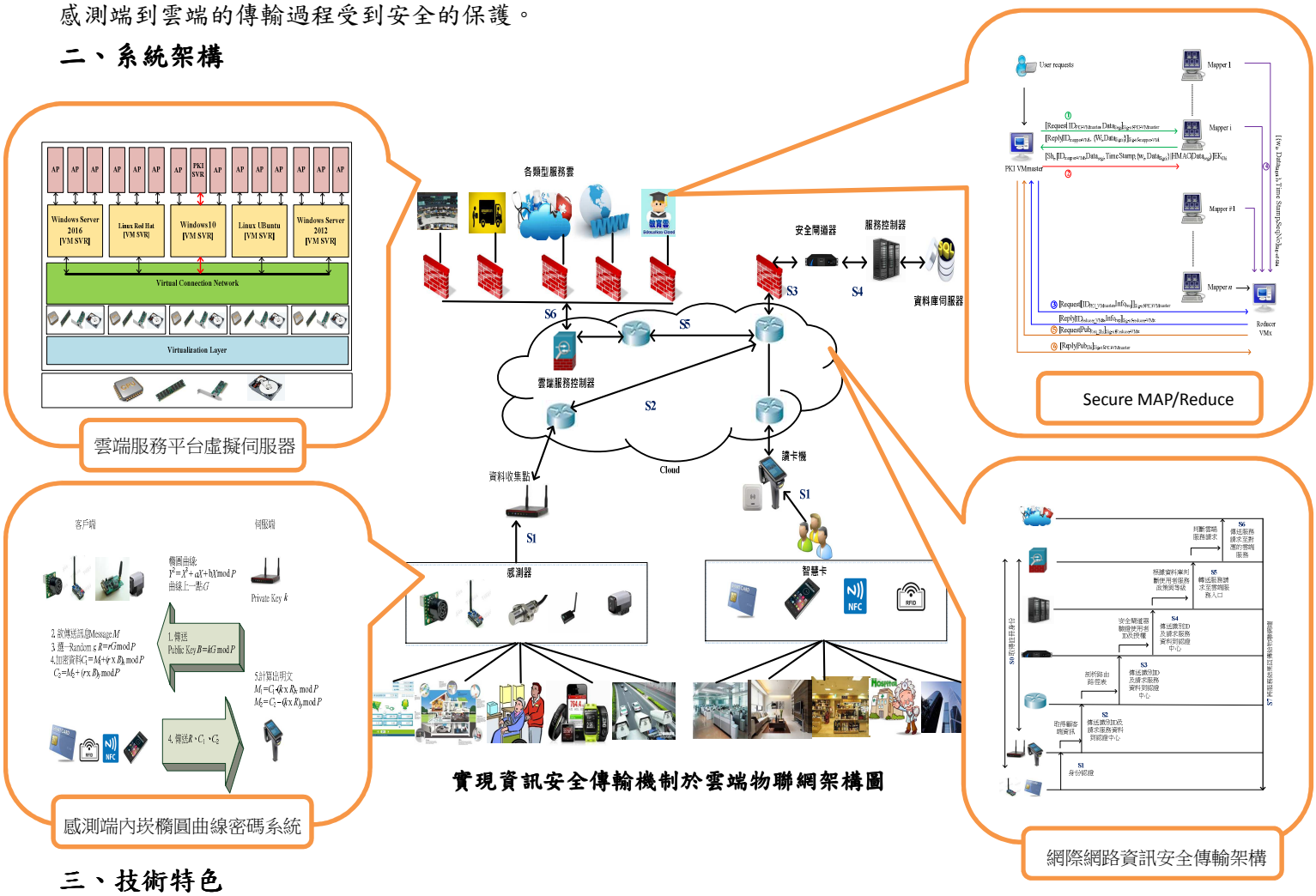
計畫名稱：實現資訊安全傳輸機制於雲端物聯網架構之研究

執行單位：中國科技大學/資管系
主持人：林華乙老師
計畫編號：MOST 106-2221-E-163-001

一、計畫摘要

雲端運算(cloud computing)與物聯網(Internet of things)是資訊科學和通信領域的新浪潮，近年逐漸成為資訊科技主流。許多研究顯示，物聯網和雲端運算的整合仍然屬於發展階段，由於其安全架構的不足，使得各種應用無法順利擴展到雲端物聯網。因此，本研究想提出具備資訊安全傳輸的雲端物聯網架構。我們將物聯網建構在橢圓曲線密碼系統之上，後端結合具備安全映對聚合運算(Secure Map/Reduce)的雲端服務平台，確保資料從感測端到雲端的傳輸過程受到安全的保護。

二、系統架構



實現資訊安全傳輸機制於雲端物聯網架構圖

三、技術特色

本計畫旨於實現資訊安全傳輸機制於雲端物聯網架構之研究，我們運用橢圓密碼曲線崁入感應器及資料收集器(Sink node)透過 ECDH 會議金鑰通訊協議，執行雲端物聯網感測端的資訊安全傳輸機制。當資料進入到網際網路傳輸階段，網際網路通訊協定層(IP Layer)可透過 IPSec，傳輸層(TCP/UDP)運用 SSL/TLS 及應用層(HTTP、FTP、POP 等)可選用 SET、PGP、S/MIME 等網路安全通訊協定對資料傳輸進行保護。最後，資料傳抵後端的雲端服務平台時則透過資訊安全映對聚合(Secure Map/Reduce)通訊協議來確保雲端運算的安全。總體而言本計畫的技術特點在於實現雲端物聯網資訊安全傳輸架構之研究。

四、技術應用範圍

本計畫在功能的完整方面可確保感應端到雲端的資訊安全傳輸之實現，產學合作方面的運用可保護佈署在環境中的感應器進行資料傳輸到雲端服務平台時避免資料被竊取或受到破壞。本研究所採用的橢圓曲線密碼系統需要較短的金鑰長度及較少的加解密運算時間卻可達到 RSA 密碼系統同樣的安全等級，更適合運用在運算資源不足的物聯網環境，此外安全映對聚合運算(Secure Map/Reduce)也可確保後端的雲端運算安全，進而實現資訊安全傳輸機制於雲端物聯網架構之研究。