Selection for Social Media Data," ACM Trans. on Knowledge Discovery form Data, Vol. 8, No. 4, Oct. 2014.

30. Tsang, S., et al. (2014), "SPAN: Finding collaborative frauds in online auctions," Knowledge-based systems 71 (2014) 389-408.
31. West J., Bhattacharya, M. (2016), "Intelligent financial fraud detection: A comprehensive review," Computer & Security 57 (2016) 47-66.
32. Valsselaer, V. et al. (2015), "APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions," Decision Support System 75 (2015) 34-48.
33. Zareapoor, M., and Shamsolmoali, P. (2015), "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier," Procedia Computer Science 48 (2015) 679-685.
34. 鄭孝儒，「 線上拍賣潛伏期詐騙者之有效偵測」，淡江大學資訊管理學系，碩士論文，民 100。

105年度專題研究計畫成果彙整表

計畫主持人：張昭憲	**計畫編號：**105-2410-H-032-042-
計畫名稱：運用資訊融合與模型融合發展穩定高效能之電子商務詐騙偵測架構	

成果項目					量化	單位	質化 （說明：各成果項目請附佐證資料或細項說明，如期刊名稱、年份、卷期、起訖頁數、證號...等）
國內	學術性論文	期刊論文			2	篇	1. 張昭憲、莊秉諺（2017），"以行為狀態變遷為基礎之線上拍賣詐騙偵測方法"，中華民國資訊管理學報，第二十四卷，第一期，頁97-130。(TSSCI) 2. 張昭憲、沈育信，"網路新聞讀者閱後情感之預測"，資訊、科技與社會學報(中央警察大學)，2016年，第十六卷。
		研討會論文			0		
		專書			0	本	
		專書論文			0	章	
		技術報告			0	篇	
		其他			1	篇	"以資料融合與模型融合為基礎之詐騙偵測方法"，撰寫整理中。
	智慧財產權及成果	專利權	發明專利	申請中	0	件	
				已獲得	0		
			新型/設計專利		0		
		商標權			0		
		營業秘密			0		
		積體電路電路布局權			0		
		著作權			0		
		品種權			0		
		其他			0		
	技術移轉	件數			0	件	
		收入			0	千元	
國外	學術性論文	期刊論文			0	篇	
		研討會論文			0		
		專書			0	本	
		專書論文			0	章	
		技術報告			0	篇	
		其他			0	篇	
	智慧財產權及成果	專利權	發明專利	申請中	0	件	
				已獲得	0		
			新型/設計專利		0		
		商標權			0		

		營業秘密	0		
		積體電路電路布局權	0		
		著作權	0		
		品種權	0		
		其他	0		
	技術移轉	件數	0	件	
		收入	0	千元	
參與計畫人力	本國籍	大專生	0	人次	
		碩士生	3		周書任、李佳蓉、陳世軒
		博士生	0		
		博士後研究員	0		
		專任助理	0		
	非本國籍	大專生	0		
		碩士生	0		
		博士生	0		
		博士後研究員	0		
		專任助理	0		
其他成果 （無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。）					

科技部補助專題研究計畫成果自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現（簡要敘述成果是否具有政策應用參考價值及具影響公共利益之重大發現）或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估
   ■達成目標
   □未達成目標（請說明，以100字為限）
   　□實驗失敗
   　□因故實驗中斷
   　□其他原因
   說明：

2. 研究成果在學術期刊發表或申請專利等情形（請於其他欄註明專利及技轉之證號、合約、申請及洽談等詳細資訊）
   論文：□已發表　□未發表之文稿　■撰寫中　□無
   專利：□已獲得　□申請中　■無
   技轉：□已技轉　□洽談中　■無
   其他：（以200字為限）

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性，以500字為限）
   電子商務的詐騙偵測雖已獲得學界與業界高度關注，亦有許多方法被提出，但仍面臨諸多挑戰。面對大數據時代的來臨，資料的量與產生速度驚人，相關問題(如安全、犯罪)已非早期方法所能處理。本計畫運用模型融合與資料融合概念提出不同的做法，對於此領域提供另一種可行的解決之道。本研究嘗試使用資料融合將大量資料以更有效方式來運用，並透過組合各種偵測模型，提供更穩定的偵測方法。若能進一步發展，將可有效運用消費者在交易平台上留下的大量數位足跡，提供更安全的交易環境。

4. 主要發現
   本研究具有政策應用參考價值：■否　□是，建議提供機關
   （勾選「是」者，請列舉建議可提供施政參考之業務主管機關）
   本研究具影響公共利益之重大發現：□否　□是
   說明：（以150字為限）