認證雲 - 成績登錄應用系統

Authentication Cloud, Applied To Student Score Uploading System

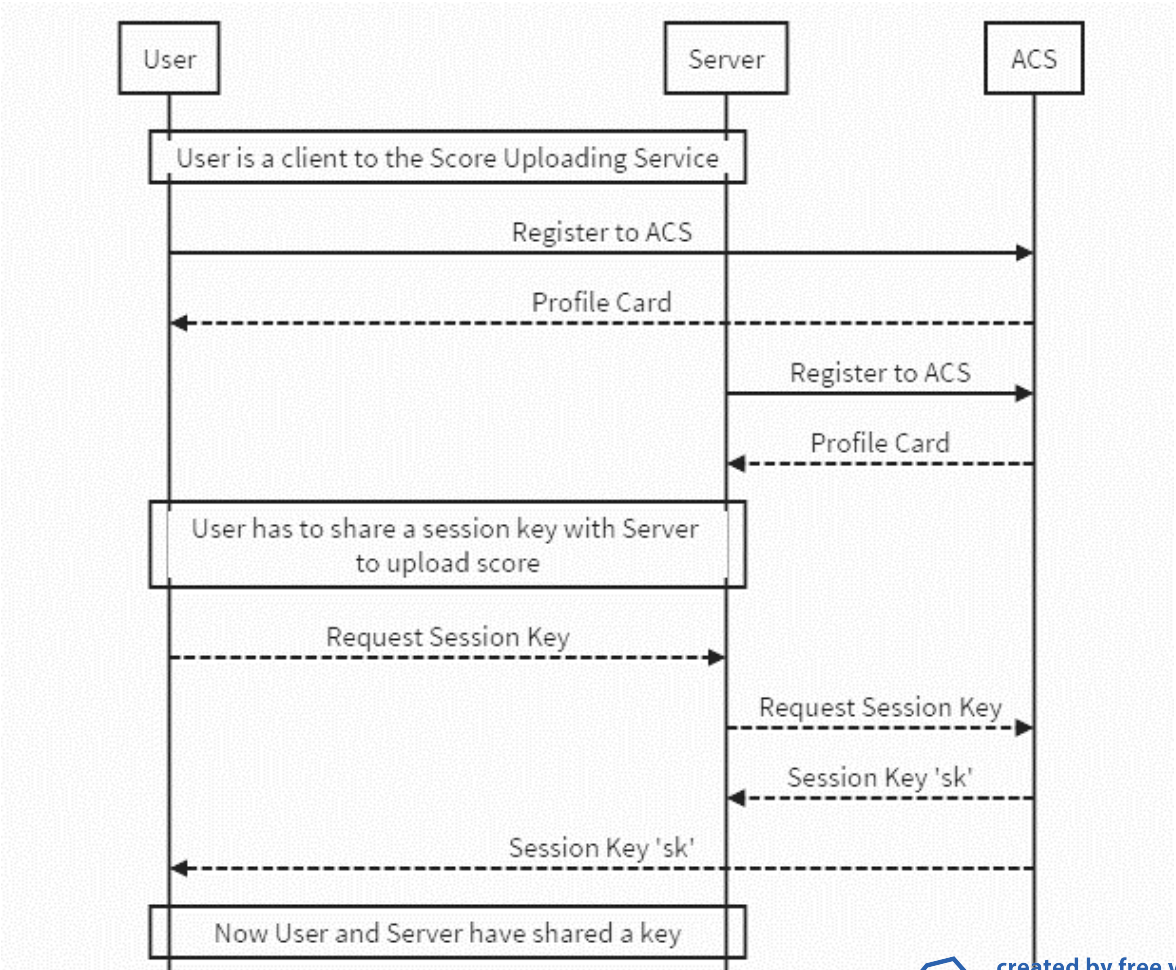
指導教授：黃宗立
專題成員：胡家瑋
開發工具：HTML5、Java、PHP
測試環境：Chrome、Firefox、JDK8、Apache2

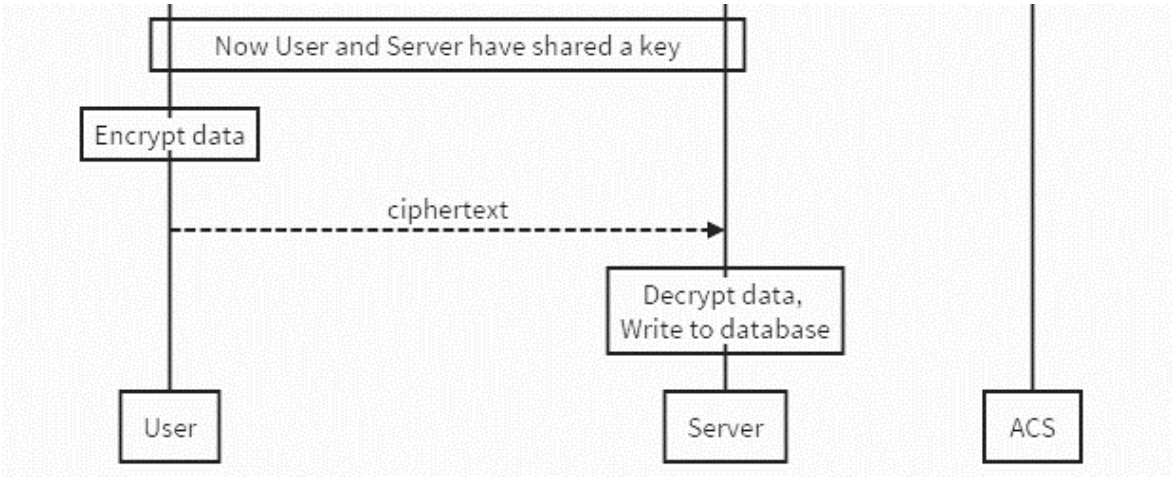
一、 簡介

現今許多網路加密傳輸過程乃是基於公鑰協定，但由於量子電腦發展日新月異，許多常用的公鑰系統將可能被破解，通訊的雙方如何約定金鑰便成為一大難題。因此我們使用雲端認證伺服器 (ACS) 實作出一套基於雜湊法的金鑰分配系統，以此為網路伺服器與其使用者之間分配一把通訊用的金鑰。

本專題以學生成績登錄系統為例，展示認證雲在成績登錄伺服器與成績登錄者（教師）之間分配金鑰的結果。使用者能以此金鑰加密上傳的成績，將密文上傳至伺服器之後再由成績登錄伺服器解密。

系統架構圖：





二、 測試結果

成功完成金鑰分配：

使用此通訊金鑰加密之後的密文：