BLOCKCHAIN® IN HEALTHCARE TODAY

敘述/系統回顧/元分析

網路安全的新趨勢：全面檢視當前威脅、評估解決方案、開拓新領域

Taskeen Zaid，博士[1] 和 Suman Garai，MBA[(2*)]

[1]印度卡納塔克邦班加羅爾 Jain (Deemed to be University) 資訊科技副教授；[2]印度奧迪沙邦布巴內斯瓦尔 Kalinga 工業技術學院。

*Corresponding Author：Suman Garai，電子郵件： mr.sumangarai.3122@gmail.com DOI:

https://doi.org/10.30953/bhty.v7.302

Keywords: Comparative analysis, cyber defense, cybersecurity, digital threat landscape, innovative framework, safeguard information

摘要

在以數位進步為主的時代，網路安全在保護資訊和系統免受不斷演進的威脅方面扮演著關鍵的角色。網路威脅的複雜性不斷提升，因此有必要對當前防禦系統的效能進行嚴格檢驗。本研究意識到目前解決方案的限制與缺口，因此引進一個旨在強化網路防禦的先進架構。本研究透過對研究文章、調查、線上媒體和實際研究的全面探索，仔細檢視網路威脅的複雜性，並評估現有解決方案的優缺點。建議的架構來自於縝密的可行性與實用性研究，並利用從不同線上來源所獲得的洞察力。如何 "則包含比較分析，針對既有解決方案評估新穎架構，以釐清各自的優點與缺點。本研究背後的動力在於提供研究人員、實際執行者和決策者寶貴的見解，以應付網路安全的多重挑戰。本論文透過現有解決方案的複雜性，並引進創新架構，旨在引導加強網路防禦的工作。最後，隨著利益相關者共同致力於適應瞬息萬變的數位威脅環境，本研究將在網路安全領域中持續循環改進與演進。

提交：2024 年 2 月 24 日；接受：2024 年 4 月 19 日；發表：2024 年 4 月 30 日

本文作者嘗試全面調查當今的網路威脅現況，仔細檢視現有的安全解決方案，並提出新穎的改善架構。主要目標包括徹底檢視目前的威脅狀況、分析目前的安全威脅、評估現有的解決方案，並指出其內在限制。本研究針對網路安全的特定領域介紹兩種創新解決方案，並與既有的安全措施進行詳細的比較分析，闡明其各自的優缺點。本研究採用的方法包括廣泛的文獻回顧、可行性與實用性研究，以及比較分析，奠定了本研究的基礎。它是產生洞察力、實際改進和確定未來研究方向的堅實基礎。

歷史觀點

在熙來攘往的數位時代，我們的生活與網際網路無縫交織。我們在網路上存錢、在社群媒體上分享想法，並將我們的秘密託付給雲端儲存。但是，在這種便利性之下，卻隱藏著一個數位威脅的陰影世界，惡意的行為者試圖利用漏洞，危害我們珍貴的資料。這個被稱為網路安全的領域，已經從間諜和密碼破譯員的領域，演變成個人、企業和國家的 重要戰場。瞭解其發展歷程 - 從早期的

網路安全的種子是在第二次世界大戰的混亂中播下的。

網路安全的種子是在第二次世界大戰的混亂中播下的。為了確保軍事通訊的安全，德國等國家部署了 Enigma 等先進的加密機器，創造出複雜的密碼，困擾盟軍情報單位多年。由布萊奇利公園 (Bletchley Park) 的傑出團隊率先破解 Enigma 的故事，證明了這個領域的智慧與決心。即使在電腦還未普及之前，密碼學已經成為對抗竊取機密和擾亂行動的對手的第一道防線[1]。

數位革命之後，重點從實體密碼轉移到電腦系統和網路的安全防護。早期只有個別事件，例如 1988 年的 Morris 蠕蟲攻擊，但隨著網際網路的擴展，網路威脅的複雜性和頻率也隨之增加。駭客為了惡作劇、詭計或經濟利益，利用作業系統、網站和使用者行為的漏洞。病毒、蠕蟲和惡意軟體氾濫，以重要基礎設施、企業甚至個人為目標。網路犯罪集團的興起增加了一層有組織的惡意，助長了資料外洩和身份盜用等攻擊[2]。

隨著這些數位敵人的演進，網路安全防衛者的武器庫也在演進。防毒軟體、防火牆和入侵偵測系統成為網路防禦的重要工具。各國政府紛紛成立網路安全機構並制訂政策。國際合作變得非常重要，促使簽訂旨在打擊網路犯罪和提倡負責任的網路行為的條約和協議。今天，網路安全是一個價值數十億美元的產業，僱用了來自不同背景的技術專業人員：道德駭客、網路安全工程師、惡意軟體分析師和事件回應專家[3]。

然而，軍備競賽仍在繼續。駭客不斷創新，利用人工智慧 (AI) 和區塊鏈等新興技術發動新式攻擊。贖金軟體、網路釣魚詐騙和供應鏈攻擊只是不斷演進的威脅範圍中的幾個例子。風險比以往更高：關鍵基礎建設、醫療保健系統，甚至民主程序都可能成為攻擊目標。當我們邁向日益互聯的未來時，對於強大網路安全措施的需求從未如此殷切[4]。

網路安全的歷程見證了人類的智慧以及攻防之間的不斷鬥爭。從戰時秘密的密碼破譯世界到今日複雜的數位戰場，這個故事強調了意識、警戒與合作對於保護我們數位生活的重要性。當我們在不斷演進的網路環境中遨遊時，瞭解其歷史和當前的挑戰，將有助於我們為所有人打造更安全、更有彈性的未來。

近期的數位安全風險

近年來，網路安全威脅的嚴重性與數量大幅增加，導致許多企業蒙受重大財務損失與聲譽受損。令人遺憾的是，幾個真實案例 (圖 1) 顯示了這些威脅的嚴重性。

供應鏈攻擊是一種複雜的網路戰爭形式，涉及攻擊協力廠商供應商以未經授權存取目標系統。此方法可讓攻擊者利用第三方供應商之間建立的信任。

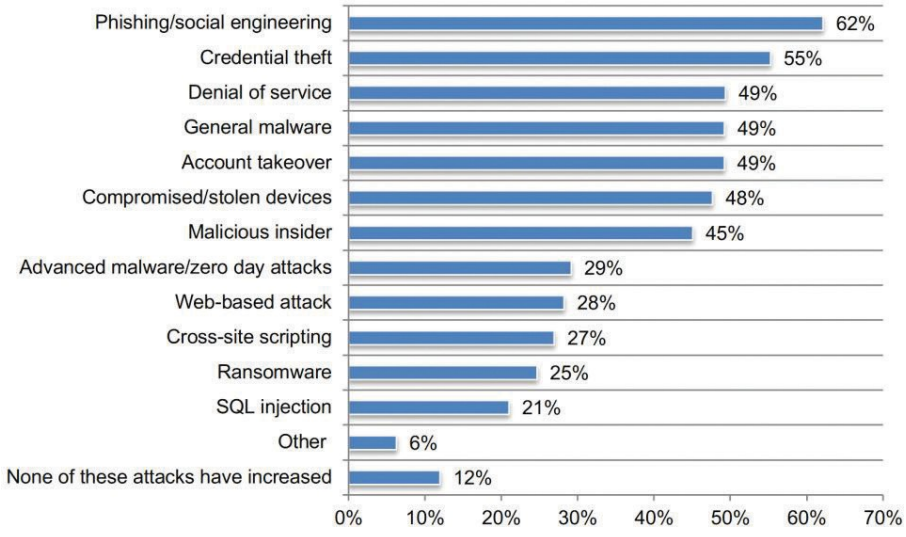


圖 1. 說明自 COVID-19 以來各種網路威脅增加的調查報告。SQL：結構化查詢語言

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

組織及其供應商。2020 年 SolarWinds 攻擊就是此策略的明證，俄羅斯駭客利用 SolarWinds 更新程序中的漏洞，滲透數以千計的組織網路[5]。

利用物聯網 (IoT) 裝置的漏洞是網路威脅的另一個層面。2016 年針對 Dyn 的 Mirai 殭屍網絡攻擊就是一個顯著的例子，該攻擊利用經過編譯的 IoT 裝置發動大規模的分散式拒絕服務 (DDoS) 攻擊，以大量流量淹沒任何伺服器或網路，造成美國東部地區大量網站中斷，估計造成 1.1 億美元的損失[(6)]。

先進持續性威脅 (APT) 涉及未經授權的使用者在未被察覺的情況下長時間存取系統。2015 年，中國駭客對美國人事管理辦公室 (OPM) 執行大規模 APT，洩露了超過 2,100 萬名個人的個人資料。[7]APT 的特點在於其隱蔽性，通常由民族國家行動者驅動，目的在於竊取敏感資料或進行其他攻擊。OPM 外洩事件突顯出組織在偵測和減緩 APT 方面所面臨的重大挑戰。

贖金軟體攻擊會加密受害者的資料，並要求支付解密金鑰。[8]另一個值得注意的事件是 2021 年的 Colonial Pipeline 攻擊，贖金軟體攻擊中斷了整個美國東部的燃料供應，強調了網路安全在保護重要基礎設施中扮演的關鍵角色。[9]社會工程是網路犯罪者使用的一種策略，以操控個人揭露敏感資訊或採取危害安全的行動。2023 年，MGM Resorts 遭受一場複雜的社交工程攻擊，駭客假冒合法供應商取得存取權，並竊取未發行的電影劇本、機密財務文件和員工資訊。

資訊。

Deepfakes 是超逼真的篡改視訊或錄音，為社交工程增添了一層複雜的技術。這些「合成媒體」工具所構成的威脅與日俱增，讓攻擊者能夠冒充高階主管、散佈不實資訊或進行複雜的勒索計畫。蘭德公司 (RAND Corporation) 在 2020 年進行的一項研究警告說，虛假訊息可能會用於破壞選舉、操縱金融市場，以及侵蝕公眾信任。[(11)]2023 年涉及女演員 Rashmika Mandanna 的虛假訊息案件展示了這項技術所造成的威脅正在不斷演變，它會造成困擾和聲譽損害。

帳戶盜用正在增加，同時影響個人和大型組織。在 2019 年，Capital One 經歷了一次重大的帳戶接管攻擊，駭客取得了數百萬使用者的個人資料。

用戶的個人資料。後果非常嚴重，黑客能夠存取社會安全號碼、信用評分和銀行帳戶號碼，導致 Capital One 被罰款 8,000 萬美元[13]。

憑證竊取是攻擊者常用來存取敏感資訊或系統的手法。2018 年萬豪國際集團 (Marriott International) 資料外洩事件暴露了約 5 億名住客的個人資料，原因是駭客從第三方廠商竊取登入憑證。萬豪因此面臨 1.23 億美元的罰款[14]。

惡意內部人員，即擁有組織系統授權存取權限的個人，如果濫用該存取權限，可能會構成重大威脅。2019 年，特斯拉的一名前員工被指控從公司系統中竊取機 密資訊和智慧財產。[(15)]2023年，五角大樓的機密文件洩漏至一個電玩遊戲聊天群組，這也突顯了內部威脅的隱蔽性。

Stuxnet 蠕蟲是零時差攻擊的一個顯著例子，攻擊者利用軟體中先前未知的漏洞。[17]它以工業控制系統為目標，利用 Windows 和 Siemens 軟體中的數個零時差漏洞來修改程式邏輯控制器，並可能造成實體損害。該攻擊被認為是由民族國家動員所進行，對網路武器的發展及零時差漏洞在戰爭中的使用有重大影響。

這些例子顯示了網路安全攻擊可能造成的破壞性財務與聲譽後果。公司可能面臨法律制裁、客戶流失，以及品牌聲譽的重大損害。此外，敏感資訊的遺失、關鍵基礎設施的中斷，以及身份盜竊和詐欺風險的增加，都可能使整個社會蒙受損失。鑑於這些風險，組織必須認真看待網路安全，並投資於強大的安全措施，以保護其系統和資料的安全。

目前防禦網路威脅的措施

在動態的網路安全領域中，領先不斷演進的威脅是最重要的。為了達到這個目標，組織必須運用最先進的解決方案。本探討深入探究六項關鍵進展，揭示其功能、優點和實際應用。

其中一個關鍵進展是整合人工智能和機器學習 (ML) 作為數位哨兵（表 1）。它們的強項在於即時分析大量資料流、解密網路流量、使用者行為和系統日誌。這可讓它們從現有的弱點中學習，並預測未來的攻擊模式。AI 與 ML 行動

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

*表 1.*機器學習在網路安全領域的使用選項[19]

使用案例	說明
弱點管理	根據關鍵性為 IT 與安全團隊提供建議的弱點優先順序。
靜態檔案分析	根據檔案的特徵來預測檔案的惡意程度，從而預防威脅。
行為分析	在執行時分析對手行為，以建立模型並預測整個網路殺戮鏈的攻擊模式。
靜態與行為混合分析	結合靜態檔案分析與行為分析，提供進階威脅偵測。
異常偵測	識別資料中的異常現象，為風險評分提供資訊，並指導威脅調查。
鑑識分析	執行反情報分析，以分析攻擊進程並辨識系統弱點。
沙箱惡意軟體分析	在隔離、安全的環境中分析程式碼樣本，以辨識和分類惡意行為，並將其對應到已知的對手。

IT：資訊技術。

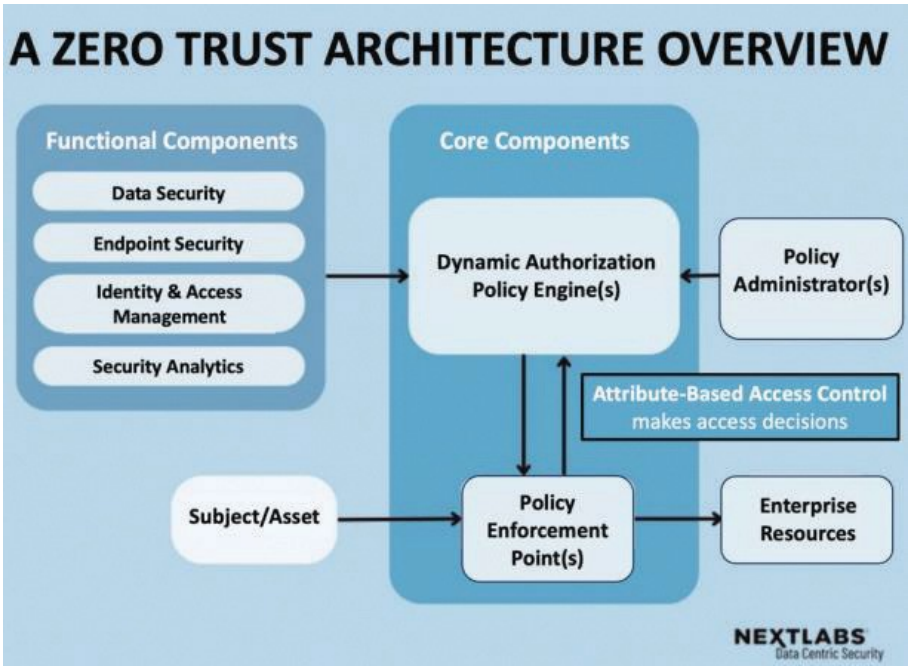


*圖 2.*為企業建立 ZTA 解決方案。ZTA：零信任架構[21]

就像超人的監控系統一樣，能夠即時識別網路活動中的細微異常、不尋常的登入嘗試，以及可疑的檔案修改。這有助於縮短回應時間，讓組織能夠及早偵測威脅，防止資料外洩。此外，這些技術擅長於識別零時差攻擊，針對新型威脅提供重要的防禦層。AI 驅動事件回應的優點在於反應迅速。這些系統可以自動隔離受到感染的系統、修復漏洞，甚至收集證據並產生報告。這不僅能防止威脅擴散，還能簡化分析流程，為加強未來防禦提供寶貴的洞察力[18]。

傳統的安全方法類似於「城堡與鎧甲」（castle-and-moat），在今日互聯的世界中已經變得過時。零信任架構 (ZTA) 可透過微區隔、存取控制來實現范式轉移、持續認證與授權。ZTA 環境可將網路分割成小型堡壘，每個堡壘都存放特定的資料或應用程式。實施最少權限存取可防止未經授權的網路橫向移動 (圖 2)。動態信任驗證可確保在整個階段中持續驗證信任，以適應不斷演變的風險狀況。ZTA 採用了「類固醇」的多因素安全系統。除了密碼之外，它還利用指紋、生物特徵掃描或一次性代碼等因素進行使用者驗證。基於風險的認證會考慮用戶背景和設備類型等因素，並根據評估的風險調整認證要求[20]。

除了加密貨幣之外，區塊鏈的分佈式防篡改總帳也為網路安全提供了獨特的優勢，包括安全的資料來源、防篡改、安全的身份管理以及分散式的身份管理。

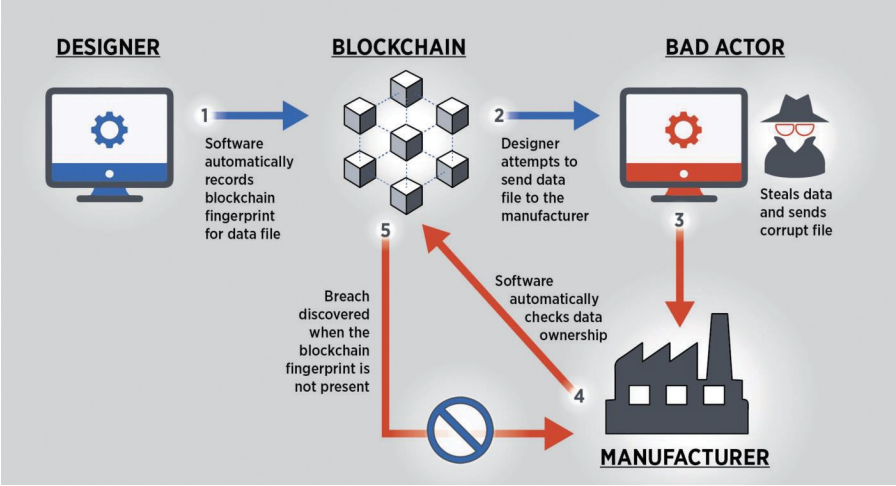


*圖 3.*區塊鏈保護資產的概括概念[22]

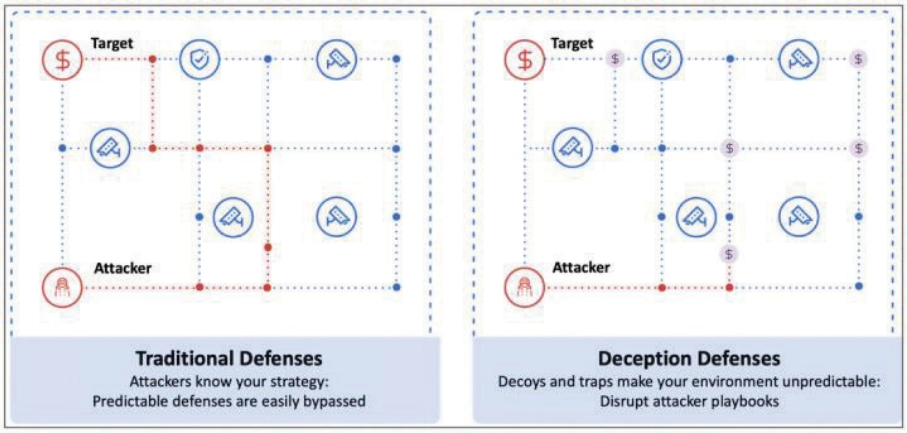


*圖 4.*騙局概念的 Pac-Man 風格範例[24]。

身份。區塊鏈採用加密雜湊和分散式總帳來保護資料區塊。每個區塊都有獨一無二的數位指紋，任何異動都能立即被偵測出來。整個網路中的分散式帳本使得篡改幾乎不可能發生。區塊鏈引入了分散式身份 (DID) 和可驗證憑證 (VC)。DID 允許使用者控制其身份資料，消除單點故障。可驗證憑證 (VC) 可讓使用者在不依賴中介的情況下發行和分享憑證，從而降低欺詐風險（圖 3）[23]。

欺騙技術可創造虛假的數位現實，利用誘捕系統、誘捕站、威脅模擬和模擬技術來誤導網路罪犯，使其失去能力。誘捕系統和誘捕站可作為數位誘餌和陷阱。誘捕系統與實際系統類似，可誘使攻擊者浪費時間。誘捕系統捕捉攻擊者的策略和技術，為安全團隊提供寶貴的情報。威脅模擬和模擬複製實際的攻擊媒介、讓組織可以測試其防禦措施並找出弱點。這些模擬可揭露現有安全控制的弱點，有助於優先修補弱點和強化防禦（圖 4）[25]。

健全的法律架構對於風險減緩和責任追究至關重要。這些法律措施與技術進步相輔相成，可提供針對惡意行為者的全面防禦。一般資料保護條例》、《網路安全資訊分享法案》(CCPA) 以及其他地區性法律設定了資料安全標準，提升了整個產業的網路安全。關鍵基礎設施保護規定了特定的安全控制，以保護重要系統免受網路威脅。CISA 鼓勵公私協作，並透過共享威脅情報進行快速回應。[26]《布達佩斯公約》等全球協定促進了針對網路犯罪的合作努力。美國的《電腦欺詐與濫用法》等法律將各種網路相關犯罪列為刑事犯罪，從法律上阻遏網路犯罪。

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

惡意活動。[27]英國的 Regulatory Sandbox 等計畫允許在受控的環境中測試新興的網路安全技術，加速開發並促進創新以因應新的威脅。定期審查和更新法律與框架對於跟上威脅形勢的演進至關重要。政策制定者、安全專家和產業利害關係人之間的開放式對話，可確保架構保持相關性。

行為生物識別技術可根據獨特的特性（如按鍵動態、滑鼠移動和登入習慣）識別使用者，從而為安全性增添新的層面。行為生物識別技術會持續監控使用者的活動，包括按鍵動態、滑鼠移動和登入習慣。這會創造出一個數位守衛，監視使用者的一舉一動，透過辨識偏離既定使用者設定檔的情況來加強安全性。這種形式的生物識別技術會根據使用者的風險概況調整防禦措施。高風險情況會觸發額外的生物識別驗證步驟，而低風險活動則保持簡化，提供友善的使用者體驗。行為生物識別技術還可以通過識別用戶行為的異常變化來輔助詐騙檢測（圖 5）[(29)]。

雖然這六項進展標誌著網路安全的重大進步，但現況仍在持續演進中。量子運算、安全多方運算 (SMPC) 和同態加密等技術，都有希望進一步強化防禦能力。然而，為了建立彈性且安全的數位環境，整體性的網路安全策略是必要的。這包括結合先進的技術、傳統的安全實務，以及促進全球合作，以對抗不斷演變的 威脅。了解不同地區的法律環境區域之間的法律環境差異對於此類策略的有效性至關重要。

分析目前針對現實世界威脅的網路復原措施

深入檢視針對多元數位威脅的防禦策略，可以發現先進技術與全面性架構之間複雜的互動關係。這種錯綜複雜的舞蹈涉及 AI、ML、ZTA、區塊鏈、法律架構和強大的網路安全實務之間的共生關係，形成了多重網路安全防禦機制。

AI 和 ML 都是警惕的哨兵，透過廣泛的資料分析來識別受入侵的元件，並偵測可疑的 IoT 活動。這可完美補充建立業界最佳實務的強大網路安全框架。即使在潛在滲透發生後，ZTA 也能限制橫向移動，進一步強化安全性。區塊鏈是一種不可變的總帳，它的使用可確保元件的來源追蹤，解決供應鏈中的真實性問題。結合認可網路安全框架的指引，例如美國國家標準與技術研究院的網路安全框架工作，可增強區塊鏈的安全實施。必須承認人工智能偏差的潛在可能性，強調道德考量和多樣化訓練資料集的重要性。此外，雖然 ZTA 的複雜性需要專業知識，但應用網路安全框架作為實作藍圖可以減少挑戰。解決當前區塊鏈實施中的可擴展性限制需要協作努力和明確的法規。

轉到 DDoS 攻擊領域，AI 和 ML 在迅速回應異常流量模式、減輕其影響方面扮演重要角色。協調事件

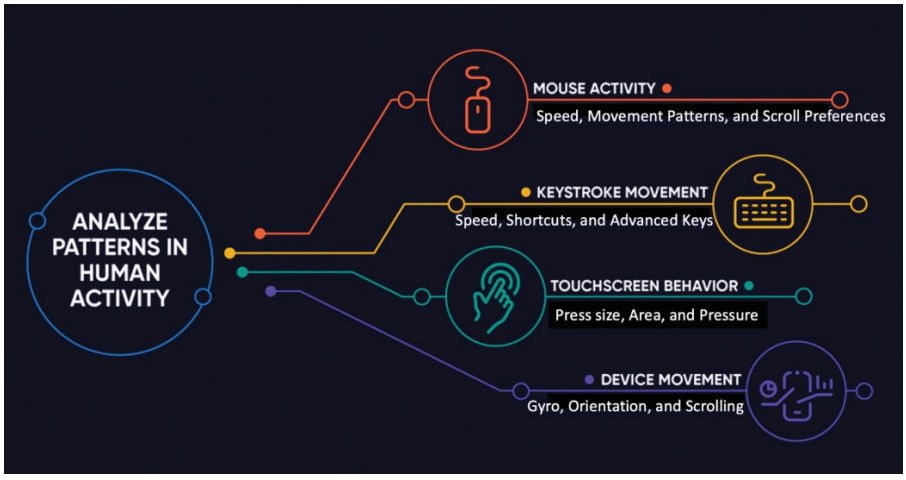


圖 5. 個人行為模式的獨特性種類[28]

在既有的網路安全框架中概述的回應計畫，可確保將停機時間減至最短。專門的 DDoS 緩解服務可作為對抗數位攻擊的堡壘，而法律框架則規定服務提供者必須對違規行為負責。ZTA 可透過身分驗證和存取限制，加強防禦來自洩密帳戶的 DDoS 攻擊。然而，必須意識到基於 AI 的 DDoS 減緩系統可能會在無意中干擾合法流量，導致服務中斷。與專業 DDoS 減緩服務相關的成本會造成財務上的障礙，特別是對於較小的組織而言。受通訊延遲和管轄複雜性的影響，事件回應期間的協調挑戰突顯了 DDoS 防禦的複雜性。

在對抗 APT 的過程中，AI 和 ML 可發揮警覺分析師的功能，分辨出潛在威脅的微妙異常現象。法律架構有助於威脅情報分享，促進對已知 APT 策略的集體防禦。ZTA 透過限制存取和持續的身分驗證，可阻止 APT 移動和資料外洩。資料外洩通報法律的存在可鼓勵迅速揭露，降低 APT 相關的損害。然而，以 AI 為基礎的 APT 偵測系統可能會產生誤報，因此必須進行資源密集的調查。APT 使用複雜的技術來掩飾其活動，突顯先進監控工具的限制。隱私權疑慮和信任的必要性可能會妨礙敏感威脅情報的協同分享。

將焦點轉移到社交工程上，安全意識訓練可讓個人識別和抵制操縱，並由網路安全框架提供支援，指導有效的方案實施。多重身分驗證增加了一層額外的安全層級，而法律框架則鼓勵採用多重身分驗證。營造開放溝通的環境可鼓勵及早偵測社會工程計畫。然而，安全意識訓練的成效可能因員工而異，尤其是技術知識有限的員工。攻擊者的不斷演變要求持續調整策略以對抗新技術。建立開放式的溝通文化可能是一項挑戰，尤其是在層級分明的組織中。

在監控使用者行為以揭露潛在未經授權的存取嘗試時，行為生物識別技術便開始發揮作用。強密碼和多因素驗證可在網路安全架構的指導下提供穩固的防禦。資料遺失防護可將敏感資料外洩的風險降到最低，而資料外洩通知法則可鼓勵迅速回應。儘管如此，收集員工生物特徵資料時可能會產生隱私疑慮，而使用者對多因素驗證的疲勞可能會影響持續採用。可能會影響持續採用。實施和維護有效的資料遺失防護 (DLP) 解決方案會帶來財務上的挑戰。

在保護智慧財產權時，資料加密可確保機密性，而法律架構會懲處未充分保護敏感資料的行為。數位版權管理可控制存取，防止未經授權的複製與散佈。網路安全架構中概述的事件回應計畫，有助於在懷疑智慧財產遭竊時迅速採取行動。然而，加密金鑰的安全管理對於確保加密的有效性至關重要。不同 DRM 系統之間的互操作性挑戰可能會妨礙內容發行。智慧財產竊取事件的回應速度需要廣泛的協調與法律考量。

在強化零時差監控方面，AI 與 ML 會持續掃描異常現象，在零時差攻擊廣泛散佈之前加以處理。誘捕系統 (honeypots) 和誘餌 (decoys) 等欺騙技術可揭露零時差攻擊，並透過法律架構提供保護。在結構化方法的協助下，威脅建模 (Threat Mod-eling)可主動採取緩解措施。然而，AI 可解釋性質的挑戰可能會導致錯誤的正確性或對威脅的疏忽。部署欺騙技術時的法律考量突顯了潛在的干擾，需要仔細規劃。威脅建模方法上的專業知識差距，對於有效規劃和緩解零時差威脅造成挑戰。

處理內部威脅包括透過行為生物識別技術監控使用者的異常行為，並在網路安全框架的指導下定期進行存取審查。匿名舉報機制可讓員工舉報可疑活動，而不必擔心報復。在監控員工活動的過程中，平衡安全需求與員工隱私權的考量至關重要。定期存取檢閱的效率可能會因程序的資源密集性而受到影響。儘管有法律保護，但害怕報復可能會妨礙內部威脅的及時報告。

在減少贖金軟體攻擊的情況下，資料備份可確保迅速還原，減輕此類攻擊的影響。及時的弱點管理可降低攻擊面，並透過法律框架鼓勵揭露弱點。安全意識訓練可讓員工了解贖金軟體風險和網路釣魚策略。然而，贖金軟體攻擊可能會以備份為目標，即使在主要系統還原後仍會造成資料遺失。及時修補弱點是一項挑戰，尤其是在複雜的 IT 環境中。頻繁的安全意識訓練課程可能會造成員工疲勞。

社會工程攻擊可透過社會　媒體　監控、　導向資料　隱私權來減緩

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

規定。提高網路釣魚意識的活動和多因素驗證可降低此類攻擊的成功率。法律架構鼓勵強大的驗證實務。但是，監控員工的社交媒體活動會引起隱私方面的疑慮，並且需要跨父母政策。開發有效的網路釣魚模擬可能是資源密集型的。多因素認證系統雖然有效，卻會帶來潛在的漏洞。根據資料保護法規規定，資料分類會優先處理和標示敏感資料。資料存取控制可限制存取，將未經授權外洩的風險降至最低。DLP 工具會在網路安全架構的指導下，偵測並防止未經授權的資料傳輸。然而，過於細緻的資料分類可能會增加作業成本，並會妨礙合法的資料存取。實施強大的存取控制系統需要身分管理與授權方面的專業知識。DLP 工具可能會產生因此必須小心處理。

透過技術和組織措施持續監控使用者，有助於防止未經授權的帳戶接管。先進的分析工具可偵測使用者登入的可疑模式。強大的驗證實務，包括多因素驗證和強大的密碼政策，可大幅降低帳戶被成功接管的風險。法律框架可以激勵組織採用並維護強大的驗證實務。然而，持續性使用者監控系統的實施與維護可能相當昂貴，尤其是對於擁有龐大使用者群的組織而言。大量的可疑活動警示可能會讓安全團隊應接不暇，導致警示疲勞和對真正威脅的潛在疏忽。說服使用者一致採用並使用強大的驗證方法是一項挑戰，尤其是對非技術使用者而言。在駕馭網路安全的複雜環境時，必須同時認清各種策略的優點與限制。人工智能、ML、ZTA、區塊鏈、法律架構和全面的網路安全實務的協同整合，有助於多層防禦在數位領域投下陰影的各種不斷演變的威脅。隨著技術的進步和威脅的演變，包含技術創新、道德考量、法規遵循和持續改善的整體方法對於保護完整性仍然至關重要、數位資產的保密性和可用性。

保障數位完整性的建議解決方案

我們已經介紹過各種專注於預防網路安全威脅的解決方案，並承認沒有放諸四海皆準的解決方案。現在，讓我們將焦點轉移到問題的另一個角度。我們該如何盡量減少機密資訊外洩？有哪些可以實施哪些措施來降低資料外洩的報酬，從而阻止潛在攻擊者發動此類行動？讓我們圍繞這些問題來探討解決方案。

防洩漏概念

積極主動的方法是有效防禦的關鍵，秉持這個理念，我提出了一個符合這個原則的概念。在深入探討細節之前，讓我們先熟悉一些基本名詞，這些名詞將有助於我們的探索。

首先，十六進位資料或十六進位資料是以十六進位數字系統表示資訊。這是編碼二進位資料的基本格式，通常用於程式設計和電腦科學。

以內容為基礎的指紋技術是一種檢視檔案的視訊或音訊內容，以製作獨特指紋的技術，也就是一種數位「切細」（hash），可在不需要重播的情況下捕捉媒體的精髓。演算法會擷取色彩、紋理、形狀或音訊頻率等特徵來組成指紋。[30]感知散列將焦點轉移到人類如何感知內容。[(30)]感知雜湊將焦點轉移到人類如何感知內容上，儘管有雜訊、壓縮假象或編輯，感知雜湊在唯一識別媒體方面仍然很強大。

蠕蟲是一種惡意軟體，能夠獨立複製並在網路和系統中傳播。蠕蟲會利用漏洞，對互連環境的安全性造成重大威脅。

同樣地，特洛伊木馬惡意軟體會將自己偽裝成合法軟體，欺騙使用者安裝。一旦被滲透，就會啟動未經授權的存取，並可能危及敏感資訊或助長其他惡意活動。

此外，邏輯炸彈是一段故意插入軟體系統的程式碼，當符合特定條件時會執行有害的動作。這些條件可由各種事件觸發，可能造成系統中斷或損害。

[32]此漏洞允許攻擊者透過製作的 .webp 檔案執行惡意程式碼，由於廣泛使用 libwebp 函式庫來處理此類影像，因此影響許多應用程式。立即更新軟體是解決此漏洞並確保受保護的關鍵。將焦點轉移到內建的防護措施，作業系統 (OS) 內建的病毒掃描程式和搜尋索引器是偵測和中和病毒與惡意軟體不可或缺的工具。這些公用程式會主動監控和識別潛在的威脅，對於整體的安全防護有顯著的貢獻。系統的安全性。

此外，內容傳送網路 (CDN) 可作為分散式伺服器系統，根據使用者的地理位置協同有效率地傳送網頁內容。除了增強網站效能之外，CDN 還能提供額外的安全層級，以對抗特定的網路威脅。

要掌握以主動防禦策略為中心的概念的細微差異，瞭解這些術語是非常重要的。現在，讓我們深入瞭解這些元素對建立強大網路安全方法的具體貢獻。

此程序包括將所需的媒體或文字檔案進行「釋放」。然後透過 hex dump 或 Vim 等軟體處理這些檔案，以取得文字檔案的 hex 資料和媒體檔案的獨特識別碼資訊，並利用內容型指紋和感知散列方法。隨後，蠕蟲程式碼就會被開發出來，其目的是透過網際網路傳播，並連結至 CDN 下載特洛伊木馬（圖 6）。

一旦蠕蟲在裝置上啟動，它就會擷取特洛伊木馬套件，而特洛伊木馬則反過來下載先前產生並散佈在各種公共或私人 CDN 上的元資料 (十六進位資料或唯一識別碼)。下一步，特洛伊木馬會與系統內建的病毒掃描程式或搜尋索引配對，啟動掃描以尋找與儲存的元資料相符的檔案。

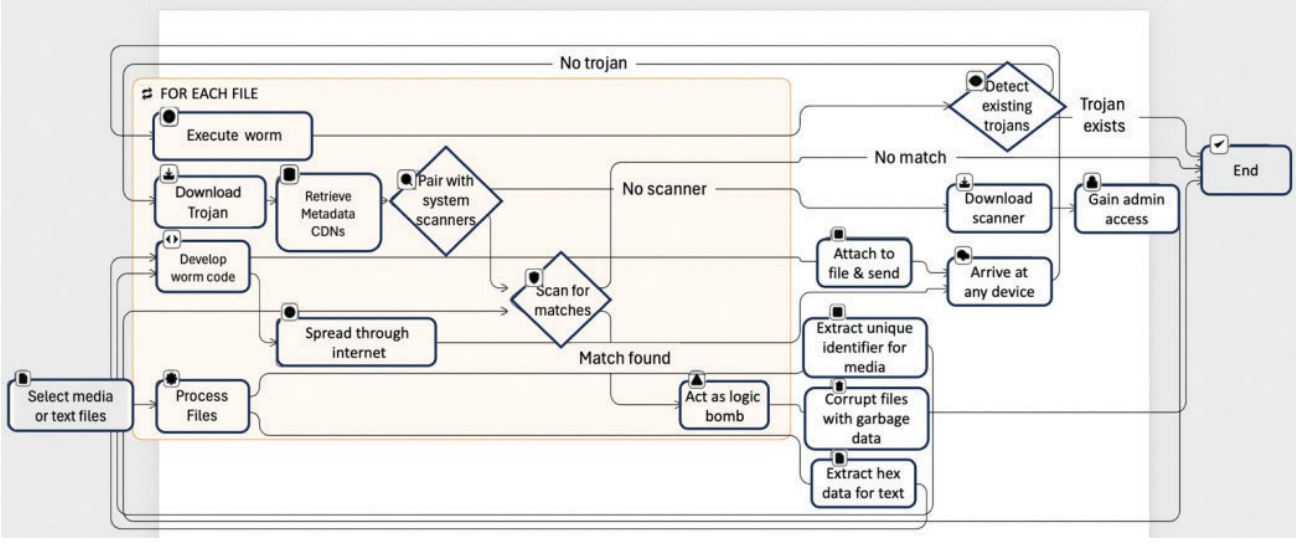
在系統缺乏 root/ admin 存取掃描器的情況下，蠕蟲可以從 CDN 中預先載入的掃描器下載自己的掃描器。利用特洛伊木馬策略，蠕蟲可能會以系統檔案的形式欺騙使用者授予管理權限。回到掃描過程，如果偵測到匹配的檔案，蠕蟲會扮演邏輯炸彈的角色，以垃圾資料取代原始資料，破壞檔案。此方法旨在移除洩漏的資訊，而不會造成任何額外的破壞動作。

在 CDN 存取無法使用的情況下，蠕蟲腳本可以附加到檔案中，然後傳送給不懷好意的使用者，讓人聯想到 Word 巨集或利用 .webp 等漏洞的技術。一旦執行，蠕蟲就會執行其任務。此外，蠕蟲程式會偵測任何現有的特洛伊木馬程式，以防止系統超載和潛在的使用者偵測。這種全面的方法可確保採用策略性且微妙的方法來處理洩漏的資訊。

Web3 資料隱私模型

從 Web 2.0 到 Web 3.0 的過渡標誌著從集中式系統到分散式系統的轉變。Web 3.0 的核心原則是分散化，從根本上改變了資料和應用程式的處理方式。這一轉變減少了對中央機構的依賴，讓個人對其個人資訊有更大的控制權，從而提高了隱私權。在 Web 3.0 中，區塊鏈、分散式識別碼、零知識證明等技術在建立更隱私、更安全、更以使用者為中心的數位環境中扮演關鍵角色。現在，我們將進入這個模型的複雜性，它利用了當前發展中的當代概念。在深入瞭解模型的操作細節之前，我們必須先熟悉相關的術語。

DIDs 是 Web 3.0 的基本要素，在為用戶提供一個分散的機制來創建和管理獨特的在線身份方面扮演著重要的角色。使用者可透過 DIDs 獨立自主地建立和控制自己的數位角色，從而提高隱私權。一個例子說明了這一點，DIDs能夠使個人在不依賴中央機構的情況下創建和管理在線身份，這與在數位領域中增強用戶隱私的首要主題是一致的[33]。



引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

圖 6. 工作機制的流程圖解釋。

數位憑證構成 Web 3.0 的關鍵部分，有助於發行和展示防篡改、可數位驗證的憑證。實際上，個人可以分享經數位簽章的憑證，例如文憑，而無需洩露不必要的個人資訊。這體現了創新科 技在加強隱私權和安全性方面的作用，提供了一個實例，說明創新科 技如何在數位環境中賦予使用者權力[34]。

零知識證明 (ZKP) 是 Web 3.0 模式中的重要加密技術，可讓各方在不透露實際資料的情況下證明資訊的真實性。ZKPs 可在不透露基本細節的情況下驗證資訊，對隱私權有重大貢獻。可以說明這個概念的一個例子是，ZKPs 可以讓某人在不透露秘密本身的情況下證明對秘密的瞭解，從而確保數位交易的隱私性。

聯盟學習 (FL) 透過促進分散式裝置之間的協同模型訓練，改變了 Web 3.0 的 ML 面貌。FL 的隱私意識方法的一個示例是，它能夠使移動設備在不交換原始數據的情況下協同訓練預測模型。這既保護了使用者隱私，又能利用聚合知識為整個系統帶來好處[36]。

SMPC 在 Web 3.0 中扮演著重要的角色，可讓多方進行安全的計算，而無需揭露個別輸入。SMPC 允許多方共同計算一個結果，而無需揭露其個別輸入，就是一個很好的例子。這項功能對於機密資料分析相當有價值，突顯其在保護隱私方面的重要性[37]。

個人資料儲存 (PDS) 可讓個人在私人儲存庫中安全地管理其個人資料。[37]個人資料儲存(PDS)可讓個人在私人儲存庫中安全地管理其個人資料，例如，PDS 可讓使用者控制對其儲存資料的存取，強化使用者對其數位身分的控制，並提高個人資料管理的隱私度[38]。

基於區塊鏈的資料儲存（Blockchain-based data storage，BBDS）是 Web 3.0 的革命性概念，可將資訊儲存分散到節點網路中。這種透明且防篡改的方法可確保資料的完整性，並將未經授權修改的風險降至最低。區塊鏈如何儲存資料，使其不易篡改，並確保資料儲存的透明性、安全性和私密性，就是一個說明這個概念的例子[39]。

可信賴的執行環境 (Trusted execution environments, TEEs) 透過在裝置上提供安全空間來處理敏感資訊，對 Web 3.0 做出了重大貢獻。TEE 的作用在於其能夠保護加密金鑰，並透過確保特定程序在設備上的可信和受保護空間中進行，從而保護使用者隱私[40]。

目前，這些術語可能還不完全清楚 (圖 7)。讓我們全面瞭解

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

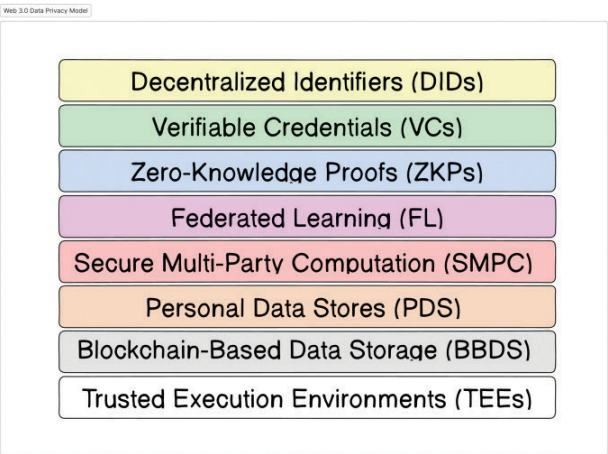


圖 7. Web3 資料隱私模型 (W3DPM)。

所有這些概念。

在這個由 Web 3.0 技術驅動的未來式投票情境中，個人將體驗一個以隱私為重點的變革式選舉過程。每位選民都配備了儲存於行動裝置上的 DID，賦予他們數位身分的所有權與控制權，不受中央機關的管控。選民透過他們的 DID 直接從政府資料庫發出安全的 VC，取代傳統的實體識別，在不洩露個人詳細資料的情況下證明資格，從而提高隱私。

為了進一步確保隱私權，選舉當局採用 ZKPs 來驗證選民資格，而無需存取個人記錄，並在不洩露特定詳細資料的情況下確認選民資格。協同預測模型是透過 FL 來實現，其中 ML 模型是在個人裝置上安全儲存的加密選民資料上進行訓練。這不僅提高了預測準確性，還在整個過程中維護了隱私。

在計算結果時，利用 SMPC 可保證選舉結果的完整性。選舉官員和獨立稽核人員共同分析投票資料，而不會直接共用敏感資訊，因此可保護個別選票的機密性。選民透過 PDS 保有對其投票歷史和偏好的控制權，選舉委員會只有在獲得選民明確同意的情況下，才能透過 DID 和 VC 存取這些資料，以盡量減少資料暴露，並賦予使用者安全管理其資訊的權力 (圖 8)。

透過 BBDS 實現透明且防篡改的儲存，將選舉結果和投票記錄安全地儲存在經過許可的區塊鏈上。這可確保選舉過程的完整性，同時限制授權實體存取。此外、

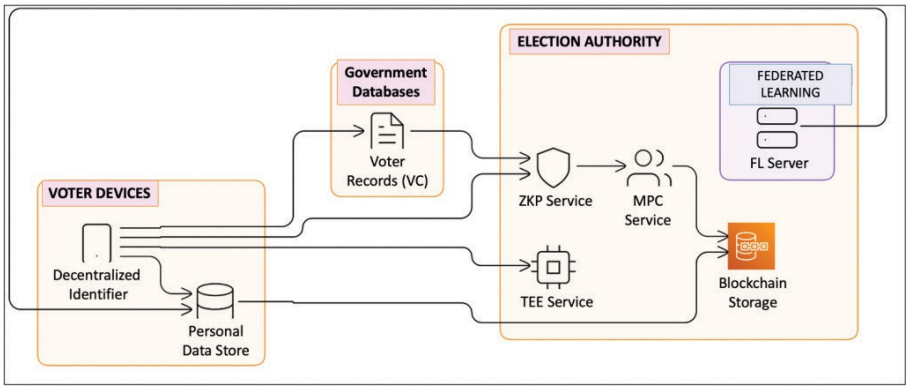


*圖 8.*投票情境範例。FL：聯盟學習；TEE：可信賴的執行環境；ZKP：零知識證明。

TEE 將敏感的計算 (例如詐欺偵測與結果驗證) 隔離在選民裝置的可信轄區內，提供額外的安全層級。

這個全面的範例展示了 Web 3.0 原則如何徹底改變現實世界的應用程式。它提供了一種安全、透明且以隱私為中心的投票體驗，在整個選舉過程中，個人都能保持對其身份和個人資料的控制。

比較與批判性分析

如前所述，我的網路安全解決方案與方法嚴重偏離該領域的主流作法。因此，與現有的方法直接比較會產生明顯的挑戰。將我們的注意力轉移到 deleakification 的概念上，這個概念具有爭議性和潛在的危險性，既有優點也有缺點。

精心設計的病毒是刪除概念不可或缺的一部分，它有可能有效率地掃描並移除目標資料，超越人工或傳統方法--在處理龐大的資料集時尤其有利。這種優勢在時間敏感的情況下尤其重要，因為在這種情況下，迅速減緩洩露資訊是最重要的。

另外一個好處是病毒有能力從受感染的系統中存取和移除資料，而這些資料透過傳統方式可能難以取得，例如離線裝置或隱藏的儲存位置。儘管在特定情況下具有優勢，但意外後果和潛在的隱私侵犯問題自然也會出現。

在此概念中，自我複製病毒的願景引進了資料移除程序自動化的前景，減少對人為介入的依賴，並可能將人為錯誤的風險降至最低。然而，這種自動化方式會引起與可控性和潛在意外擴散或損害有關的合理疑慮。

必須承認的是，這種病毒的實際執行會面臨相當大的挑戰。要在不影響合法線上內容的情況下，精確定位以移除洩漏資料，是一項複雜的任務。由於病毒傳播迅速且不受控制，因此很有可能會影響無關的資料，造成附帶損害。更複雜的是，洩漏的資料通常以分散的形式存在於多個網站和平台。病毒需要非常精密的設計，才能找到並移除所有洩漏資訊的實例。

在大多數情況下，這實際上是不可能的。此外，這種病毒的基礎技術：

雖然是為了 deleakification 內的道德目的而設計，但可能會被濫用於惡意目的。這為未來潛在的網路攻擊開創了令人擔憂的先例，突顯了重大的道德與安全問題。

Web 3.0 資料隱私解決方案為個人管理其身分的方式帶來了範式上的轉變，其中 DID 扮演了關鍵的角色。透過允許個人擁有和管理自己的身份，DIDs 減少了中央機關的影響力，從而將資料的脆弱性降至最低。然而，管理 DID 和 VC 的複雜性可能會妨礙其廣泛採用，尤其是在非技術使用者之間。為了確保不同平台之間的無縫協作，標準和互操作性的持續改進是至關重要的。

虛擬身份證提供了分享特定資料屬性的安全方式，可降低資料篡改和身份盜用的風險。然而，要在各行各業整合虛擬身份證，就需要廣泛採用一致的格式，以促進無縫的驗證和使用。合乎道德的實施對於防止虛擬身份證的潛在歧視性使用至關重要。

ZKPs 提供了創新的解決方案，可在不透露詳細資料的情況下證明擁有資訊，從而減少資料曝光。然而，實施和理

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

ZKPs 對開發人員和使用者而言都是挑戰，需要專業的技術知識。複雜 ZKPs 的計算成本可能會影響處理資源，因此在整合時需要謹慎考量。

FL 透過在本機裝置上訓練模型，將資料共用減至最低，從而提高隱私性。然而，分散式資料的聚集與管理可能會導致流程變慢。強大的安全協定對於確保跨不同裝置和網路的資料安全至關重要，而精心設計的獎勵措施對於鼓勵使用者參與至關重要。

SMPC 可在不透露個人貢獻的情況下進行聯合資料分析，從而促進安全協作。然而，複雜協定的計算費用以及擴充大型資料集的挑戰，都需要強大的硬體設備。有效的實作需要專業的技術知識與專長。

PDS 賦予個人擁有和管理其資料的權力，可降低集中式資料外洩的風險。然而，一致的資料格式和存取通訊協定對於無縫分享至關重要。強大的備份和復原機制對於避免資料遺失至關重要，而使用者教育則是廣泛採用的關鍵。

BBDS 可確保資料的不變性和透明度，但在擴充大量資料方面仍有挑戰，而且某些共識機制仍存在環境問題。隱私保護技術對於平衡透明度與使用者隱私的好處至關重要。

TEE 為敏感的運算提供安全的外圍環境，以加強資料的安全性。然而，需要考慮所有裝置的有限可用性以及潛在的執行開銷。持續的研究對於解決潛在的弱點和確保穩健的安全性至關重要。

總體而言，deleakification 與 Web 3.0 資料隱私解決方案的概念提供了極大的潛力，可讓個人對其資料擁有更大的控制權，並確保數位世界中的隱私權。然而，每種技術都有其自身的優點和缺點，要成功實施這些技術，需要仔細考慮這些因素，並與不同的利害關係人合作，以解決現有的挑戰，並確保道德和負責任的發展。

結論與未來範圍

目前的 unleakification 和 Web3 資料隱私權模型面臨限制，這些技術仍處於早期階段。然而，這個萌芽階段提供了重要的改進機會，使其更可行、更易於使用、更廣泛地被採用，最終增強其穩定性。技術複雜性、使用者採用和可擴充性等挑戰需要解決，但分散化和使用者擁有資料所帶來的機會，為更安全且以使用者為中心的未來帶來希望。

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

在人工智慧與網路安全領域中，人工智慧整合所造成的攻擊面增加令人擔憂。ISO 42001 與歐洲 AI 法規等框架與法規，是朝向負責任的開發與穩健安全性的正確方向邁進。雖然量子密碼技術等新興解決方案大有可為，但對於潛在威脅的警覺性，尤其是來自人工智慧 (AGI) 的威脅，仍是至關重要的。除了技術上的考量，解決人工智慧與資料隱私的社會與道德影響也至關重要。公開討論資料所有權、算法偏見以及人工智慧驅動的操控，對於負責任的發展是必要的。強調人類與人工智能之間的合作，將人工智能視為增強能力的工具而非替代品，可以促進符合倫理且有益的發展。隨著人工智能革命的進展，它同時帶來了進步和挑戰。AI 在各個領域的廣泛應用擴大了攻擊面，對必須提升其遊戲水準的網路安全專業人員構成挑戰。儘管已有框架，但仍有許多需要保護的地方。AI 的電腦運算能力可能會讓目前的安全技術過時。[41]持續的研究、合作，以及對挑戰與倫理影響的謹慎考量，將有助於利用這些技術的潛力，創造一個安全、公平、豐富的未來。

經費來源

本篇文章的撰寫未獲得任何資助。

財務及非財務關係與活動

作者無任何報告。

貢獻者

本研究論文的所有作者都直接參與了本研究的規劃、執行或分析。本文所有作者均已閱讀並通過所提交的最終版本。

資料可用性聲明 (Das)、資料分享、可重複性及資料庫

文章開發過程中未使用原始資料。

應用人工智能產生的文字或相關技術

本文撰寫過程中未使用 AI 及相關技術。

鳴謝

無。

參考文獻

1. 英格瑪布萊奇利公園。[於 2024 年 1 月 13 日引用]。網址: https://bletchleypark.org.uk/our-story/enigma/
2. 電腦病毒與蠕蟲年表。維基百科；2024 [2024 年 1 月 13 日引用]。Available from: https://en.wikipedia.org/w/index.php?title=Timeline_of_computer_viruses_and_worms&oldid=1194773804
3. cybercrimemag.預測 2017-2021 年全球網路安全支出將超過 1 兆美元。網路犯罪雜誌。2024 [2024 年 1 月 13 日引用]。網址：https://cybersecurityven-tures.com/cybersecurity-market-report/
4. 2023 年最嚴重的網路安全威脅。思科。[2024 年 1 月 13 日引用]。Available from: https://www.cisco.com/c/en/us/products/secu-rity/top-cybersecurity-threats-2023.html
5. M.C. D. O. C. (CDOC) Intelligence Microsoft Threat. 深入探討 Solorigate 第二階段啟動：從 SUNBURST 到 TEARDROP 和 raindrop。微軟安全部落格。[2024 年 1 月 15 日引用]。網址：https://www.microsoft.com/en-us/ security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
6. 什麼是 Mirai Botnet？Cloudflare.[cited 2024 Jan 12].可從以下網址取得：https://www.cloudflare.com/learning/ddos/glossary/ mirai-botnet/
7. OPM黑客事件解析：糟糕的安全措施遇上中國的美國上尉。CSO Online.[cited 2024 Jan 12]. 網址：https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america. html
8. 什麼是 WannaCry 勒索軟體攻擊？| UpGuard。[cited 2024 Jan 12].Available from: https://www.upguard.com/blog/ wannacry
9. 殖民地管道贖金軟體攻擊。維基百科；2023 [2024 年 1 月 12 日引用]。Available from: https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&oldid=1189897140
10. Times F. 打個電話到客服中心很可能就能入侵 MGM。Ars Technica.[cited 2024 Jan 12]. 網址：https://arstechnica.com/security/2023/09/a-phone-call-to-help-desk-was-likely-all-it-took-to-hack-mgm/
11. Helmus TC.Artificial intelligence, deepfakes, and disinfor-mation: a primer.RAND Corporation; 2022 [於 2024 年 1 月 12 日引用].Available from: https://www.rand.org/pubs/perspectives/ PEA1043-1.html
12. Rashmika Mandanna deepfake 案件：德里 警方 追捕 4 名嫌犯，追捕主要同謀。 印度斯坦時報》。 [cited 2024 Jan 12].Available from: https://www. hindustantimes. com/india-news/rashmika-mandanna-deepfake-case-delhi-police-track-down-4-suspects-hunt-for-key-conspirator-on-101703043714888.html
13. 2019 Capital One 網路事件 | 發生了什麼事。Capital One.[cited 2024 Jan 12].網址: https://www.capitalone.com/ digital/facts2019/
14. 萬豪資料外洩常見問題：到底發生了什麼事？Hotel Tech Report。[cited 2024 Jan 12].網址: https://hoteltechre-port.com/news/marriott-data-breach
15. Page C. Tesla 表示影響 75,000 名員工的資料外洩事件是內鬼所為。TechCrunch.[於 2024 年 1 月 12 日引用]。網址：https://techcrunch.com/2023/08/21/tesla-breach-employee-insider/

引用：區塊鏈在醫療保健的今天2024，7：302 - https://doi.org/10.30953/bhty.v7.302

16. Hern A, A. H. U. 技術編輯。 Pentagon leak traced to video game chat group users arguing over war in Ukraine.《衛報》；2023 年 4 月 11 日 [引用日期：2024 年 1 月 12 日]。*衛報*》；2023 年 4 月 11 日 [2024 年 1 月 12 日引用]。網址：https://www.theguardian.com/world/2023/apr/11/pentagon-leak-traced-to-video-game-chat-group-users-arguing-over-war-in-ukraine
17. Stuxnet.*維基百科*；2024 年 1 月 10 日 [2024 年 1 月 12 日引用]。網址：https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=119468 7512
18. 網路安全中的 AI：捍衛您的數位領域。[於 2024 年 1 月 13 日引用]。Available from: https://www.veritis.com/blog/ai-in-cy-bersecurity-defending-against-evolving-threats/
19. 網路安全中的機器學習 (ML)：使用案例 -Crowd-Strike.crowdstrike.com ；[cited2024Jan15].Availablefrom:https://www.crowdstrike.com/cybersecurity-101/machine-learning- cybersecurity/
20. Chandramouli R, Butcher Z. A zero trust architecture model for access control in cloud-native applications in multi-cloud environments.National Institute of Standards and Technology, NIST Special Publication (SP) 800-207A; 2023.
21. Zhou L. 什麼是零信任架構 (ZTA)？ |NextLabs Data-CentricSecurity.NextLabs.[cited2024Jan13].Availablefrom: https://www.nextlabs.com/what-is-zero-trust-architecture-zta/.
22. NIST: 区块链为智能制造提供安全性和可追溯性。 *NIST*; 2019 [于 2024 年 1 月 13 日引用]。可从以下网址获取：https://www.nist.gov/news-events/news/2019/02/nist-block-chain-provides-security-traceability-smart-manufacturing。
23. Gartner.Gartner.[於 2024 年 1 月 13 日引用]。Available from: https://www.gartner.com/en/documents/4004851
24. 什麼是欺騙技術？重要性與效益| Zscaler。[cited 2024 Jan 13].Available from: https://www.zscaler.com/ resources/security-terms-glossary/what-is-deception-technology
25. Han X, Kheir N, Balzarotti D. 網路電腦安全中的欺騙技術：研究觀點。ACM Comput.Surv.2018;51(4):80:1–36. https://doi.org/10.1145/3214305
26. 首頁| CISA。[cited 2024 Jan 13].網址: https:// www.cisa.gov/
27. 歐洲理事會：7億公民的人權、民主和法治的守護者 -Portal-www.coe.int 。Portal.[cited 2024 Jan 13].Available from: https://www.coe.int/en/web/portal
28. 什麼是行為生物統計？[cited 2024 Jan 13]. 網址：https://www.biocatch.com/blog/what-is-behavioral-biometrics
29. Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the Internet-of-things era: an artificial intelligence perspective.IEEE Internet Things J. 2020;7(9):9128-43. https://doi.org/10.1109/JIOT.2020.3004077
30. Du L, Shang Q, Wang Z, Wang X. Robust image hashing based on multi-view dimension reduction.J Inf Secur Appl. 2023;77:103578. https://doi.org/10.1016/j.jisa.2023.103578
31. Qin C, Liu E, Feng G, Zhang X. Perceptual image hashing for content authentication based on convolutional neural network with multiple constraints.IEEE Trans Circuits Syst Video Technol.2021;31(11):4523–37. https://doi.org/10.1109/ TCSVT.2020.3047142
32. 揭露隱藏的 WebP 漏洞：一個 CVE 的故事，其影響遠遠大於我們原先的想像。Cloudflare 部落格。[cited 2024 Jan 14].Available from: https://blog.cloudflare. com/uncovering-the-hidden-webp-vulnerability-cve-2023-4863
33. 分散式識別碼 (DID) v1.0。[cited 2024 Jan 14]. 網址：https://www.w3.org/TR/did-core/

34. Barker E. Recommendation for key management: part 1-general.Gaithersburg, MD: National Institute of Standards and Technology; 2020.
35. Fenzi G. Zero knowledge proofs theory and applications.聖安德魯大學。2019 年 9 月。[cited n.d.].Available from: https://info.cs.st-andrews.ac.uk/student-handbook/files/ project-library/cs4796/gf45-Final_Report.pdf
36. Mahlool DH, Abed MH.聯合學習的全面調查：概念與應用。ArXiv.2022. https://doi. org/10.48550/arXiv.2201.09384
37. Merino L-H, Cabrero-Holgueras J. Secure multi-party compu-tation.在：V Mulder, A Mermoud, V Lenders, B Tellenbach, 編輯.資料保護與加密技術的趨勢。Cham：Springer Nature Switzerland, 2023; p. 89-92.
38. Arewa O. Data Collection, Privacy, and Children in the Digital Economy.George Mason Legal Studies Research Paper No. LS 23-22, Chapter in FAMILIES AND NEW MEDIA (Springer Link 2023).2023.[cited n.d.].可從以下網址取得：https://ssrn.com/abstract=4617953 或 https://doi.org/10.2139/ssrn.4617953
39. 世界經濟論壇。[cited 2024 Jan 14].Available from: https://www.weforum.org/publications/realizing-the-potent ial-of-blockchain/
40. Lee D, Kohlbrenner D, Shinde S, Asanovi K, Song D. Key-stone: an open framework for architecting trusted execution environments.In Proceedings of the fifteenth European con-ference on computer systems, in EuroSys '20.New York, NY： New York, NY: Association for Computing Machinery, 2020; p. 1-16.
41. Kaur R, GabrijelčiD, Klobučar T. Artificial intelligence for cyber-security: literature review and future research directions.Inf Fusion.2023;97:101804. https://doi.org/10.1016/j.inffus.2023.101804