國立中山大學 工學院 聯合專題競賽與展示

資訊工程學系
Department of Computer Science and Engineering

第13組：彭煜博、陳品中、柯冠宇　指導老師：范俊逸 教授

植基於屬性加密之外掛式郵件系統

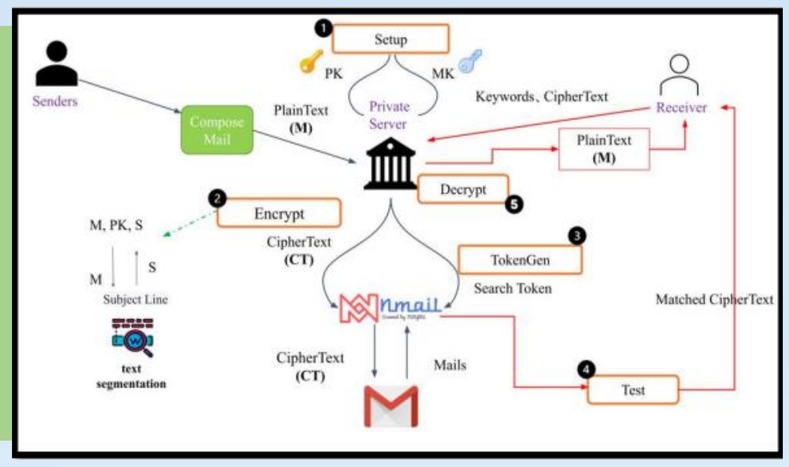
摘要

電子郵件服務提供商作為通信雙方之間的傳訊者，可能具有權限得知或儲存信件內文，因此對通信雙方來說，必然冒著資訊洩漏的風險。為了減少此類資安問題，本團隊將設計出一面向企業內部使用之郵件系統 Nmail，提供加密信件之搜尋和寄送功能，其中寄送郵件之服務提供商可為其他公司所提供之服務，例如 Gmail，而企業只需提供一內部伺服器負責加密金鑰的儲存和加密信件，再經由Nmail寄出加密信件，使服務提供者因為無法對信件進行解密從而知悉信件內容，只單純提供寄送與儲存郵件的功能，實作出一個外掛式的郵件加密系統。

動機

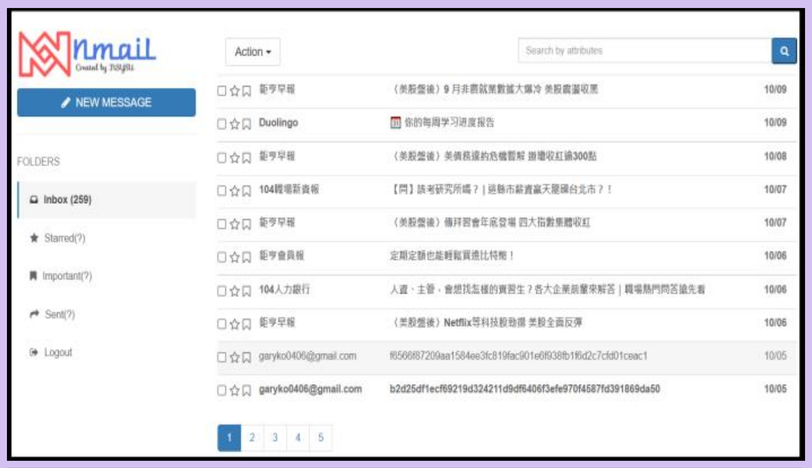
人們往往會忽視網路世界中的安全性及隱私性的問題，如何確保使用者在網路上儲存的資料不會被截取、偷窺，便是本研究要探討的議題。假設所有的電子郵件系統皆不具安全性，為了防範使用這些系統時發生資料外洩的問題，使用者必須讓重要資料以最低限度曝露在網際網路上。因此本團隊提出一種「外掛式郵件加密系統」，讓處理資料的伺服器端「看不到」使用者寄送的資訊和內容，期望能減少諸如上述的風險，保護使用者的資料。

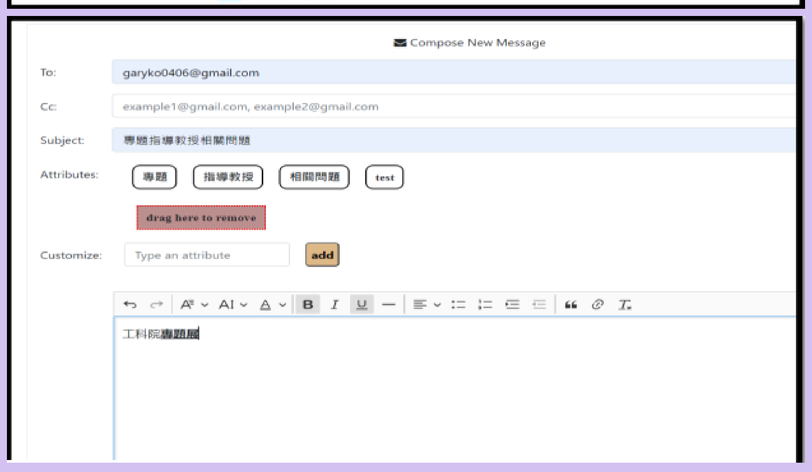
系統總覽圖



成果展示

點我看 demo





未來與展望

實際層面上也不能確定提供訊息傳遞的業者是否可信，因此在日常中的訊息加密上還可以做得更完善。未來這個加密郵件的概念可套用在公司群組或是醫院的病歷系統等注重使用者個人隱私的通訊環境中，落實資訊安全於生活之中。