Regular Paper

Communications of the CCISA
Vol. 28 No. 1 Feb. 2022

以 Bilinear Pairings 為基礎建構推播系統

吳信德 [1]
國立宜蘭大學資訊工程學系 [1]
[1]hsinte@niu.edu.tw

摘要

隨著行動裝置以及行動網路發展運用使資訊日趨透明化，許多行銷人員過去都以傳單或者信件進行產品推銷或者活動行銷資訊傳遞，由於許多行銷公司都透過簡訊、Line 或者電子郵件進行商品行銷，但這些系統都不具有網路安全保護，使得消費者的資訊遭到外洩，另外行銷人員在使用消費者資料分析時，沒有相關保護措施或者進行身分驗證，消費者相關消費資訊容易遭到惡意使用，在網路與資訊傳播時代，企業需要進行不同客戶消費分析以及產品分析，但這些資料屬於客戶的隱私，如果工作人員沒有任何授權或者隱私保護，則會造成資料洩漏，企業需要有更好的方法進行客戶資訊保護。

本文主要提出以 Bilinear Pairings 為基礎建構推播系統，本文提出法如下：1.建置推播機上盒，可將設備放置企業任何地方進行環境監控外，使用者可以設定機上盒帳密以及企業內部人員帳密，確保資料的安全性，2. 建構訊息推播系統，訊息推播方式有 E-mail、簡訊以及 Line，讓業主可以自由選擇推播方法，讓業者一次性將訊息推播到簡訊、mail 以及 Line 中，當機房有緊急事件發生時可以透過這些推播進行通報，3. 建置個資保護加密機制，避免內部人員匯出客戶個人相關資料。

關鍵詞：網路安全、推播系統、Bilinear Pairings、社群軟體、行銷系統

Regular Paper

Communications of the CCISA
Vol. 28 No. 1 Feb. 2022

Building a Push Broadcast System Based on Bilinear Pairings

Hsin-Te Wu[1]
[1] Department of Computer Science and Information Engineering, National Ilan University
[1]hsinte@niu.edu.tw

Abstract

With the development and application of mobile devices and mobile networks, information has become more and more transparent. In the past, many marketers used leaflets or letters to transmit product promotion or event marketing information. Since many marketing companies use SMS, Line or email for product marketing, However, these systems do not have network security protection, so that consumers' information is leaked. In addition, when marketers use consumer data analysis, they do not have relevant protection measures or identity verification, and consumer-related consumer information is easily malicious. Use, in the era of Internet and information dissemination, companies need to conduct different customer consumption analysis and product analysis, but these data belong to the privacy of customers, if the staff does not have any authorization or privacy protection, it will cause data leakage, and companies need to have better. method to protect customer information.

This paper mainly proposes to build a broadcast system based on Bilinear Pairings. The method proposed in this paper is as follows: 1. Build a broadcast machine top box, which can be placed anywhere in the enterprise for environmental monitoring. Users can set the set top box account secret and 2. Build a message push system. The message push methods include E-mail, SMS and Line, so that the owner can freely choose the push method, allowing the industry to push the message at one time. In SMS, mail and Line, when an emergency occurs in the computer room, you can report it through these push broadcasts. 3. Build a personal information protection encryption mechanism to prevent internal personnel from exporting personal information about customers.

Keywords: Cyber Security、Push Broadcast System、Bilinear Pairings、Social Media、Marketing Systems

壹、前言

現今許多使用者都習慣使用手機進行資訊取得，在 2019 年台灣數位廣告達到 458 億元，比往年成長 17.6%，其中社群軟體數位廣告達到 168 億元，現今大多民眾習慣使用社群軟體進行訊息傳遞或者資訊取得，因此本文推播系統加入 Line 社群軟體，並且推播訊息無上限，本文主要利用機上盒以及模組租用為主，因此價格平價有助台灣中小企業或者小型電子商務使用，訊息傳遞是行銷重要一環，因此企業可以利用本系統與客戶傳遞最新資訊，並且企業可以將客戶進行分類，並依照客群進行行銷資訊傳遞，由於中小企業人力吃緊，因此本系統導入人工智慧進行客服服務，另外本計劃會將客戶問題一一分類，有助公司進行產品改善，目前客戶資料安全性很重要，因此本文也導入資訊安全機制，確保客戶個資安全，內部人員也無法從伺服器中獲得客戶明文資料。

本文提出的產品主要可以適用於不同企業屬性的推播系統，本文提出的產品主要是以物聯網機上盒方式讓企業可以自行選擇適合的功能，並且物聯網可以連接不同感測器監控機房環境，另外物聯網機上盒可以儲存組織帳密以及相關資料，客戶資料則會利用加密方式放置伺服器中，本文利用機上盒可以有效進行企業行銷功能以及內部訊息傳送量身訂做，每一個機上盒都有獨立的加密機制驗證使用者身分，並且與伺服器端的資料加密也是獨立的。

本文主要建置具有資訊安全機制的多功能推播系統，1. 建置推播系統，可以將設備放置機房進行環境監控外，每個業主可以自行設定設備的帳密以及企業人員帳密，確保資料的安全性，因此就算企業內部員工竊取也無法得知資料明文，設備會將資料備份到伺服器中，並且與伺服器建立唯一的共同金鑰，避免其他人員進行竊取，2. 建置訊息推播系統，訊息推播方式有 E-mail、簡訊以及 Line，讓業者可以選擇各種推播方式，讓業者一次性將訊息推播到簡訊、mail 以及 Line 中，有些企業需要緊急通知時，就需要利用各種推播方式通報相關人員回公司，或者機房環境異常時也需要進行通報，3. 建立階層式訊息內容驗證機制，讓每一筆訊息內容透過組織階層驗證，避免訊息錯誤造成企業形象受損，4.建立網路安全機制，確保訊息傳送當中不被竄改。由實驗結果可以得知，本文提出的方法是可行的，並且可以實際進行運作。

貳、文獻探討

在文獻[1]中提到物聯網是感測器、嵌入式、計算和通訊技術的集成。物聯網的目的是隨時隨地為任何事物提供無縫服務。物聯網技術在任何地方都發揮著至關重要的作用，它帶來了繼物聯網和資訊通訊技術之後的第四次顛覆性技術革命。產業界預測，物聯網對社會的影響將超過互聯網和資訊通訊技術，從而改善社會和產業的福祉。解決主要的系統設計方面，如能源效率、穩健性、可擴展性、互操作性和安全問題，導致使用潛在

的物聯網系統。在文獻[2]中提到一種新穎的架構框架，它能夠以最少的功能實現物聯網平台的虛擬化，以支持特定的物聯網服務並將實例託管在靠近最終用戶的邊緣節點中。由於實例在 MEC 節點和網路切片所在的邊緣節點提供服務，最終用戶的流量無需穿越回雲端。在文獻[3]中主要目的是對物聯網領域的安全風險進行廣泛概述，並討論一些可能的對策。為此，在對物聯網領域的安全進行了大致介紹後，將討論最流行的物聯網通訊協定所採用的具體安全機制。在文獻[4]中主要物聯網正在實現前所未有的應用，這些應用基於在受限設備之間傳輸小數據量。當終端設備或傳感器節點位於地形難以接近的偏遠地區時，直接到衛星物聯網 (DtS-IoT) 已被提議作為一種有吸引力的解決方案。在 DtS-IoT 中，孤立的感測器節點可以直接在廉價的納米衛星 (即 CubeSats) 之間傳輸數據。然而，由於感測器節點和立方體衛星都在非常有限的能源供應和存儲上運行，因此對耗電通訊子系統的有效管理至關重要。

在文獻[5]中提出了 IoT 硬體平台安全架構 (IoT-HarPSecA)，這是一個 IoT 生產者提供支持的安全框架。 IoT-HarPSecA 提供了三個功能特性，即安全需求啟發、安全開發的安全最佳實踐指南，最重要的是，一個為軟體和硬體實現推薦特定輕量級加密算法 (LWCA) 的特性。在文獻[6]中提到隨著物聯網在多個領域的採用不斷增長，涉及低成本末端用戶設備的網路安全攻擊也相應增加，破壞了物聯網解決方案在廣泛場景中的預期部署。為了應對這一挑戰，新興的網路功能虛擬化 (NFV) 和軟體定義網路 (SDN) 技術可以引入新的安全推動力，從而賦予物聯網系統和網路更高程度的可擴展性和靈活性，以應對大規模物聯網部署的安全性。在文獻[7]中提到輕量級解決方案使物聯網系統的資源豐富端 (例如，邊緣、霧或云模式) 易受攻擊，因為這些端的節點具有計算量更大的加密協議的能力，並且它們在相對更惡意的環境中運行。物聯網系統的這種非對稱計算特性需要能夠適應其運行節點的資源可用性的安全協議。

在文獻[8]中提出給定物聯網一部分的受限終端設備開發一種極其輕量級的身份驗證方案。身份驗證發生在終端設備和充當邊緣計算設備的網關之間。所提出的認證方案通過正式和非正式的安全驗證。測量電壓降、電流和功率以衡量安全方案的整體影響。在文獻[9]中提到對物聯網領域的安全風險進行廣泛概述，並討論一些可能的對策。為此，在對物聯網領域的安全進行了大致介紹後，我們將討論最流行的物聯網通訊協議所採用的具體安全機制。然後，我們報告並分析了文獻中報導的一些針對真實物聯網設備的攻擊，以指出當前商業物聯網解決方案的安全弱點，並指出將安全性視為物聯網系統設計中不可或缺的一部分的重要性。在文獻[10]中提出物聯網系統面臨的主要挑戰以及區塊鏈在解決這些挑戰中的作用。它還評估了當前研究在將區塊鏈與物聯網網路合併領域的地位和最新的實施階段。此外，它還討論了與物聯網區塊鏈集成本身相關的問題。最後，本研究提出了一種架構設計，使用霧和雲計算將物聯網與區塊鏈分兩層集成。在文獻[11]提到物聯網結構、終端設備的計算能力、邊緣、霧和雲平台，並對現有的輕量級密碼協議進行了分類。對現有輕量級密碼解決方案及其優點、缺點和漏洞的比較分析突出了對能夠適應物聯網系統中不同節點的非對稱能力的彈性密碼協議的需求。在文獻[12]中提

到許多研究人員提出了許多機器學習技術模型來阻止物聯網網路中的惡意流量。然而，由於不恰當的特徵選擇，一些機器學習模型容易對惡意流量進行錯誤分類。儘管如此，仍然需要更深入研究的重要問題是如何選擇有效的特徵來準確檢測物聯網網路中的惡意流量。

參、方法

3.1 系統模組

本文系統示意圖如圖 1 所示，本計劃系統主要分為機上盒以及伺服器端，機上盒主要是由物聯網開發版當作小型伺服器，其中機上盒可以連接感測器，例如:溫溼度、火焰感測器等，也可以連接監控設備進行機房環境監控，另外機上盒可以建構小型資料庫進行資料儲存,並且資料庫具有資訊安全加密,可以避免資料被竊取時暴露客戶真實資料，在推播系統主要有 mail、簡訊以及 line 的訊息通訊功能，在伺服器端主要有模組與軟體更新、資料庫以及 XMPP 平台，企業業主可以透過機上盒安全連線到伺服器端選擇模組,伺服器端會記錄企業使用那些模組,當模組有新的軟體需要更新時,可以透過 XMPP 平台發送指令通知機上盒更新時間，業主可以選擇更新軟體時間，機上盒會主動從伺服器端下載最新模組軟體，機上盒中的資料會定期加密備份到資料庫中，避免機上盒損壞造成資料遺失。

本文主要會將客戶資料進行加密放置資料庫中，並且每一位企業機上盒與伺服器的加密金鑰皆不相同，可以確保資料的安全性，本文在機上盒中有進行語意分析以及對話機器人，當客戶傳訊息時，如果等待一段時間，客服沒有回答訊息時，會依照客戶傳送的訊息進行分析，並且啟動對話機器人回應客戶訊息，本文主要建立具有安全機制的整合式推播系統，推播系統主要以模組化方式建構，並且利用物聯網開發板建置小型伺服器，可以銜接不同的感測器設備，有助於本文提出系統的擴充性，本文使用平價式開發板有助提升系統的普及性。

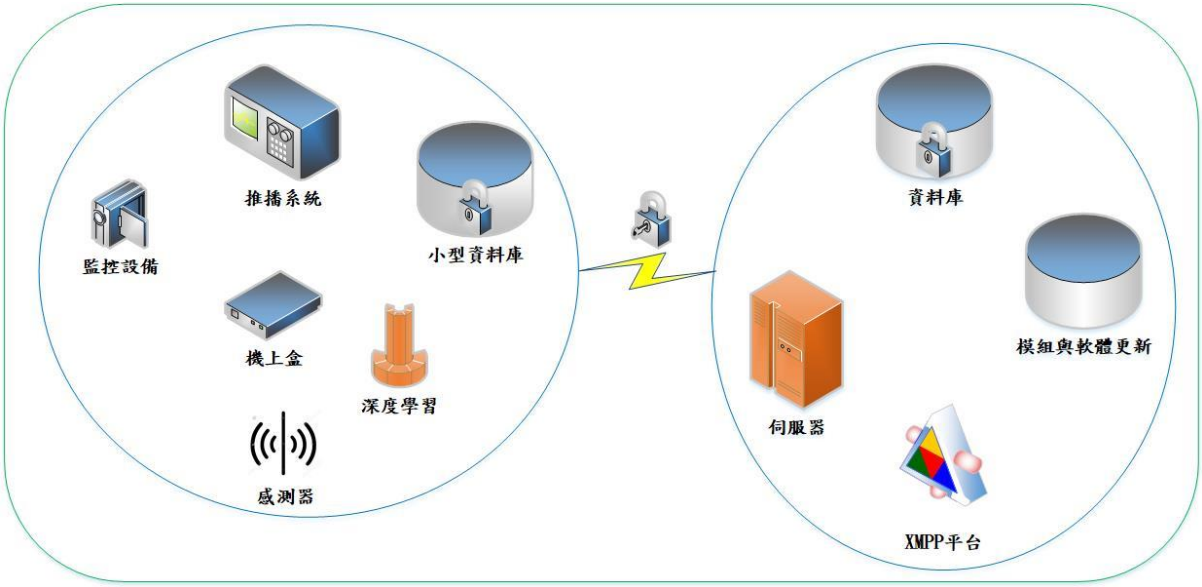

圖 1：系統示意圖

3.2 資訊安全機制建立

本文主要利用 Bilinear Pairings 建構整體網路安全機制，假設 TA 為伺服器端，首先計算 TA 以及機上盒(I_1~I_n)的 Public Key 以及 Private key 等安全係數，計算如下：

1. TA 選擇 $c \in Z_q^*$ 當作 secret key，r 是公開值。
2. TA 的 ID 為 ID_{TA}，其中 Public Key 為 $\mathrm{PK}_{\mathrm{ID}_{TA}} = \mathrm{ID}_{TA} \cdot P$，Private key 為 $\mathrm{PR}_{\mathrm{ID}_{TA}} = r^c \cdot \mathrm{ID}_{TA} \cdot P$。
3. TA 的公開值為 $\mathrm{PU}_{\mathrm{ID}_{TA}} = r^{\frac{1}{c}} \cdot P$。

接下來計算 I_1~I_n 的 Public Key 以及 Private key，計算如下：

1. I_n 的 Public Key 為 $\mathrm{PK}_{\mathrm{ID}_{I_n}} = \mathrm{ID}_{I_n} \cdot P$。
2. I_n 的 Private key 為 $\mathrm{PR}_{\mathrm{ID}_{I_n}} = r^c \cdot \mathrm{ID}_{I_n} \cdot P$。

以上 I_1~I_n 的 Public Key 以及 Private key 為機上盒預設密碼，其中 ID_{I_1} 為機上盒名稱，企業第一次連線時需要重新更改私密金鑰，此時可以利用 TA 的 Public Key 以及目前 I_1 的 Private key 建立 Common session key，Common session key 主要只有 TA 以及 I_1

得知其他使用者無法從 Public Key 中破解得知 c，計算為 $\mathrm{SK}_{\mathrm{ID}_{I_1\leftrightarrow TA}}=e\left(\mathrm{PRG}_{\mathrm{ID}_{I_1}},\mathrm{PKG}_{\mathrm{ID}_{TA}}\right)=e\left(\mathrm{PKG}_{\mathrm{ID}_{I_1}},c\cdot\mathrm{PKG}_{\mathrm{ID}_{TA}}\right)$，接下來 TA 與 I_1 就可以利用對稱式加密 SK 進行私密通訊，計算如演算法 1，首先 I_1 選擇 $s\in Z_q^*$ 當作 secret key，接下來計算 TA 新的 Private key 並利用 SK 將訊息加密後傳送給 TA，TA 一開始利用自己的 Private key 與 I_1 原本的 Public Key 計算出 common session key 進行解密，接下來收到新的 Private key($\mathrm{PR}_{\mathrm{ID}_{I_1}}$,)後，TA 會重新計算 SK($\mathrm{SK}_{\mathrm{ID}_{I_1\leftrightarrow TA}}$,)，並且利用自己的 Public Key 將 $\mathrm{PR}_{\mathrm{ID}_{I_1}}$,加密儲存在資料庫中，TA 利用 $\mathrm{SK}_{\mathrm{ID}_{I_1\leftrightarrow TA}}$,將自己的 Public Key 加密後傳送給 I_1，I_1 收到訊息解密後會再回傳給 TA 告知已經收到訊息。

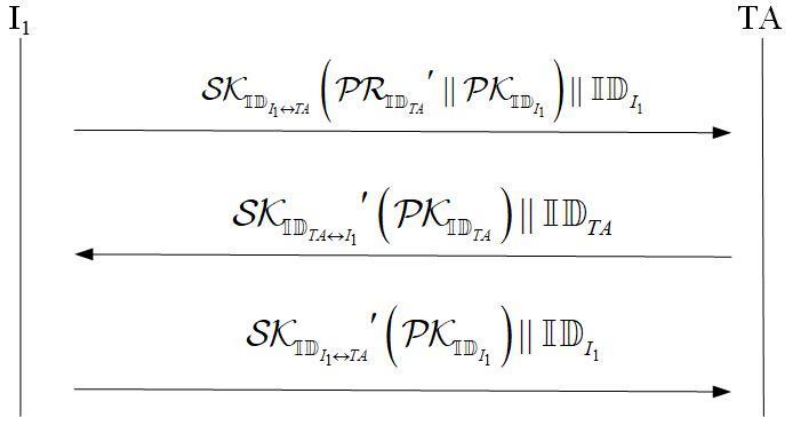

圖 2：演算法 1

3.3 資料備份機制

本計畫機上盒會將客戶資料以及相關資料備份到資料庫中，首先 I_1 會利用自己的 Public key 加密，再利用與 TA 的 $\mathrm{SK}_{\mathrm{ID}_{I_1\leftrightarrow TA}}$,將資料加密後傳送給 TA，計算為 $\mathrm{SK}_{\mathrm{ID}_{I_1\leftrightarrow TA}}{}'\left(\mathrm{PK}_{\mathrm{ID}_{I_1}}(M)\|H\left(\mathrm{PK}_{\mathrm{ID}_{I_1}}(M)\right)\right)\|\mathrm{ID}_{I_1}$，當 TA 收到密文後，利用 common session key 解密，接下來驗證訊息的完整性，TA 利用雜湊技術將 $\mathrm{PK}_{\mathrm{ID}_{I_1}}(M)$ 進行計算，如果與 $H\left(\mathrm{PK}_{\mathrm{ID}_{I_1}}(M)\right)$ 相同，表示訊息沒有被竄改過，接下來 TA 會利用自己的 Public Key 加密，並且儲存在資料庫中，當內部人員竊取資訊時，無法得知真正資料 M，就算內部人員竊取 TA 的私密金鑰進行解密，也無法解密 $\mathrm{PK}_{\mathrm{ID}_{I_1}}(M)$。

肆、實驗結果

本文在網路安全分析方面主要利用表 1 所示，透過加解密效能分析來計算本文的加解密效能，如表 2 所示，本文的加解密方法在可接受範圍內。

表 1、加解密速度

符號	描述	執行速度 (ms)
T_p	配對計算	≈4.5
T_m	點乘法群	≈0.6
T_e	雙線性配對	≈0.54
H	HMAC	0.002
S_e	AES 加密	<0.19
S_d	AES 解密	<4.65
$S_e^{'}$	非對稱加密	0.19
$S_d^{'}$	非對稱解密	4.65

表 2、本文執行方法效能分析

項目	**本文提出的方法**
身分驗證	執行速度: 9.68 (ms)
私密通訊	執行速度: 4.84 (ms)
隱私	執行速度: 9.68(ms)

伍、結論

本文提出的系統有助推播系統的安全性，本文提出的方法可以在階層式架構進行每位身分驗證以及私密通訊，本文提出的方法有助企業推播系統資訊的安全性，並且推播方式多元化有助企業多種選擇，本文提出的建立網路安全機制，確保訊息傳送當中不被竄改，由實驗結果可以得知，執行效能在可接受範圍內。

[誌謝]

This work was supported in part by the Ministry of Science and Technology of Taiwan, R.O.C., under Contracts MOST 109-2622-E-197-012 and MOST 110-2622-E-197-015. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

參考文獻

[1] S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," IEEE Access, vol. 8, pp. 188082-188134, 2020, doi: 10.1109/ACCESS.2020.3029847.

[2] J. Hwang, L. Nkenyereye, N. Sung, J. Kim and J. Song, "IoT Service Slicing and Task Offloading for Edge Computing," IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11526-11547, 15 July15, 2021, doi: 10.1109/JIOT.2021.3052498.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[4] R. Ortigueira, J. A. Fraire, A. Becerra, T. Ferrer and S. C?spedes, "RESS-IoT: A Scalable Energy-Efficient MAC Protocol for Direct-to-Satellite IoT," in IEEE Access, vol. 9, pp. 164440-164453, 2021, doi: 10.1109/ACCESS.2021.3134246.

[5] M. G. Samaila, J. B. F. Sequeiros, T. Sim?es, M. M. Freire and P. R. M. In?cio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," in IEEE Access, vol. 8, pp. 16462-16494, 2020, doi: 10.1109/ACCESS.2020.2965925.

[6] A. M. Zarca, J. B. Bernabe, A. Skarmeta and J. M. Alcaraz Calero, "Virtual IoT HoneyNets to Mitigate Cyberattacks in SDN/NFV-Enabled IoT Networks," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1262-1277, June 2020, doi: 10.1109/JSAC.2020.2986621.

[7] M. N. Khan, A. Rao and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, 15 March15, 2021, doi: 10.1109/JIOT.2020.3026493.

[8] S. Sathyadevan, K. Achuthan, R. Doss and L. Pan, "Protean Authentication Scheme - A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments," in IEEE Access, vol. 7, pp. 92419-92435, 2019, doi: 10.1109/ACCESS.2019.2927818.

[9] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[10] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," in IEEE Access, vol. 9,

pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[11] M. N. Khan, A. Rao and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, 15 March15, 2021, doi: 10.1109/JIOT.2020.3026493.

[12] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.