

# 香港紅卍字會大埔卍慈中學

高中應用學習課程資訊科技精要  
2023-2025ECC學年

單元六數據通信和網絡  
課業六網絡安全認知 (生成式人工智能)

組員  
馬亦恒(組長)  
陳展軒  
劉妍  
楊樂

# 目錄



## 1.技術介紹與應用

1.1.技術基本概念與應用範圍

1.2.技術介紹

1.3.技術優勢

1.4.技術應用

## 2.網絡安全威脅分析

2.1.網絡安全威脅

2.2.威脅分析

2.3.安全問題來源

2.4. 案例研究

## 3.保護措施與模型連繫

3.1. 保護措施

3.2. OSI 模型連繫

3.3. TCP/IP 模型連繫

3.4. 網絡架構模型連繫



# 目錄

## 4. 跨領域整合與合作

- 4.1 跨領域整合
- 4.2. 合作機制

## 5. 法律规范和教育

- 5.1 法律和規範
- 5.2 用戶教育
- 5.3 未來展望

---

# 技術介紹與應用



# 生成式人工智能技術基本概念與應用範圍

## 生成式人工智能

結合計算機科學和統計科學最前沿的模型和技術屬於深度學習的一個分支，工作原理是一類機器學習模型，通過學習數據中的規律或模式來生成新的內容**通過用戶輸入來創造新內容**文本、圖像、聲音、動畫和3D 模型等其它類型，應用於**所有業務範圍**，包括工程、行銷、客戶服務、金融和銷售。



# 技術介紹

**機器學習** — 用資料或以往的經驗，以此最佳化電腦程式算法和模型可以讓電腦系統根據模式和推理來執行任務

**神經網絡** — 可讓電腦用來從錯誤中學習並持續改善的適應型系統

**深度學習** — 可指導電腦以受人腦啟發的方式來處理資料

**大語言模型** — 基於大量資料進行預訓練的超大型深度學習模型



## 技術優勢

傳統的人工智慧是為解決特定任務、分析數據並做出預測而設計的

而生成式ai將創建與其訓練資料類似的新資料

傳統人工智慧可以分析數據並告訴你它看到了什麼，現代人工智慧可以使用相同的數據來創建一些全新的東西

因此它可以快速生成大量內容，快速提供全面且綜合的數據并具自定義和個性化



## 技術應用

最常見的應用有ChatGPT它包括文字生成、對話、分析和偵錯等可用在市場營銷如處理用戶查詢

商戶可考慮採用ChatGPT 技術串連至聊天機械人(Chatbot)代替客服人員，接入公司API讀取數據，為客戶提供及時的幫忙。常見於網店結合WhatsApp 及ChatGPT，提供24小時對話服務。協助解答一般問題，例如退貨流程、保養期等，查找個別客戶的交易記錄及訂單進度；甚至協助處理投訴



---

# 網絡安全威脅分析



# 網絡安全威脅

生成式人工智能的網絡安全威脅主要分為兩類

## 模仿

網絡釣魚  
深度偽造

## 入侵

入侵攻擊  
人工智能模糊測試



# 威脅分析


訊息的可信度降低

知識產權遭竊取

外部攻擊者蓄意的攻擊

而那這威脅對於平民百姓們可能導致嚴重的金錢損失，利用gen AI生成一張面孔或一段短信來騙用戶的金錢。

而這些威脅發生的可能性是相當大，特別都用戶在互聯網上輸入個人資料令攻擊者有機會哄騙用戶。



運用生成式AI的深層偽裝技術實時換臉及換聲，來騙取財物。  
影響了互聯網的信任度並且損害了他人的財富。  
這些相應的事件在社會中發生的可能性是極大的，因為其的便捷度與方便性驗證。



## 安全問題來源

這些安全問題主要是因用戶對那些哄騙的短信沒有防備心，令攻擊者有機可乘

這不會影響系統，但透過使用生成式人工智來偽做用戶認識的人來能欺騙用戶的錢會違反香港法律，而主要被針對的對象通常是那些會很容易被騙的人。

最近有很多關於詐騙集團用AI詐騙新手法，令受害者損失大量資金。



## 安全問題來源

目前此問題的解決方案是在接到未知來源電話或消息時掛斷電話及忽略這些消息，警方可以設置一些特定的行動裝置來接收這些消息或電話，並追蹤這些消息和電話的來源。

開發人員設置程式跟蹤人們向 AI 提出的問題，有人要求 AI 複製某人聲音程式將跟蹤使用者的歷史記錄，使用者向 AI 詢問了哪些內容，如可疑程式會向警方報告使用者。



# 案例研究

AI生成的深度偽造技術使得攻擊者能夠製作高度逼真的虛假視頻和音頻用於製造假新聞、企業詐騙或政治宣傳，損害個人和機構的聲譽。

2024年1月，一段虛假視頻開始流傳，其中香港特首李家超在銷售投資產品。罪犯透過使用深度偽造技術生成了李家超的假聲音，使這段視頻看起來更加真實。

罪犯製作一段虛假視頻，使用深度偽造技術生成了李家超的假聲音，以吸引更多多人買他銷售的投資產品。

李家超本人出來澄清該視頻不是他本人。



# 案例研究

## 從中學習：

即使在網上看到的樣子與聲音都一樣，也不能完全相信。

## 未來預防：

建議香港政府立法監管使用電腦的方式。



---

# 保護措施與模型連繫



## 保護措施

當收到此電話和消息時，用戶可以通過收聽電話或消息的回復來識別它是否是假的，**如回復太簡單，像“是”或“否”。**

檢查在電郵裏收到的訊息和**小心任何要求你快速作出行動的電郵、電話以及影片**，這通常都是騙案的跡象。

雖然這些措施的有效性相對低但實施成本一定最便宜



## OSI 模型連繫

成式人工智慧的安全問題在OSI模型中，主要體現在最上層的「應用層」。因為人們可輕易利用人工智慧進行**詐騙或攻擊或盜取**。

由於這些活動都涉及到資料的完整性和存儲，因此在這一層上可能會遇到各種安全風險。

主要的安全考慮包括：

**存儲安全:**有些公司用gen ai來幫助他們管理/存儲公司的數據，由於gen ai在幫助他們管理/存儲公司的數據中無意地上傳了公司的數據令公司的數據外洩。

**完整性問題:**騙徒會利用人工智慧生成一些短信或電話進行詐騙或攻擊或盜取。



# TCP/IP 模型連繫

生成式人工智能的安全問題主要集中在TCP/IP模型的應用層上。這是因為所有的生成式人工智能管理操作都是在應用層中完成的。在這一層級，數據的**傳輸**和**處理**都需要特別的防護措施來確保安全。

主要的安全考慮包括

用戶安全行為：僅僅依賴技術手段可能並不能完全解決生成式人工智能安全問題。用戶的安全意識和行為也對生成式人工智能的安全有著重要影響。例如，用戶需要定期更新和升級他們的生成式人工智能軟件，以防止舊版本中存在的漏洞被攻擊者利用。同時，用戶也需要對他們的私鑰和訊息數據進行定期備份，以防止數據的丟失或損壞。

安全應用程序：使用安全的應用程序，如加密的生成式人工智能，可以保護用戶的資料和訊息免受盜竊。加密的訊息通常會使用強大的密碼學技術對用戶的私鑰進行保護，使得即使客戶的數據被攻擊者獲取，攻擊者也無法直接使用這些私鑰進行交易。



# 網絡架構模型連繫

在零信任架構中,安全問題可以從以下幾個角度進行考慮:

## **資料加密和完整性：**

在網絡層,使用IPsec等協定保護IP數據的機密性和完整性。

在傳輸層,採用TLS/SSL等加密通道確保端對端通信安全。

在應用層,對敏感數據進行加密存儲。

## **身份驗證和授權：**

在物理層和網絡層,使用較強身份驗證方式(如Multi Factor Authentication)來確認用戶和設備身份。

在傳輸層和應用層,基於最小權限原則實施動態和細粒度的訪問控制。

## **安全自動化和協調響應：**

利用 SOAR 技術自動化安全運營和事件響應流程。

跨層級整合安全控制,實現協調一致的安全策略執行。



# 網絡架構模型連繫

它主要會影響網絡架構的三個部分

## **物理層和網絡層：**

物理設備的安全性,包括防止物理訪問、防止設備被篡改或破壞。

網絡基礎設施的安全性,如防護路由器、交換機等關鍵設備受攻擊。

網絡協定的安全性,如 IP 數據被攔截或篡改的攻擊。

## **傳輸層：**

端對端通信的安全性

關鍵應用程序(如 VPN、SSL)能夠提供安全的數據傳輸。

## **應用層：**

常見的漏洞攻擊,如 SQL 注入、XSS 等。

身份驗證和授權機制的安全性。

敏感數據的安全性,如加密儲存和傳輸。

針對網絡架構各層面的安全問題,有很多專門的防禦措施和技術可以採用

---

# 跨領域整合與合作



# 跨領域整合

生成式人工智慧作為新興技術，可以與**5G通訊**，**機器翻譯**，**通用圖形處理器**，**機器視覺**，**無螢幕顯示**和**立體打印**整合。例如，**機器翻譯** 人手自然語言翻譯語言變得形式化

整合後的技術可以應用於更多的場景，如**無人駕駛**，**翻譯各類語言及電腦語言**，**3D打印**，**影像投影** 等等，整合過程中可能面臨的挑戰包括數據兼容性這些挑戰需要輸入更多數據讓人工智慧學習演算法

一個具體的整合**案例**是**生成式人工智慧與無人駕駛**，**機器視覺**可以幫助無人駕駛系統計算，減少人手輸入環節，提高計算效率





## 合作機制

技術發展過程中常見的合作機制包括聯合開發、技術轉讓、戰略聯盟等。這些合作機制能夠促進資源共享、技術交流，提升生成式人工智能研發技術

合作可以促進技術資源的整合，降低研發成本和風險，並加速技術的商業化應用

生成式人工智能合作過程中可能面臨的主要問題包括知識產權的歸屬、數據共享的安全性等。需要通過簽訂明確的合作協議來保障企業和機構之間的權益，並採取有效的安全措施來保護數據安全。

建立和維護合作伙伴關係的最佳實踐包括：制定明確的合作協議，明確各方的權利和義務；建立風險管理機制，預防和應對潛在的合作風險；制定合理的利益分配方案，確保各方的利益均衡。通過這些措施，可以建立穩定、持久的合作伙伴關係，促進生成式人工智能的共同發展。

---

# 法律規範和教育



## 法律和規範

對於解生成式人工智能，許多國家已經制定了相關的法律和規範。例如，歐盟的GDPR，為AI系統的數據使用設定了明確的標準，還有一些國家和組織正在研究制定AI安全標準和最佳實踐指南如IEEE的"Ethically Aligned Design"倡議

法律和規範的存在可以提高生成式人工智能的透明度和信任度，有助於吸引更多的投資者和用戶。然而，過於嚴格的規範也可能限制技術的創新和發展。

目前的法律和規範多集中於打擊非法活動和保護用戶權益，但對於技術創新和市場發展的支持仍顯不足，未來需要在平衡安全和創新的基礎上進一步完善相關法規。



# 用戶教育

普通用戶需要了解生成式人工智能的**基本概念以及常見的安全風險**，例如**詐騙、詐欺、冒充、勒索軟體、貨幣盜竊、資料收集等犯罪行為的風險**。

可以通過**實體課程、在線課程、社交媒體宣傳、線下講座**等多種方式進行教育。生成式人工智慧應用程式或平台的提供風險提示。

在線課程可以覆蓋到**普通民眾和學生**或在社交媒體宣傳、線下講座等多種方式教育普通民眾



## 未來展望

未來可能面臨更加**複雜**人工智慧輔助的詐騙、詐欺、冒充、勒索軟體、貨幣盜竊、資料收集等**犯罪行為**

生成式人工智能可能會在更多的行業中得到應用，例如**教育和培訓**等

隨著技術的進步，生成式人工智能和網絡安全的交互模式將更加緊密，安全技術將成為生成式人工智能應用的基石，而生成式人工智能的發展也將推動新的安全技術的出現



# Q&A TIME

**感謝聆聽**

---