計畫名稱：雲端物聯網之自動化佈建、動態事件監測、與主動式大數據服務-雲端物聯網資訊隱密處理與安全資料查詢

執行單位：國立台灣科技大學/資訊工程系
主持人：金台齡

計畫編號：MOST 106-2221-E-011-003

計畫摘要

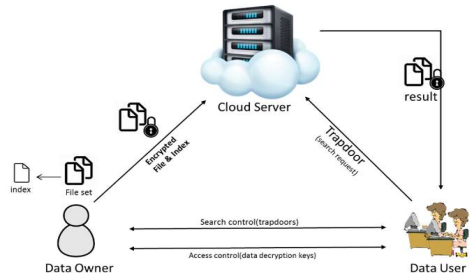
我們針對雲端網路的加密雲數據搜尋與位置服務(LBS)之安全性做更深入的研究。在雲端運算的環境下，數據擁有者在上傳資料前進行加密是必須的，以避免私密訊息遭受雲端伺服器或惡意攻擊者窺探。另外，對保障資料隱私與查詢結果準確性下取得適當的權衡是我們要研究的目標。除此之外，由於行動物件與移動電子設備的普及應用，LBS在各領域廣泛流行，雖然LBS帶給用戶極大的便利性，卻也對用戶的隱私造成威脅，因為用戶在使用LBS的同時會對伺服器揭露過多自身位置與查詢訊息，用戶的隱私訊息可能被惡意侵犯，因此我們也將探討LBS的用戶隱私。

系統架構

本計畫針對加密數據搜尋和位置服務建立了兩種不同的系統架構，以下將分段說明：

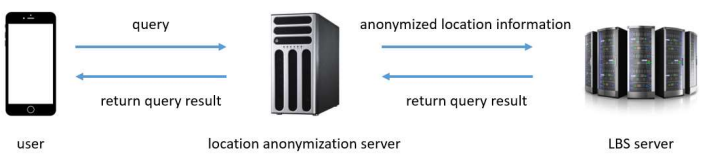
加密數據搜尋

1. 加密索引建子系統：針對Data Owner的文章檔案，為每個檔案建立對應的索引向量，並將檔案和索引加密後上傳至Cloud Server。
2. 關鍵字加密子系統：根據使用者(Data User)下達的搜尋關鍵字，將關鍵字傳至Data Owner並建立對應的暗門(Trapdoor)向量，再回傳給使用者
3. 密文查詢子系統： Cloud Server在收到使用者的暗門向量後，會與內部存放的索引向量進行計算，並回傳搜尋的結果。



位置服務

1. 當使用者(user)想查詢某個興趣點時會將自己的位置資訊(座標、興趣點)作為query傳給匿名伺服器(location anonymization server)
2. 匿名伺服器接收到這些query時會經由分群演算法選擇一個cloaking area，使用者的座標則隱藏在這個區塊中，再將這此區塊傳給LBS server做搜尋。
3. LBS server將此區塊的搜尋結果傳至匿名伺服器，再由匿名伺服器回傳給使用者。



技術特色

加密數據搜尋

1. 利用類神經網路計算文字間的語意關係，得到具有語意關係的word embedding矩陣，並建立對應的索引和查詢向量。
2. 利用矩陣乘法的特性快速的為檔案索引和查詢向量加密，且加密後所計算的搜尋結果與加密前一致。

secret key $SK = \{M_1, M_2, S\}$, M_1, M_2為可逆矩陣，S為split vector

用S將index I分離成兩個向量$\{I', I''\}$，分離的規則如下：

若$S[j]$的值為1，則$I'[j] = I''[j] = I[j]$ ；

若$S[j]$的值為0，則$I'[j] + I''[j] = I[j]$

最後得到的加密索引為$\{M_1^T I_j', M_2^T I_j''\}$

利用S將query vector Q分離成兩個向量$\{Q', Q''\}$，建立secure index的方式如下：

若$S[j]$的值為1，則$Q'[j] + Q''[j] = Q[j]$；

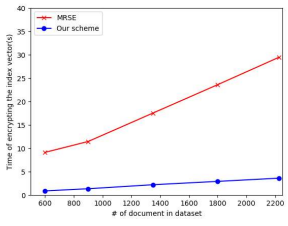
若$S[j]$的值為0，則$Q'[j] = Q''[j] = Q[j]$。

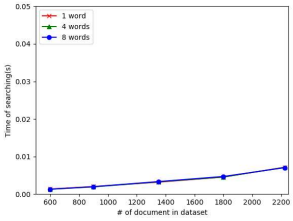
最後得到的暗門為$\{M_1^{-1}Q, M_2^{-1}Q\}$

$$RScore_j = \{M_1^T I_j', M_2^T I_j''\} \cdot \{M_1^{-1}Q, M_2^{-1}Q\}$$

$$= I_j' M_1 M_1^{-1} Q' + I_j'' M_2 M_2^{-1} Q''$$

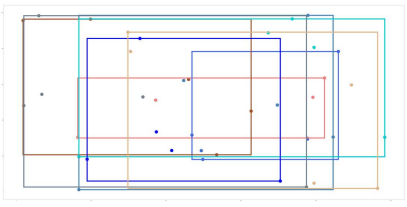
$$= I_j' Q' + I_j'' Q'' \quad = I_j \cdot Q$$

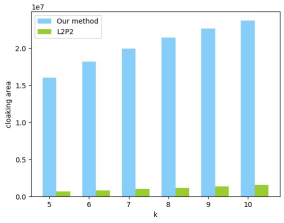




位置服務-分群演算法

1. 盡可能的將群集內每個點的最短距離最大化
2. 座標隱藏在一個區塊中，導致位置服務商不知道在這個區塊中的哪裡
3. 避免選擇的區塊太小，以至於所在的座標大略位置暴露給位置服務商





技術應用範圍

- 汽車導航：避免在連續的查詢中將自己完整的行車軌跡暴露給其他人
- 範圍內興趣點的查詢：在搜尋想要去的興趣點(如：麥當勞)時，避免讓服務提供商知道使用者所在的位置與哪個興趣點比較接近，進而推估出使用者下一個會去的地點。
- 搜尋感興趣的文章：避免讓雲端伺服器知道使用者的興趣習慣