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）

單元四：數據分析與數據庫

課業四：數據分析書面報告

第一組組員 ：

5D張文桔(組長）

5D黃港寧

5D王偉昌

5A侯柏亨

次序

1.技術介紹與應用-物聯網(IOT)

2.網絡安全威脅分析

3.保護措施與模型連繫

4.跨領域整合與合作

1.技術介紹與應用-物聯網(IOT)

物聯網介紹

特點-

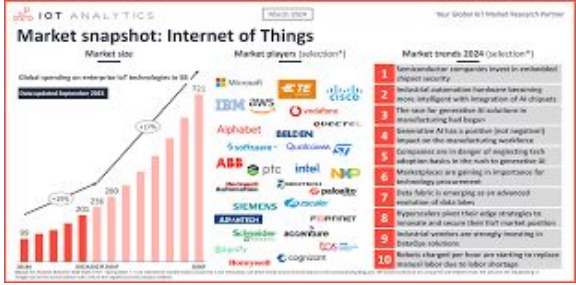
物聯網是一種計算裝置、機械、數位機器相互關聯的系統，具備通用唯一辨識碼，並具有通過網路傳輸數據的能力，無需人與人、或是人與裝置的互動。

物聯網將現實世界數位化，應用範圍十分廣泛。物聯網可拉近分散的資料，統整物與物的數位資訊。物聯網的應用領域主要包括以下方面：運輸和物流、工業製造、健康醫療、智慧型環境（家庭、辦公、工廠）、個人和社會領域等[5]。

物聯網為受各界矚目的新興領域，但安全性是物聯網應用受到各界質疑的主要因素[6]，主要的質疑在於物聯網技術正在快速發展中，但其中涉及的安全性挑戰，與可能需要的法規變更等，目前均相當欠缺。

特性及運作原理-

物聯網的技術路線其依據時間軸可分為四個階段供應鏈輔助、垂直市場應用、無所不在的定址，最後可以達到「The Physical Web」即是物聯網上的每一個智慧型裝置都以URL來標示。



歷史發展和未來趨勢

最早的概念

物聯網的概念可以追溯到1980年代初期，全球第一台隱含物聯網概念的裝置為位於卡內基·梅隆大學的可樂販賣機，它連接到網際網路，可以在網路上檢查庫存，以確認還可供應的飲料數量。馬克·維瑟（Mark Weiser）於1991年發表了「21世紀的電腦」（The Computer of the 21st Century）論文，當中揭櫫普及計算的概念，為物聯網的發展拓展了重要的道路。

面世

最早提出「物聯網（Internet of things）」這個名稱的人可能已經很難斷定，但任職於寶鹼公司的前瞻技術開發者凱文·阿什頓（Kevin Ashton）說，他自己應該是最早明確使用「物聯網」名稱的人，1999年他在寶鹼公司所做一次演講的標題即為「Internet of things」。他並表示，相較於「Internet of things」，他自己更喜歡「Internet for things」這個名稱。當時，他認為射頻識別對於物聯網至關重要，這將使電腦可以管理所有個別物體。

迅速發展

部分人士認為金屬氧化物半導體場效電晶體（MOSFET）技術的進步是促成物聯網快速發展的推手。主要的論點在於MOSFET到了21世紀製程已可微縮至奈米等級，大幅降低了功耗，而低功耗設計正是物聯網中的感測器可否被廣泛運用的關鍵因素。除了MOSFET之外，絕緣層上覆矽（silicon-on-insulator）與多核心處理器技術的發展，也是促成物聯網普及的原因。

技術優勢

拿農業為例

- 敏捷: 即時監測和預報系統讓農民能 夠快速應對天氣變化，作物狀況，和潛在的威脅，最大限度地減少損失並保護產量。
- 提高產品質量: 農業中的物聯網在很大程度上有助於提高生 產水平. 通過使用連接的系統，農民現在可以最大限度地提高營養價 值並重新創造更好的 產品條件。
- 永續實踐: 物聯網支援的智慧農業最大限度地減少農藥和化肥的使用 ，與傳統方法相比，產品更清潔，環境足跡更小。

創新

天氣和環境監測

配備智慧感測器和連接功能的氣象站可以對農作物進行最新的微氣候監測 . 數據流入平台分析霜凍等潛在風險 , 乾旱, 降雨和害蟲壓力觸發即時警報進行幹預。

智能溫室

利用物聯網技術控制溫室 內部的溫度、濕度、光照等參數 ,自動調節以確保作物生長最佳環境 ,降低人工管理成本。一些溫室還會結合電子標籤、RFID等技術實現智能化管理和追溯。

智慧灌溉和水管理

使用物聯網水監測和智慧灌 溉系統, 農民可以在優化使用的同時保持理想的濕度水平 . 整合天氣資料和土壤感測器驅動按區域定制的自動滴灌計劃 , 作物和生長週期 .

創新-技術升級

現有的技術下過於依賴人工，可改用 物聯網技術 完成,提高準確性

效率方面：農業物聯網使農民能夠實時監控他們輕鬆生產的作物. 他們獲得洞察力，幫助他們在問題發生之前更快地預測問題 . 熟悉農作物後，產品更有可能更快、更容易進入市場。

成本方面：運營成本低；資源消耗，運營成本，透過自動化農作物種植過程可以顯著減少人為錯誤，受傷，和增加收穫。

資源節約：基於物聯網的精準農業，水等資源，活化，可以根據現場感測器的數據準確分配適量的土地來優化土地。

便利性：手機上便可操作、監視及控制整個農場。

技術應用

具體應用場景或案例

物聯網(Internet of Things, IoT)的技術應用非常廣泛,可以應用在以下幾個場景

智慧家居:

可以讓普通的家庭電器,**具備遠程控制功能 ,**實現家電、照明、安防自動化控制,提高生活便利性和居家安全性。
1.家電自動化:可遠程控制燈光、空調、門窗等家庭設備。
2.安全監控:配備攝像頭、門磁等設備,提供安全預警和遠程監控功能。
3.健康管理:結合可穿戴設備,實現對家庭成員健康狀況的監測。

智慧城市:

物聯網技術可應用於城市管理的各個領域,如交通、能源、環境監測、公共服務等,實現城市的智慧化管理。
1.智能交通管理:利用物聯網技術監測道路交通狀況,實時調整信號燈、引導駕駛者繞行等。
2.智能環境監測:部署環境傳感器,實時監測空氣質量、噪音水平,提供環境數據分析。
3.智慧停車系統:通過車牌識別、車位傳感器,提供停車位預訂、引導等服務。

交通運輸:

車聯網技術可實現車輛的實時定位、行駛狀態監控、交通信息共享等 ,提升交通效率和安全性。

1.利用路側傳感器和攝像頭,實時監控交通流量、車輛速度等指標

2.依據數據動態調整信號燈時序,疏散擁堵路段的車流

3.預測交通流量,提前優化路網規劃,引導車輛最優路徑行駛

環境監測:

部署物聯網感測設備可以實現對環境狀況 (如空氣質量、水質、噪音等)的實時監測和預警。

1.利用空氣質量監測站和移動監測設備,實時收集PM2.5、二氧化硫等指標數據

總結

物聯網技術的應用為各行各業帶來了智能化、自動化、高效率的變革 ,成為推動社會進步的重要技術手段之一。未來隨著技術的進一步發展 ,物聯網必將在更多領域發揮重要作用。

2.網絡安全威脅分析

威脅的性質和來源：

物聯網的威脅主要來源於外部攻擊。物聯網的主要威脅來源黑客入侵。開發是疏忽安全問題誤導致黑客有機可趁。

威脅的嚴重程度：

數據丟失、被黑客監視、家中被輕易入侵、資金被黑客轉移。

威脅的可能性：

缺乏有效的安全機制和監管，設備普及速度快，使得此類威脅發生的可能性很高。針對每種威脅的對策：身份驗證、設防火牆、加強物聯網安全標準和法規的制定與執行。

網絡威脅的類型:

1.惡意軟件攻擊:包括病毒、木馬、蠕蟲等各種旨在破壞系統、竊取數據的惡意程式。

2.網絡釣魚:通過偽造網站或電子郵件欺騙用戶洩露敏感信息的攻擊手段。

3.DDoS:大量的互聯網流量使目標伺服器或其周圍的基礎設施不堪重負。

4.網絡入侵:利用系統漏洞非法獲取目標系統控制權的行為。

5.內部人員威脅:由內部人員如員工、合作伙伴等出於各種動機引起的安全事故。

網絡威脅分析方法

1.資產梳理與風險評估:識別關鍵信息資產,評估其面臨的安全風險。

2.威脅情報收集與分析:收集各類網絡安全態勢信息,識別新興威脅。

3.異常行為檢測與響應:監控系統日誌,發現並應對可疑活動。

4.安全事故調查與溯源:分析事故原因,追蹤攻擊者身份與手法。

5.安全防護措施的制定:根據風險評估結果,制定切實可行的防護措施。

在網絡安全領域,目前最主要的問題包括以下幾個方面 :

3.1. 資料洩露

- 黑客利用軟件漏洞、社會工程等手段 ,盜取個人隱私數據和企業機密信息
- 一旦用戶的身份信息、銀行賬號等外洩 ,極易遭受盜用、詐騙等犯罪風險

3.2. 木馬病毒

- 惡意程序植入用戶設備,監控用戶行為、盜取信息、發動攻擊
- 木馬病毒傳播迅速 ,一旦感染會給用戶帶來巨大損失

3.3. 分布式拒絕服務(DDoS)攻擊

- 黑客控制大量被感染設備,發動大規模流量攻擊,癱瘓目標網站或系統
- 對政府部門、金融機構等重要行業造成嚴重影響

3.4. 勒索軟件

- 加密用戶文件並索要贖金,給個人和企業帶來極大經濟損失
- 即便支付贖金也無法完全恢復被加密的數據

3.5. 物聯網設備安全

- 物聯網設備(如攝像頭、智能家電)安全性較差,易被黑客控制
- 一旦被入侵,可能成為發動 DDoS 攻擊的"肉機"

綜上所述,網絡安全問題不容忽視,需要政府、企業和個人共同加強防範力度,保護好自身的數字資 產。

4. 案例研究

選擇案例：

選擇一個能夠展示新興技術在實際應用中遇到網絡安全問題的真實案例。

詳細描述問題：

說明該案例中的具體問題，包括問題的起因、過程和影響。

解決過程：

詳細描述問題是如何被解決的，包括使用的具體方法、採取的措施和過程中遇到的挑戰。

評估解決方案：

分析該解決方案的有效性，包括它在何種程度上解決了問題，以及解決方案對實際操作的影響。

從中學習：

根據該案例，提出對其他類似問題的借鑒意義，包括可以學習的經驗教訓和可以避免的錯誤。

未來預防：

根據該案例，提出預防未來出現類似問題的策略和建議。

威脅的性質和來源：

物聯網的威脅主要來源於外部攻擊。

系統漏洞分析：

定期掃描系統，辨識已知漏洞，並及時修補修復。關注作業系統、應用程式、網路設備等關鍵元件。

密切注意漏洞公告,了解最新威脅動態,並儘快採取相應措施。在網絡安全領域,目前最主要的問題包括以下幾個方面：

1. 資料洩露:

- 黑客利用軟件漏洞、社會工程等手段,盜取個人隱私數據和企業機密信息
-旦用戶的身份信息、銀行賬號等外洩,極易遭受盜用、詐騙等犯罪風險

2. 木馬病毒:

- 惡意程序植入用戶設備,監控用戶行為、盜取信息、發動攻擊
-木馬病毒傳播

3.保護措施與模型連繫

1. 保護措施

針對惡意軟件攻擊,網絡釣魚,DDoS,網絡入侵,內部人員威脅時,可使用一些保護措施或防禦策略

- 入侵防禦:

  部署入侵偵測和防禦系統,持續監控網絡活動。
  實施嚴格的身份驗證和訪問控制機制。
  定期備份關鍵數據,以便在發生事故時能夠恢復。

- DDoS 防護:

  採用雲端 DDoS 緩解服務或使用專門的 DDoS 緩解設備。
  設定網路路由器和防火牆以阻擋可疑流量。
  與互聯網服務提供商合作,以識別和緩解 DDoS 攻擊。

- 網絡釣魚防護:

  提高員工的網絡安全意識和識別釣魚郵件的能力。
  部署電子郵件篩選系統,阻擋可疑的釣魚郵件。
  建立嚴格的帳號管理和權限控制政策。

有效性和實施成本:

- 入侵防禦:
  組織需要根據自身的網絡規模、安全需求和預算進行成本效益分析。
  可以採取分階段部署的方式,先針對關鍵系統和數據進行保護。
  結合其他防護措施,如身份管理、加密和備份等,形成多重防線。
  定期評估系統性能和有效性,根據需求調整部署方案。

- DDoS 防護:
  組織需要根據自身的網絡規模、業務性質和可承受的風險程度來選擇 DDoS防護方案。
  若面臨高頻率或大流量的DDoS攻擊,使用專業服務可能更合適和高效。
  對於低頻或小流量的攻擊,自建系統可能更經濟實惠。
  可以採取混合防禦策略,將雲端服務和本地防護系統相結合。
  定期評估DDoS防護系統的性能和效果,根據實際需求調整部署。

- 網絡釣魚防護:
  組織需要根據自身的業務性質、數據敏感性和風險承受能力來制定最合適的防護策略。
  可以採用分層防護的方式,將重點放在關鍵系統和數據上。
  定期評估防護效果,持續優化和調整部署,提高整體的安全性。
  同時加強員工安全意識培訓,減少員工成為攻擊目標的可能性。

2. OSI 模型連繫:

OSI模型是描述網絡通信的一個標準參考模型,其模型分為七層:
1.物理層:負責定義物理連接設備之間的機械、電氣、功能和過程特性。例如,定義電纜的物理特性、信號的電壓、電流等。
2.數據鏈路層:負責可靠地傳輸數據幀,確保數據在物理層無差錯傳輸。例如,MAC地址管理、差錯檢測糾正等。
3.網路層:負責為數據包選擇最佳路徑,實現端到端的邏輯寄址和路由選擇。最著名的就是IP層。
4.傳輸層:負責在端節點之間提供可靠的數據傳輸服務。最著名的是TCP和UDP協議。
5.會話層:負責建立、維護和同步通信雙方的對話,例如建立驗證的會話。
6.表示層:負責定義數據的語法和語義,確保不同系統之間的數據可以正確解釋。例如,數據壓縮、加密等。
7.應用層:為最終用戶提供網絡服務,例如電子郵件、文件傳輸等。

而物聯網在物理層,網絡層和應用層中經常受到攻擊。舉個例子:
物理層:設備安裝位置不當,容易被惡意物理接觸或破壞,缺乏防護措施,易受到電磁干擾,導致通信中斷。

網絡層:采用IPv4/IPv6協議,存在眾多安全漏洞,易被利用發動DoS攻擊。防火牆配置不當,可能遭受非法訪問和入侵。

應用層:應用程序本身存在漏洞,可能被利用發動遠程控制、信息泄露等攻擊。缺乏良好的身份驗證和訪問控制機制。

3 TCP/IP 模型連繫

物聯網的安全問題主要集中在TCP/IP模型的應用層上。因為物聯網設備大多位於應用層其內置的軟體、韌體以及應用程式容易存在安全漏洞,使得整個物聯網系統容易受到攻擊因此我們需要透過加密和常更改密碼來解決問題。

主要的安全考慮包括:

1.身份驗證和授權

實施嚴格的身份認證和權限管理,避免未經授權的訪問。例如在智能家居系統中,通過用戶賬號密碼、生物特徵等方式讓用戶身份驗證,並根據賬號權限控制用戶對家電、安防設備等的訪問權限。

2.加密和安全通信

對通信內容和傳輸過程進行加密,確保數據的機密性和完整性。
例如在車聯網系統中,對車輛傳感器採集的行車數據進行加密處理,並採用安全的通信協議如TLS/SSL進行加密傳輸,防止數據被攔截和竄改。

3.固件/軟體更新機制

例如在工業設備監控系統中,定期自動檢查並更新設備的軟體固件版本,修補已知的安全漏洞,保證設備始終運行在安全狀態。

4. 跨領域整合與合作

4.1 跨領域整合

1.大數據分析和物聯網的整合

物聯網作為新興技術可是深度整合 例如:數據分析可以挖掘和分析各種數據, 而物聯網則是可提供海量的數據供大數據分析來進行分析因此二者可相互幫忙來確保數據的準確性。

2.應用場景和機遇

這項整合技術可以運用到很多範疇如:智慧城市、精準醫療、個性化服務等可讓社會更加發達各大行業的效率提升

3.技術挑戰和安全問題

海量資料處理能力:物聯網產生的海量實時資料給大數據分析系統帶來巨大處理壓力,導致資料可能會出現被修改或者消失的問題。

系統安全性和隱私保護:大量敏感資料的集中管理和分析,容易面臨資料洩露、系統攻擊等安全風險。

演算法偏差和道德風險:基於大數據分析得出的結論可能存在偏差或歧視性,最終需要運用人工花大量的時間修改偏差和歧視性的問題。

4.具體的整合案例和技術上的支持

小愛同學。當你對小愛同學查找資料是物聯網便會將大量資料傳輸到小愛同學然後再經過數據分析篩選出兩份準確資料完成使用著的指令從而方便使用者查找資料。

5.評估整合技術的成本效益和操作可行

本項技術在開發商的成本取決於你對技術開發的成熟、投入多少資金和時間。高可到智慧城市、醫療低可到小愛同學、手機兩者都是受到民眾的認可以小愛同學智能音箱舉例他的製作成本為50元左右出價100多依舊被大多民眾購買可見物聯網和數據分析的技術的合作不僅滿足民眾的好奇還跳過自己尋找資料部分幫民眾節省時間

4.2. 合作機制

- 在技術發展過程中，不同企業和機構之間的合作機制有聯合開發、技術轉讓和戰略聯盟。

- 合作能讓技術的開發成本或風險降低也能提升開發的速度,因為合作能讓技術資源的流動性大大增加 。以合作也能讓技術能更快地商業化應用，不同公司也能發揮各自的優勢，將利益最大化。

- 合作中最主要可能遇到的知識產權問題是版權的歸屬權，需要雙方簽訂保護的對方的合約，以保護雙方的利益。還有常見的數據安全問題有數據共享的安全性，這個問題也能用上面的方法解決。

- 對於物聯網技術，聯合開發和技術轉讓是較為適合的合作模式。因為此技術需要耗費大量的時間和成本去研發技術。

- 提出建立和維護合作伙伴關係的最佳實踐，包括協議制定、風險管理和利益分配等。