Communications of the CCISA
Vol. 27 No. 4 Nov. 2021

基於深度學習之無線電硬體特徵識別邊緣運算架構

張禮恩[1] 陳麒元[2] 卓信宏[3]
國立宜蘭大學資訊工程學系[1, 2, 3]
[1]B0743031@ems.niu.edu.tw、[2]chiyuan.chen@ieee.org、[3]awp.boom@gmail.com

摘要

隨著近距離無線通訊 (Near-field Communication) 的普及，門禁設備的攻擊以及防禦也備受關注，然而目前市面上的不少電子門禁系統的身分驗證機制仍舊是基於門禁卡片的 UID (Unique Identifier) 進行身分識別。近年來已有相關研究成果指出，透過硬體元件之間的差異性，可有效識別出不同的裝置設備指紋 (Device Fingerprinting)，以此間接判斷使用者的合法性，以提高無線電通訊設備的資訊安全。為了解決門禁裝置身分識別上的風險，本研究使用軟體定義無線電收取 NFC 頻段訊號，提取 I/Q 訊號樣本當作特徵，利用卷積神經網路 (Convolution Neural Network，CNN)，將提取到的無線電裝置設備的特徵交由人工智慧進行學習建立模型的方法，進一步結合邊緣運算 (Edge Computing) 的架構，驗證識別 NFC 卡片複製攻擊 (Clone Attack) 的可行性。

關鍵詞：近距離無線通訊、深度學習、邊緣運算、設備指紋、身分識別、實體安全

Regular Paper

Communications of the CCISA
Vol. 27 No. 4 Nov. 2021

Deep Learning based Wireless Radio Identification Architecture for Edge Computing

Li-En Chang[1], Chi-Yuan Chen[2], Hsin-Hung Cho[3]
[1, 2, 3]Dept. Computer Science and Information Engineering, National Ilan University
[1]B0743031@ems.niu.edu.tw, [2]chiyuan.chen@ieee.org, [3]awp.boom@gmail.com

Abstract

With the popularity of Near-field Communication(NFC), attacks and defenses of access control systems have also attracted much attention. However, the identity verification of many commercial electronic access control systems at present is still based on the Unique Identifier (UID) of the access control card for identity identification. In recent years, the literature shows the difference between hardware components can effectively identify different device fingerprinting, thereby indirectly judging the legitimacy of the user, to improve the information security of radio communication equipment. To solve the risk of identification of access control devices, the software-defined radio is used to collect NFC band signals to extract I/Q signal samples as features in the study. The extracted radio device features are handed to learn and build a model, and further combined with the Edge Computing architecture to verify and identify NFC card replication.

Keywords: Near-field Communication, Deep Learning, Edge Computing, Device Fingerprinting, Unique Identifier, Security

壹、前言

隨著近距離無線通訊的發展，NFC 裝置設備成為生活中增加便利性不可缺少的一環，以 NFC 作為門禁門鎖驗證的系統也十分普遍，無論從公司企業、學校機關或是住家都可以發現。然而無線電設備的普及雖增加了生活中的便利性，但也讓駭客思考如何讓門鎖機制變成一道形同虛設的透明門。一般市售不少電子門禁使用透過唯讀的 UID 進行使用者的身分識別，但駭客可透過複製攻擊 (Clone Attack) [1]，將未加密的卡片或使用一般卡片的預設金鑰進行所有的數位資料的複製，並且無視唯讀的 UID 區塊。相關研究專家甚至有開發出特有卡片使得特有卡片的 UID 區塊位置可以無限次數的覆寫。

近期隨著硬體設備指紋的技術與研究發展，給予硬體設備獨一無二的「身分證」。透過硬體電路上的差異性，即使是相同廠商製作的相同設備，也會因為電路板上的焊接點的細微差異而導致產生的訊號也有細微的差異性。收取目標裝置設備的訊號可以當作裝置特徵，用於裝置的身份的識別。

而設備指紋的優點，是相較於以 UID 作為識別的卡片識別碼更難以被複製。雖然大多市售的 NFC 卡的 UID 可能為直接於出廠時就無法更改，即 S0B0 (Sector 0 Block 0) 為不可修改，但一般都還是能讀取到的，只需透過其他 UID 可寫的卡片以及工具如 Proxmark3[9]都有機會將卡片資訊複製。而使用硬體特徵產生出的差異性進行身份的識別可使得識別特徵更難以竄改及偽造。

軟體定義無線電 (Software-Defined Radio，SDR) 的技術從軍事及航太用途到逐漸普及市面普及。其功能讓使用者使用硬體設備，便能在廣泛的無線電射頻範圍內捕捉、解調變 (Demodulate) 並取得特定頻率的 RF (Radio Frequency)，增加了收取訊號的容易性並且軟體定義無線電能結合其他軟體達到可視化的功能，在訊號的收集提供了不少幫助。但隨著無線通訊技術發展下，訊號逐漸複雜，在特徵提取方法仍是一大難題，所幸隨著人工智慧的蓬勃發展下，深度學習以模型學習特徵，以及特徵識別能力的演進，降低了不少特徵提取的難度。

綜合上述，本研究藉由 HackRF One (Software-Defined Radio Device)，作為收取訊號的裝置，利用 RFID-RC522 作為 13.56MHz 的讀取器 (Reader)。透過主動式讀取器與 Mifare 1k[2]的 NFC 終端進行讀取區塊時，HackRF One 收取該頻段訊號，並提取出 I/Q (In-phase/Quadrature components, I/Q) 樣本資料作為設備指紋，將樣本處理後，透過卷積神經網路 (Convolution Neural Network，CNN) 進行特徵學習與識別，為提升驗證機制的可行性，本研究亦提出結合邊緣運算的架構。

在本文的第一小節，我們介紹了一些門禁安全的攻擊方式，也描述了為何使用設備指紋當作特徵。第二小節將介紹 NFC 通訊的相關資訊、NFC 訊號調變方式人工智慧背景以及設備指紋的研究文獻[5,7,8]。第三小節將介紹本研究所提出的架構及實驗結果。第四小節將進行總結。

貳、背景及相關研究

2.1 NFC 類型及操作模式

NFC 標籤類型依照 ISO/IEC 的標準下可以分為 A、B 以及 F，如圖 1 所示，操作模式主要分成三類[3]，被動模式、主動模式以及雙向模式 (Peer-to-Peer)。被動模式為 NFC 終端扮演著單純被讀取的角色，它只能在透過其他裝置設備發出的無線射頻中被動響應，提供的功能只能被讀取資訊以及被寫入資訊。主動模式為 NFC 終端不再只是單方面接受訊號的角色，在主動模式中 NFC 終端可以作為讀卡器，主動發出無線射頻去識別和讀寫其他 NFC 裝置訊息。在雙向模式下 NFC 終端與設備進行通訊方式相當於點對點，NFC 可以視情況切換成被動或主動模式中進行交換資料，如圖 2 所示。

	Polling/ Listening	Coding	Modulation	Data Rate
NFC-A	Polling	ModifiedMiller	ASK 100%	106 kb/s
	Listening	Manchester	Load modulation (OOK)	106 kb/s
NFC-B	Polling	NRZ-L	ASK 10%	106 kb/s
	Listening	NRZ-L	Load modulation (BPSK)	106 kb/s
NFC-F	Polling	Manchester	ASK 10%	212 kb/s /424 kb/s
	Listening	Manchester	Load modulation (OOK)	212 kb/s /424 kb/s

圖 1：NFC 類型對應圖

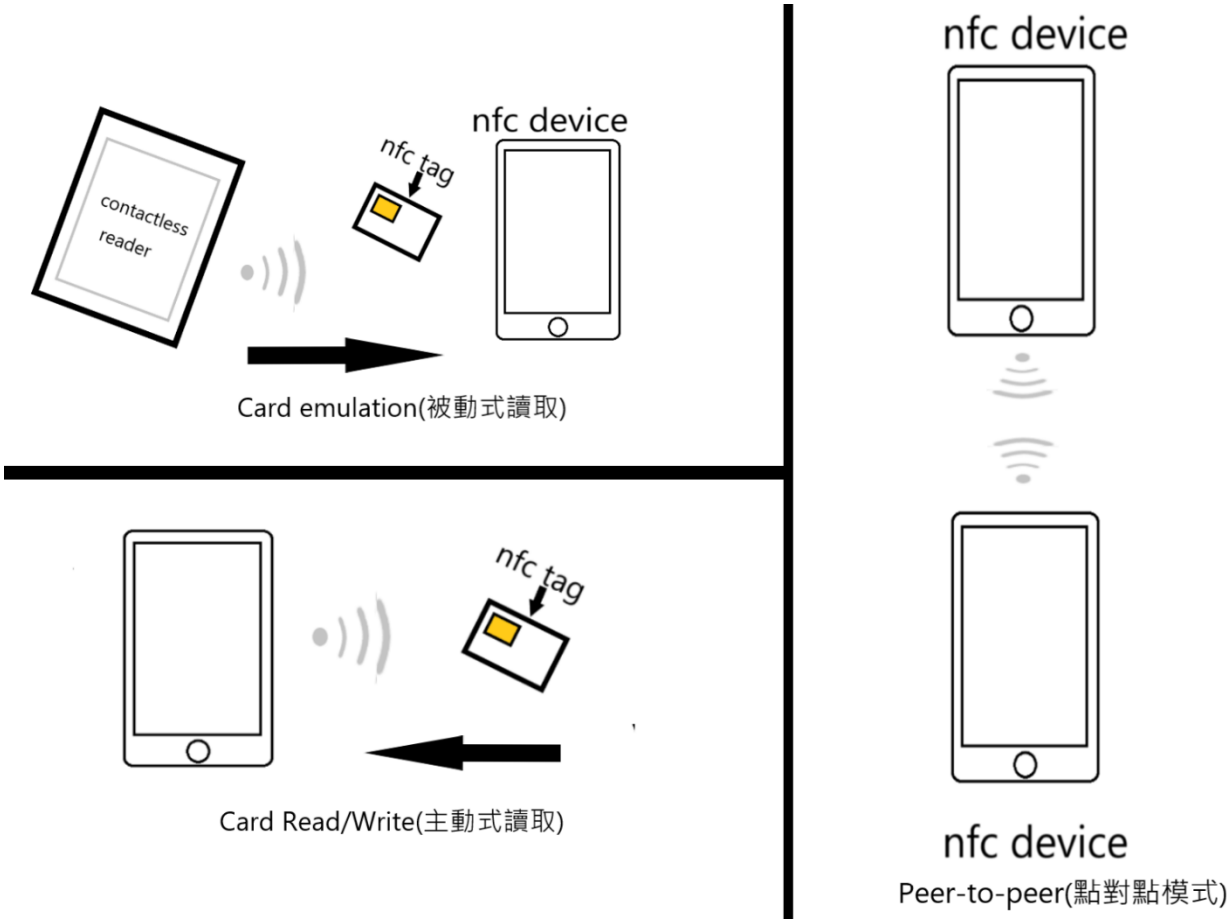


圖 2：NFC 操作模式

2.2 NFC 訊號調變及編碼

NFC 以 13.56Mhz 的頻率範圍進行資料的操作。在不同 NFC 終端類型下會使用不同深度的調變方式、編碼方式以及傳輸速率，其中包含有 10%的 ASK (Amplitude-Shift Keying)，100% ASK 的調變方法，ASK 是幅度調變 (Amplitude Modulation) 的一種形式，它將數據資訊表示為載波幅度的變化。編碼方式也包含 Modified Miller 以及 Manchester 等方法，傳輸速率範圍從 106kb/s 到 424kb/s[3]，如圖 1 所示。

2.3 人工智慧

在通訊技術的進步下，無線電技術的發展及應用也更加廣泛了，訊號的複雜程度及多樣性也隨之增長。所幸隨著人工智慧的演進，無論是在語言辨識、圖像識別、自然語言處理又或者訊號識別[4]方面都有實際不錯的應用以及表現。在訊號特徵的擷取上可以使用訊號的時域、頻域以及 I/Q 樣本等許多方法。訊號特徵研究上結合深度學習模型有

著良好的表現,[4]提到使用了軟體定義無線電收取多種無線電裝置的I/Q樣本當作特徵,透過深度學習模型學習訊號特徵後能夠成功透過訊號識別出不同的無線電裝置。

而人工智慧之所以能夠學習主要是因為在類神經網路中從大量的資料中讓多層結構的神經元在接收到資料後不斷地經過權重計算以及分類,直到最後有個輸出結果作為神經元判斷的依據,當擁有了判斷的依據後就能對輸入的資料進行判斷並給予結果。

2.4 無線電設備指紋

無線電指紋主要源自於無線電設備的各個組件在製造過程中環境的細微不同,如電路板的材質在焊接上細微的不同導致訊號經過電路調變時產生出的無線電訊號也會有細微的差異性。且這種無線電設備指紋是難以被偽造或者根本無法被偽造的,因此本研究選擇設備指紋當作學習的特徵而達到用戶的身分識別。

在[5]中提到,他們針對網路卡 (Network Interface Card,NIC) 的實體層 (Physical layer) 上進行無線電設備的辨識,使用相同廠商製造的 130 幾張相同的網路卡進行設備的辨識,並且準確度能高達 99%。為了使結果達到最完美,他們將多個訊號特徵結合進行機器學習,其中特徵包含了頻率誤差 (Frequency Error)、I/Q 偏移差 (I/Q offset) 等 5 種特徵。

在[7]中提到,當攻擊者如果能偽造憑證或者假冒身份時對於無線網路的安全造成了重大的威脅。尤其是在移動式設備 (Mobile Device) 上易受到破壞及逆向工程而取得合法節點上的密鑰,並且透過密鑰模擬出合法節點。提供了使用設備指紋技術開發新的無線電安全的解決方法,其中方法包含了基於白名單的學習方法以及非監督式學習方法在內的設備指紋演算法。

在[8]中提到了在實體層上透過深度學習的方式結合自動編碼器 (autoencoder) 的應用,並最後呈現了使用原始 I/Q 樣本上進行調變分類的應用。綜合上述,深度學習模型對於實體層的無線電設備識別技術已有良好的表現,因此我們選擇透過深度模型的方法對 NFC 訊號進行特徵提取、學習並最後能夠有效進行 NFC 標籤的身份識別進而達到防止複製卡相關的攻擊方法。

參、基於人工智慧與邊緣運算 NFC 卡片識別系統

本研究提出結合邊緣運算 (Edge Computing) 以及雲端 (Cloud) 存取技術的方式對系統架構進行整合。透過使用邊緣運算裝置如 NVIDIA 的 Jetson Nano 開發版作為深度學習模型驗證的平台。在模型訓練完成後能夠透過網路的方式,將訓練出來的模型上傳到雲端平台,提供給邊緣運算裝置佈署模型驗證環境,若讀卡機能取得卡片的 I/Q 訊號特徵的話,可以透過雲端的方式將資料傳送給邊緣運算的裝置作為判斷 NFC 卡的身份,

也能透過雲端的方式進行模型的替換及更新，如圖 3 所呈現。

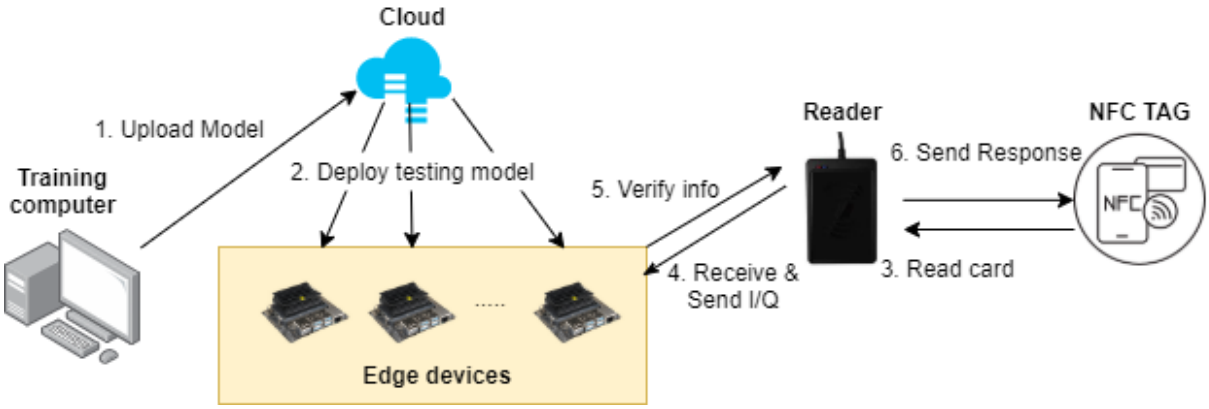


圖 3：應用架構圖

3.1 實驗架構

根據[5]所述，有許多種方法能夠決定要選取的設備指紋特徵，本研究選擇了以 I/Q 樣本在訊號調變時能夠識別硬體的方式進行實驗。我們使用軟體定義無線電 HackRF One 當作訊號的接收端並指定 13.56Mhz 的頻段，將 Mifare 1k s50 的卡片以被動式感應方式接觸 RFID-RC522 讀取器進行卡片資料的讀取，並從中提取出 I/Q 樣本。透過軟體定義無線電的方式收取訊號將會收取大量的樣本訊號，在經過實驗發現大約將 Mifare 1k s50 的卡片進行 16 個區塊讀取資料時每張卡片會產生出約 170 幾萬組 I/Q 樣本。將收取到的 I/Q 樣本進行一些前處理後，放入深度學習模型中的卷積神經網路架構，進行特徵的學習。我們這裡使用三張 Mifare 1k s50 的白卡作為合法使用者資料去做訓練並學習這三張卡片的特徵，圖 4 為實驗架構圖。

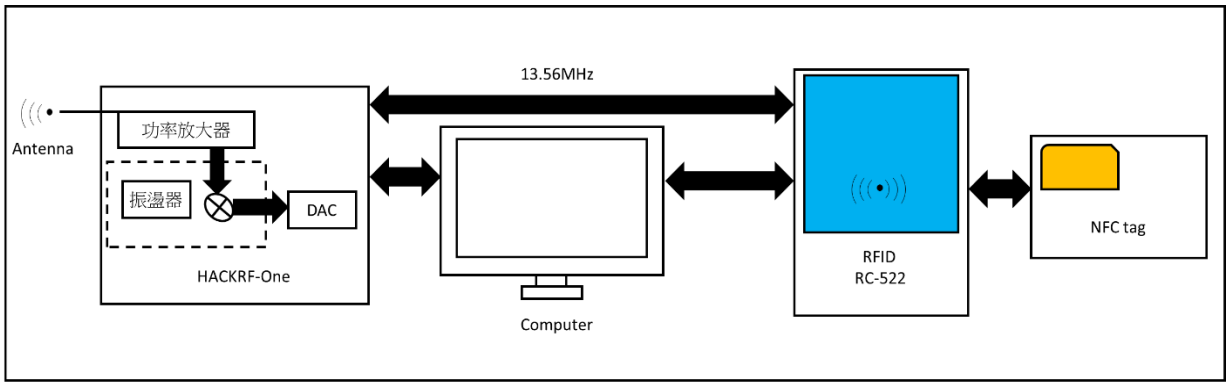


圖 4：實驗架構圖

3.2 資料前處理

實際收取到的部分 I/Q 樣本如下圖 5 所示，收取到的資料型態為複數的 I/Q 樣本，其精度為 8bit 的 ADC (Analog Digital Converter) 正交採樣。

	I	Q
1	-22	-3
2	-20	-4
3	-23	-2
4	-20	-5
5	-21	-6
6	-19	-11
7	-22	-10
8	-18	-10
9	-18	-9
10	-20	-8

圖 5：實際 I/Q 資料

我們將 I/Q 訊號先進行了資料的標準化。以 one-hot 的方式進行編碼 (label)，並取整體訊號中的前段部分作為特徵，NFC 標籤在被觸發時會有較為明顯的電位差的變化，因此前段訊號帶有較為明顯的特徵。所以我們將前段訊號中提取 256*256 個 I/Q 樣本並將 3 張合法卡收取 100 份的訊號進行上述的處理而產生出 300 份的總資料。將其中 300 份的總資料切分 7 成作為模型的訓練資料 3 成為模型的驗證資料，放入深度學習模型中進行特徵的學習。

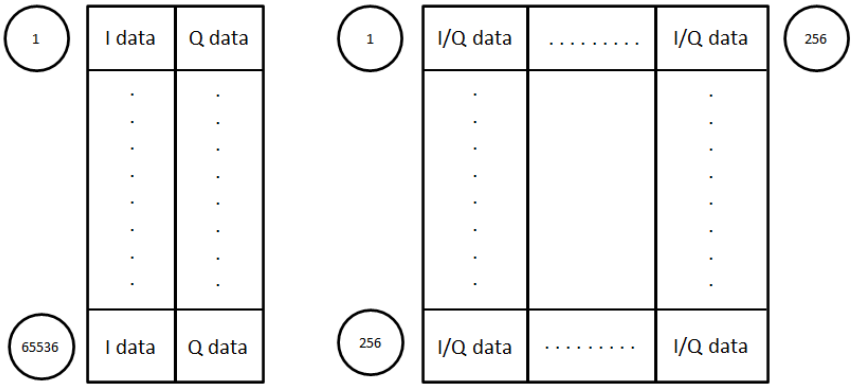


圖 6：每份 I/Q 樣本圖

3.3 神經網路架構

在神經網路架構中，我們選用卷積神經網路 (CNN)。總共使用 2 層卷積層，神經元數量皆為 64，其卷積核大小皆為 (4,4)，在 strides 使用上，兩者皆為 (2,2)，activation 皆選擇 (Rectified Linear Units，Relu)。並在每層卷積層後接上池化層，大小皆為 (3,3)，strides 皆為 (2,2)。使用 flatten 將輸入轉化成一維後，連接三層全連接層，神經元分別為 516、128 以及 64，activation 也皆選擇 (Rectified Linear Units，Relu)，最後輸出的全連接層的激活函數則使用 Softmax，如圖 7 所示。

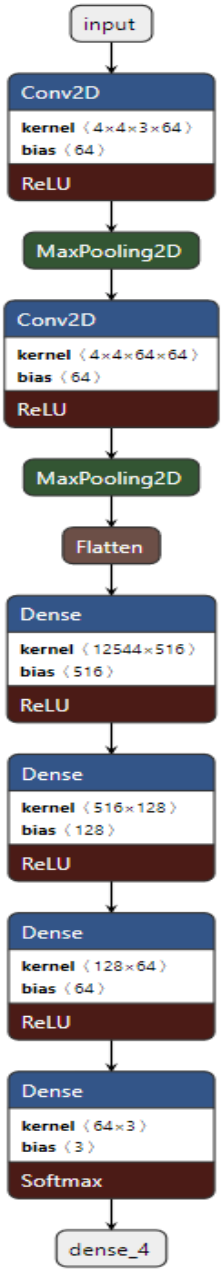


圖 7：神經網路架構圖

3.4 實驗結果

本研究在訊號特徵的學習中，我們選擇使用較長的回合數作為訓練。雖然在訓練時會有些震盪，但準確度圖 8 及損失率圖 9 皆是往理想的方向作為趨勢的。圖 8 顯示了在最終的準確度依舊能達到 9 成以上。

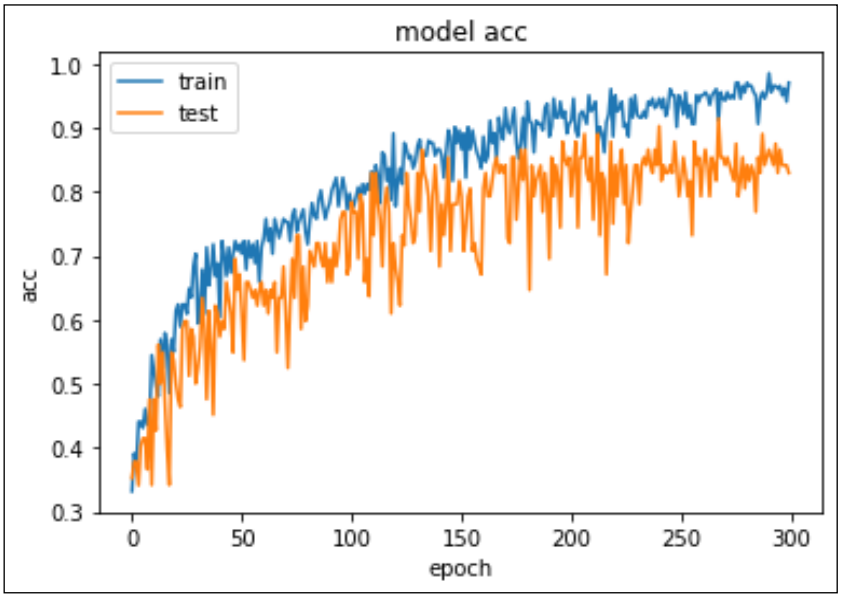


圖 8：訓練準確度圖

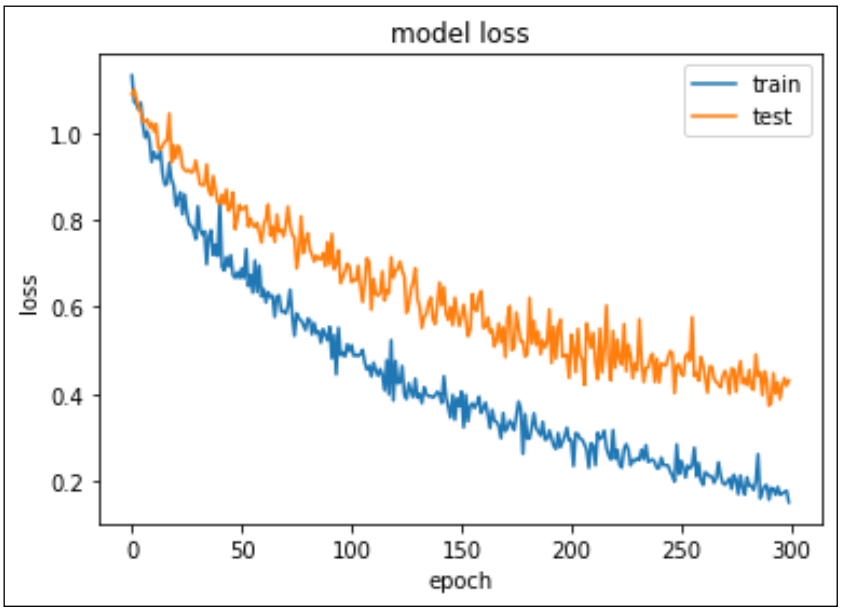
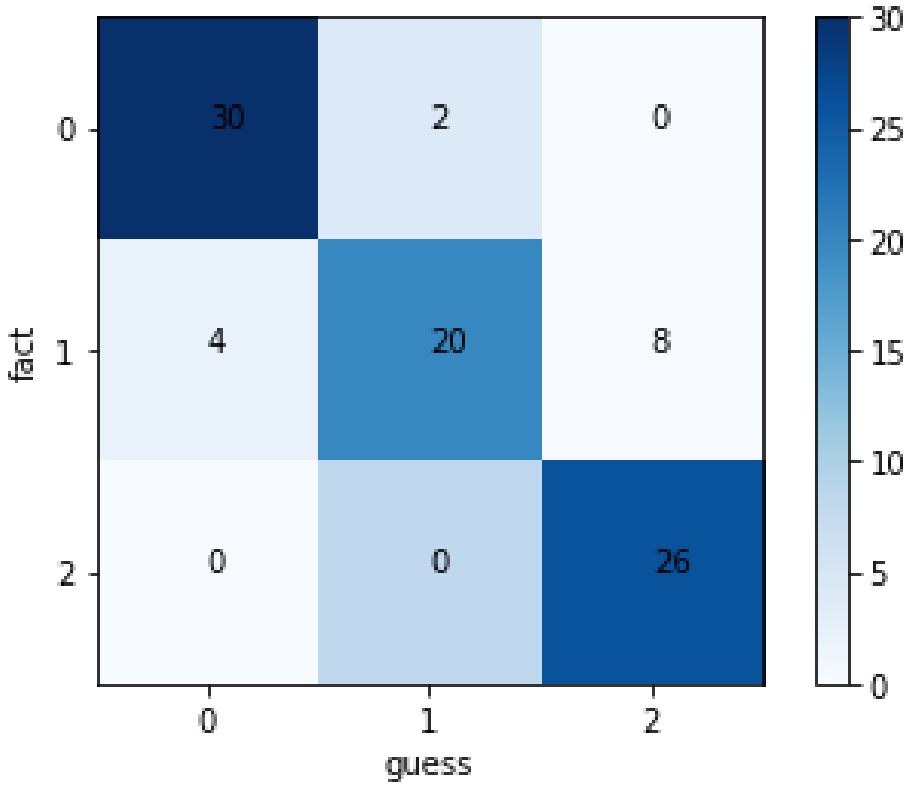


圖 9：訓練時 Loss 圖

我們在初步實驗結果呈現了在三張同個型號的 NFC 標籤(Mifare 1k s50)中，在深度學習模型學習訊號特徵中的測試資料的分辨率為 84.4%，說明了透過訊號的 I/Q 樣本是帶有裝置指紋的。表 1 為模型辨識率所產生出的混淆矩陣。

表 1：NFC 標籤辨識率混淆矩陣



本研究最終為了能夠阻擋複製卡攻擊亦設計了以白名單的方式作為身份識別的依據的方法作為使用者驗證平台。同時也在最後模型完成訓練完成後進行了驗證系統的測試，透過收取實際的合法卡訊號以及複製卡訊號對平台進行驗證。由圖 10 可以看到當合法卡進入系統時，因合法卡有事先進行特徵的提取，在特徵比對上有著高度的吻合度(紅框)，因此驗證平台可以通過驗證。

通過驗證必須要具備以下兩點：

- 明顯的硬體特徵
- 硬體特徵與白名單高度吻合

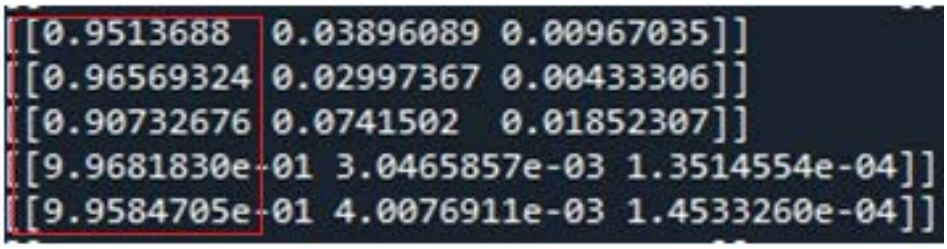


圖 10：合法卡與白名單對比結果圖

在複製卡攻擊的實作上我們使用 proxmark3 實際實現了複製卡攻擊，並將複製卡攻擊放入驗證系統中進行驗證。由圖 11 可以發現複製卡的訊號波並未符合任何白名單內的特徵，因此模型給出的結果是分散到其他張標籤上的而無法通過驗證。

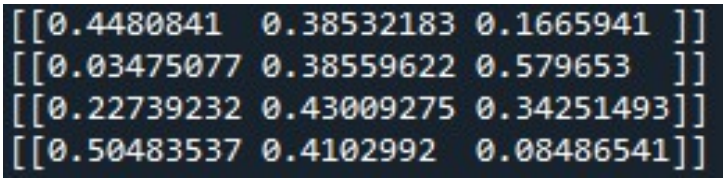


圖 11：複製卡與白名單對比結果圖

肆、結論

隨著通訊科技的進步以及 NFC 系統的普及，電子化的門禁設備也四處可見，如門鎖、電梯、倉庫及機房等地方都有所見得。而若仍使用著依靠 UID 識別身分的驗證方式，仍有高機會遭受到複製卡攻擊，導致可能有偽造身分的風險，使得有心人士可以任意進出。因此本研究採用實體層的設備指紋作為身份識別的依據。

我們使用 HackRF One 軟體定義無線電的方式進行訊號的採樣，以及為了處理大量的 I/Q 樣本以取得特徵值，我們提出了以深度學習模型的方式採用卷積神經網路對設備指紋特徵進行學習，並結合邊緣運算的架構以應對系統部署的需求。本研究證實了硬體指紋在 NFC 上的有效性，並且也透過實際測試成功阻擋複製卡攻擊。

[誌謝]

本研究由科計部計畫 MOST 110-2221-E-197-002 補助支持，特此誌謝。

參考文獻

[1] Steve Boggan, "'Fakeproof' e-passport is cloned in minutes." The Times, 6 August 2008, Available: https://www.thetimes.co.uk/article/fakeproof-e-passport-is-cloned-in-minutes-9h7jscpsbr8

[2] "MIFARE Classic EV1 1K – Mainstream contactless smart card IC for fast and easy solution development," [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf

[3] "Near Field Communication (NFC) Technology and Measurements White Paper" Available: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5E_NFC_WHITE_PAPER.pdf

[4] H. Jafari, O. Omotere, D. Adesina, H. Wu, and L. Qian. IoT devices fin gerprinting using deep learning. In 2018 IEEE Military Communications Conference (MILCOM), pages 1-9, 2018.

[5] V. Brik et al., "Wireless Device Identification with Radiometric Signatures," Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008, pp. 116-27, 2008.

[6] S. U. Rehman, K. Sowerby and C. Coghill, "Analysis of receiver front end on the performance of rf fingerprinting", 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications - (PIMRC), pp. 2494-2499, Sept 2012.

[7] Q. Xu, R. Zheng, W. Saad and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities", IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 94-104, 2016.

[8] T. Oshea and J. Hoydis, "An introduction to deep learning for the physical layer", IEEE Transactions on Cognitive Communications and Networking, no. 99, pp. 1-1, 2017.

[9] "Proxmark:Home", Available: https://proxmark.com/