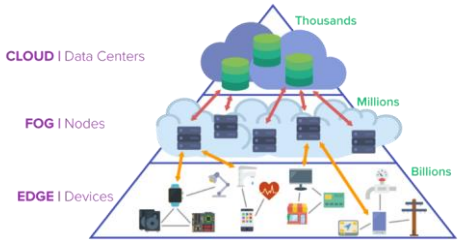
同學論文心得報告:

A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational

隨著雲端儲存與雲端運算的普及化，資料的**隱私性**、**正確性**、**完整性**與**可存取性**成為消費所關注的重點。而在一般傳統的做法中(利用存取限制、資料加密方式)，無法抵禦 internal attackers，因此本篇旨在利用所提出的 *Hash-Solomon code* 與基於 *Fog Computing* 的三層儲存架構。其中 cloud server 儲存大部分的資料，fog server 次之，而 local machine 也會儲存一部分資料，因此當中的任一角色被 compromised 或資料被攻擊者擷取，也無法 100%還原整個原始資料，縱使為 CSP 本身也無法取得關於檔案的有用資訊。



通篇論文最關鍵的部分便在於該如何透過 Hash-Solomon code 演算法，**將資料分散儲存**以保護隱私。當中最關鍵的兩個變數為 k(將資料切成幾塊)與 m(要有多少冗餘資料塊)，提升 k 值有助於降低使用者 local 端的所需空間。k 與 m 的組合會影響所需要的儲存空間效率、頻寬耗用、decoding rate 等等。依據實驗分析結果，可得知隨著 k 上升，編碼與解碼需時皆會上升。因此於實際應用情況中，尚需考量使用者所能容忍的延遲時間，且同時需考慮使用者 local machine 的效能來動態調整 k 值，如：資料塊數量越多，雖能減少使用者本機端所需的儲存空間，但會令 encoding 與 decoding 的效率下降而變得耗時。

除此之外，本篇論文在後面也有提到可以利用 **Computational Intelligence(CI)**以依照當前情況，進行 Hash-Solomon code 運算的調整，期望能提升效率。而依照作者所進行的實驗，也可發現於轉換矩陣中，**Cauchy Matrix** 利用「AND」運算相較於 Vandermonde matrix 利用「XOR」運算更具效率。

總的來說，雖然此三階層儲存架構在現行雲端架構中尚未實現，但隨著資安與隱私意識抬頭，以及未來 IoT 將產生大量非結構化資料，藉由 Fog Computing 能預先將資料儲存或處理。在保證資料隱私與安全性的前提下，能為使用者帶來**更即時的運算**與**更低的延遲**，從而提升使用者體驗並使應用範圍更廣。