Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

設計與建置利用開源結合 AI 之校園資安監測平台–以臺灣中部某大學為例

林子煒[1*]、蔡國裕[2]、郭崇韋[3]、林玟欣[4]、李品臻[5]、梁瑋宸[6]、黃千芸[7]、范秩嘉[8]、陳宣廷[9]、王富貴[10]
逢甲大學資訊總處資訊安全中心[1]
逢甲大學人工智慧技術與應用學士學位學程[1,6,7,9,10]
逢甲大學資訊工程學系[2,3,4,5,8]
[1]tweilin@fcu.edu.tw, [2]kytsai@fcu.edu.tw, [3]cwkuo@mail.fcu.edu.tw, {[4]d1104427, [5]d1047274, [6]d1149324, [7]d1146304, [8]d1225414, [9]d1146233, [10]d1146202}@o365.fcu.edu.tw

摘要

隨著資訊科技的迅速發展，為高等教育機構帶來教學與研究上的協助與便利，但面臨日益複雜的網路環境，卻也大幅增加資訊安全管理的複雜性。本研究以臺灣中部某大專院校為例，針對當前校園資安事件通報系統進行分析。本研究發現現有外部通報機制存在調查耗時、易錯過最佳應對時機等問題。此外，儘管已部署專門儲存安全設備的日誌於系統中，但欠缺視覺化呈現與高效率資安事件查詢與調查，導致通報流程缺乏時效性與準確性，進而影響防禦之回應與策略的制定。為解決上述問題，本研究建置資安事件洞察分析平台，整合大數據分析技術、人工智慧預測模型及使用者友善介面設計，降低資訊安全人員的工作負擔，同時提高對資安事件的監控與應對能力。

關鍵詞：資安事件分析、人工智慧、大數據分析、使用者友善介面

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

Design and Implementation of Open-Source Cybersecurity Monitoring System Using AI: A Case Study at a University in Central Taiwan

Tzu-Wei Lin[1*], Kuo-Yu Tsai[2], Chung-Wei Kuo[3], Wen-Xin Lin[4], Pin-Chen Li[5], Wei-Chen Liang[6], Chien-Yun Huang[7], Zhi-Jia Fan[8], Xuan-Ting Chen[9], Fu-Guei Wang[10]
[1] Information Security Office, Office of Information Technology, Feng Chia University, Taiwan, [1,6,7,9,10] Bachelor's Program of Artificial Intelligence and Technology Applications, i. School, Feng Chia University, Taiwan, [2,3,4,5,8] Department of Information Engineering and Computer Science, Feng Chia University, Taiwan,
[1]tweilin@fcu.edu.tw, [2]kytsai@fcu.edu.tw, [3]cwkuo@mail.fcu.edu.tw, {[4]d1104427, [5]d1047274, [6]d1149324, [7]d1146304, [8]d1225414, [9]d1146233, [10]d1146202}@o365.fcu.edu.tw

Abstract

Rapid development of information technology provides supports and convenience for teaching and research of higher education institutions. However, information security management becomes complicated because of heterogeneous networks. After interviewing a university in central Taiwan, we found that information security events system for campus nowadays highly depends on alerts from other institutions, which occurs that investigation of information security events takes lots of time. Moreover, although log system has been established, lacks visualization will be an obstacle for searching and investigating information security events with efficiency and accuracy, which will have influences on deciding defense strategy. Proposed system integrates big data analysis techniques, prediction model of artificial intelligence, and user-friendly interface design and is expected to not only solve problems above but reduce loading of information security personnels and improve monitoring and response abilities.

Keywords: Information security events analysis, artificial intelligence, big data analysis, user-friendly interface design

壹、前言

隨著資訊時代的快速發展，網際網路已成為我們生活中不可或缺的一部分，在校園中更是各項教學、研究與管理學校系統的重要媒介。網路的廣泛使用雖然帶來便利，但也伴隨著日益增長的資訊安全威脅，這些威脅對校內系統管理構成顯著的資訊安全風險。因此，校園網路環境的安全性需要得到有效保護，以確保校內各項程序順利進行。

為減少資安事件的發生，許多校園已部署多種資訊安全網路設備。然而，傳統的資訊安全防護手段和措施已無法完全應對現代化、多樣化的網路攻擊。因此，如何有效監控和管理校園網路流量，及時發現並處理潛在的資安事件，成為校園資訊安全管理的重要挑戰。

在本研究所調查的大學中，其校內的資訊安全環境依賴多種資訊安全網路設備的部署，以達成縱深防禦的目的。然而，資訊安全事件發生時，通常仰賴外部通報，且在日誌查找時依賴人工作業。這樣的作法不僅耗費人力和時間，還可能因此錯失最佳調查事件的時間。雖然其校內有日誌收容系統協助收容各項資訊安全設備，但該系統缺乏視覺化介面及查詢功能，導致資安事件通報上耗時且無法迅速、精準地察覺問題來源。這樣的情況促使我們考慮如何改進校園資安事件的管理，提升事件處理的效率和準確本研究的主要目標是針對日誌收容系統所收容的日誌進行各維度之分析，並以視覺化的方式呈現於介面，透過建立資安事件洞察分析平台，能夠根據長期收容資料進行事件種類趨勢分析、事件發生區域分析及事件發生安全等級分析。不僅能夠提供短時間內所需的資安事件調查，還能夠提供長時間資安事件分析，幫助了解校園面臨的資安事件趨勢，從而提升校園整體資訊安全管理效率。

貳、文獻探討

2.1 預測

人工智慧技術在資訊安全領域的應用，主要是透過分析大量數據提前發現潛在的安全威脅，並在攻擊發生前採取防護措施，甚至避免威脅的存在。深度學習(Deep Learning)屬於機器學習的子領域，基於神經網路(Neural Network)架構，模仿人類腦部功能。深度學習模型能自動從大量數據中學習並提取特徵，通過多層複雜的非線性轉換進行數據表達和模式識別。常見應用於入侵偵測系統(Intrusion-detection system, IDS)的深度學習演算法包含遞迴神經網路(Recurrent Neural Network, RNN)。

RNN 是一種適合處理具有序列數據的模型，其具有記憶功能且能捕捉序列中的時

間依賴關係。在資訊安全的應用中，RNN 可分析網路流量的時間序列數據並檢測異常模式。 然而 RNN 無法捕捉長期時間之間的關聯，會逐漸忘記早期的記憶。簡單的 RNN 結構無法解決隨遞迴權重指數級消失的問題 [11]。

基於上述 RNN 的限制，可透過衍伸出的長短期記憶(Long Short-Term Memory, LSTM) [4][5] 來解決。LSTM 包含輸入門、輸出門和忘記門，這些門能夠控制資料的流入、流出或保留，使模型能長時間記住資料，在處理長序列數據方面具有優勢 [5]。在實際應用中，LSTM 被廣泛應用於異常行為檢測和網路流量分析，如 Kim 等人 [6] 使用基於 LSTM 的入侵偵測系統模型來偵測資料集中的異常，比其他分類器表現更好，提高了對於資料和網路安全防護的能力。

為了提高模型特徵提取的自動度跟準確度，導入了卷積神經網路(Convolutional Neural Network, CNN)，CNN 擅長於從網絡流量中自動提取高維度的特徵，特別是當這些網路流量有著明顯的空間結構 [7]。

依照學者 Ma [8] 使用 CNN 和 LSTM 來進行針對防火牆決策模型的研究，CNN 與 LSTM 結合後，可以同時捕捉網絡流量的時間以及空間特徵，以此提高異常檢測的準確性和效率。CNN 可以有效地提取每個封包的空間特徵，而 LSTM 則可以記住和分析這些特徵在時間上的變化。這樣子的結果會使得 IDS 能夠更精確地識別出持續時間較長或模式較為隱蔽的攻擊行為。

2.2 分類

透過資料探勘的演算法可以辨識出攻擊，而分類是資料探勘中重要的功能之一，透過使用各種演算法將資料分類為不同類別，並在網路入侵偵測領域有著廣泛的應用，包含決策樹、單純貝氏分類器、多層感知器、隨機森林等 [3]。

學者 Aljabri 等人比較 KNN (K-Nearest Neighbor)、單純貝氏分類器、決策樹、隨機森林、人工神經網路等模型，應用在防火牆日誌的分類分析，並依照防火牆採取的回應分別為「Allow」、「Drop」、「Deny」、「Reset-both」作為分類依據，且研究結果得出透過隨機森林(Random Forest, RF)可以獲得最高的精確率 [1]。

隨機森林屬於機器學習中的監督式學習，可以用來執行迴歸和分類的任務，並透過降維的方法可以處理缺失值與異常值，性能優於其他分類器 [9]。攻擊是經常發生的，而在防火牆應用演算法來自動辨識攻擊則可以提高防禦效率。

根據學者 Thang 的研究，對於參數化的任務透過隨機森林可以提高檢索分類的精確率，為攻擊檢測奠定了基礎 [10]。學者 Aung 等人則是結合了 K-means 以及隨機森林針對入侵偵測系統實例進行分類，並發現 K-means 結合隨機森林的模型在偵測攻擊以及正常實例的正確性上，優於單一隨機森林演算法 [2]。

參、方法

本研究以「如何改進校園資安事件的管理」作為討論核心，以日誌收容系統所收容的日誌進行各維度之分析，旨在透過建立資安事件洞察分析平台，能夠根據長期收容資料進行事件種類趨勢分析、事件發生區域分析及事件發生安全等級分析。短時間內所需的資安事件調查，還能夠提供長時間資安事件分析，幫助了解校園面臨的資安事件趨勢，從而提升校園整體資訊安全管理效率。本研究流程圖如圖 1 所示。

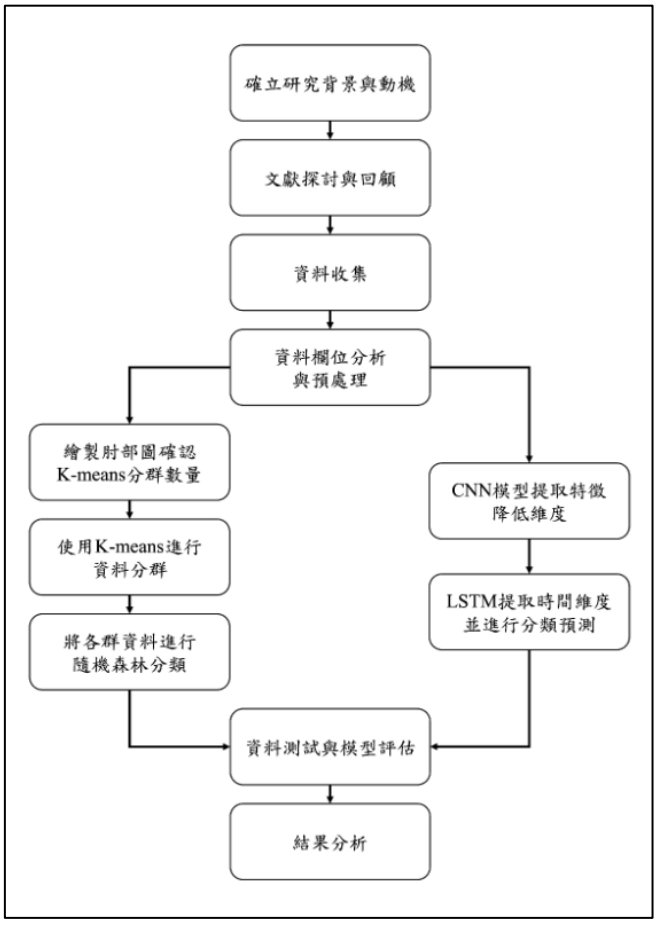

圖1，流程圖

本研究收集來自校園防火牆中的網路流量資料，這些資料包括來源 IP、威脅權重、嚴重性指數及風險指數等。使用 Python 中的 Pandas 庫進行數據收集和處理，確保數據的一致性和準確性，包括資料清洗，使用插補法填補缺失值，並排除異常數據。接著，使用 scikit-learn 庫中的 K-means 算法進行資料分群，並確定最佳分群數目。在分群後，採用隨機森林算法對資料進行分類，同時使用交叉驗證法提高模型的穩定性。

在特徵提取與模型預測階段，利用 TensorFlow 和 Keras 框架訓練 CNN 模型進行特

徵提取，隨後使用 LSTM 模型提取時間序列特徵並進行分類預測，確保模型能夠有效捕捉資料中的時間依賴性。

在模型測試與評估階段，使用 Matplotlib 和 Seaborn 進行數據和結果的可視化；利用混淆矩陣、準確度、召回率和 F1-score 等指標對模型進行性能評估。根據測試結果，進一步調整模型參數，以提高模型的準確性和穩定性。目的是為了確保數據的完整性和準確性，從而進行有效分析；分群和分類有助於了解不同類型的資安事件，從而針對性地制定防禦策略。使用先進的機器學習算法進行特徵提取和分類預測，可以提高模型的準確性和有效性。而使用多種指標對模型進行全面評估，有助於確保研究結果的可靠性和有效性。

在 15 個聚類之中，Random Forest 的整體準確度約為 96%。各聚類的分類報告中，精度、召回率和 F1-score 顯示了模型的性能。

以下為各個聚類的分類結果摘要：

聚類0：準確度為96.23%，精度、召回率和 F1-score 均表現良好。

聚類1：準確度為96.24%，在大部分分類中均達到高準確度。

聚類2：準確度為96.21%，大部分分類具有高精度和召回率。

聚類3至聚類14：均達到類似的分類效果，準確度均在96%以上。

這些結果表明，K-means 聚類和隨機森林分類器結合，可以有效地對網路威脅數據進行分類。

肆、實驗結果

4.1 威脅分析

透過對收集到的網路流量數據進行分析，可識別出多種潛在的安全威脅，如：

1. 惡意軟體攻擊：如病毒、木馬及勒索病毒等，這些攻擊可能導致數據洩露或系統癱瘓。
2. 網路釣魚：針對校園用戶的釣魚攻擊，可能導致用戶憑證被盜取。
3. 阻斷服務攻擊(DoS/DDoS)：這類攻擊可能使校園網路資源無法正常使用，影響教學與研究活動。

4.2 威脅分析

針對識別出的威脅進行了風險評估，評估其對校園資訊安全的潛在影響，風險評估的過程包括：

1. 風險等級劃分：根據威脅的嚴重性、發生概率及潛在影響，將風險劃分為高、中、低三個等級。
2. 影響分析：分析各類威脅對校園系統、數據及用戶的影響，特別是對教學、研究及管理活動的潛在干擾。

伍、結論

本研究通過結合 K-means 聚類與隨機森林分類器，實現了對網路威脅數據的有效分析。實驗結果顯示，此方法在分類準確度上具有較高的性能，可以為網路安全監測提供有效的技術。未來的工作也能夠進一步優化聚類數量和分類器參數，提升模型的泛化能力和預測準確度。

參考文獻

[1] M. Aljabri, A. A. Alahmadi, R. M. A. Mohammad, M. Aboulnour, D. M. Alomari, and S. H. Almotiri, “Classification of firewall log data using multiclass machine learning models,” *Electronics*, vol. 11, no. 12, 2022.

[2] Y. Y. Aung and M. M. Min, “An analysis of random forest algorithm based network intrusion detection system,” *in Proc. 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (*SNPD*), pp. 127-132, 2017.

[3] P. Bhoria and K. Garg, “An imperial learning of data mining classification algorithms in intrusion detection dataset,” *International Journal of Scientific & Engineering Research* (*IJSER*), vol. 4, no. 6, pp. 2394-2399, 2013.

[4] X. Du, X. Ding, and F. Tao, “Network security situation prediction based on optimized clock-cycle recurrent neural network for sensor-enabled networks,” *Sensors*, vol. 23, no. 13, 2023.

[5] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural Computation*, vol. 9, no. 8, pp.1735-1780, 1997.

[6] J. Kim, J. Kim, T.-T.-H. Le, and H. Kim, “Long short term memory recurrent neural network classifier for intrusion detection,” *in Proc. International Conference on Platform Technology and Service* (*PlatCon 2016*), pp. 1-5, 2016.

[7] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, “A survey of convolutional neural networks: Analysis, applications, and prospects,” *IEEE Transactions on Neural Networks and*

Learning Systems, vol. 33, no. 12, pp. 6999–7019, 2022.

[8] X. Ma, "CNN-LSTM based machine learning model to identify firewall decision," *in Proc. 2024 IEEE 4th International Conference on Electronic Technology, Communication and Information* (*ICETCI*), pp.951–954, 2024.

[9] A. S. More and D. P. Rana, "Review of random forest classification techniques to resolve data imbalance," *in Proc. 2017 1st International Conference on Intelligent Systems and Information Management* (*ICISIM*), pp. 72-78, 2017.

[10] N. M. Thang, "Improving efficiency of web application firewall to detect code injection attacks with random forest method and analysis attributes HTTP request," *Programming and Computer Software*, vol. 46, pp.351-361, 2020.

[11] P. TS and P. Shrinivasacharya, "Evaluating neural networks using bi-directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448-454, 2021.

[作者簡介]

林子煒先生於 2021 年取得長庚大學企業管理研究所博士班博士學位，自 2021 年 8 月起擔任逢甲大學創能學院助理教授，並於 2022 年 8 月起兼任逢甲大學資訊總處資訊安全中心主任。研究領域包括資訊安全、網路安全、密碼學、物聯網應用安全、雲端運算應用安全、醫療資訊系統、健康照護系統、行動商務、人工智慧等。

蔡國裕先生 2009 年取得國立臺灣科技大學資訊管理系博士班博士學位，現於逢甲大學資訊工程學系擔任副教授，並兼任逢甲大學創能學院資訊教學中心主任。主要研究領域為區塊鏈應用、物聯網應用與安全、行動裝置應用開發、電子商務應用，目前主要研究方向為電子貨幣、智能合約、物聯網之遠端居家照護應用、Android App 保護等。

郭崇韋先生 2016 年取得逢甲大學資訊電機學院電機與通訊工程博士學位學程博士學位，現於逢甲大學資訊工程學系擔任助理教授。主要研究領域為積體電路電磁相容、微控制器應用、硬體安全、人工智慧模型應用於軟體及硬體安全。

林玟欣小姐目前為逢甲大學資訊工程學系學生，主要接觸與研究領域為後量子密碼學，並應用於醫療資訊安全領域以及遠端照護系統安全保護。

李品臻小姐目前為逢甲大學資訊工程學系學生，主要接觸與研究的領域爲軟體開發與網站建置與設計，並應用於智慧校園場域。

梁瑋宸先生目前為逢甲大學人工智慧技術與應用學士學位學程學生，主要接觸與研究的領域為人工智慧，並應用於資料科學及業務流程優化和創新發展。

黃千芸小姐目前為逢甲大學人工智慧技術與應用學士學位學程學生，主要接觸與研究的領域為智慧物聯網，並應用於醫療與居家的智慧化發展。

范秩嘉小姐目前為逢甲大學資訊工程學系，主要接觸與研究的領域爲軟體開發、敏捷專案管理、後端維護等領域，並具有全端開發的基礎知識。透過將技術應用於實務，

致力於協助他人實現創意與使用者需求。

陳宣廷小姐目前為逢甲大學人工智慧技術與應用學士學位學程學生，主要接觸與研究的領域為人工智慧，並應用於優化行銷策略及提高產業特色及競爭力。

王富貴小姐目前為逢甲大學人工智慧技術與應用學士學位學程學生，主要接觸與研究的領域為雲端運算與數據分析，並應用於商業智慧與智慧校園資料視覺化分析。