Communications of the CCISA
Vol. 25 No. 3 Aug. 2019

以雲端技術為基礎建構車聯網資訊安全傳輸系統

吳信德
資訊工程系, 國立澎湖科技大學
wuhsinte@gms.npu.edu.tw

摘要

本文主要是設計一套雲端應用在 VANETs 的網路安全機制，目前雲端計算是政府推動產業發展重點之一，在本文中我們將雲端分成公有雲、私有雲以及混合雲，車輛或者乘客可以透過公有雲存取道路狀況或者大眾運輸資訊，私有雲部分大眾運輸可以存取目前行車紀錄，使用者可以存取企業的相關資訊，混合雲則是將公有雲與私有雲結合，不管在雲端計算或 VANETs 都需要網路與資訊安全保護，目前很多 VANETs 安全研究只針對訊息溝通，沒有針對資訊儲存的部分，雲端計算安全研究只有針對資訊保護，沒有針對使用者隱私以及匿名性，本文設計一套網路與資訊安全機制符合 Confidentiality、Authentication、Non-repudiation、Conditional Anonymity、Conditional Untraceability 要求。

本文主要是需要達到 1.身分驗證機制，乘客與車輛之間可以互相驗證對方身分，並且可以與單一簽入進行身分驗證，2.保持車輛或使用者的隱私以及匿名，需要可以更換車輛或使用者匿名 ID 以及相關參數，3.私密通訊機制，任何車輛或使用者都可以進行私密通訊，4.資訊安全加密方法，讓資料可以在雲端伺服器上保持密文，避免內部人員或者駭客入侵擷取資料。

關鍵字: 車聯網、雲端、網路安全

Communications of the CCISA
Vol. 25 No. 3 Aug. 2019

Constructing Vehicle Network Information Security Transmission System Based on Cloud Technology

Abstract

This paper is mainly to design a cloud security mechanism for cloud applications in VANETs. At present, cloud computing is one of the key points for the government to promote industrial development. In this paper, we divide the cloud into public clouds, private clouds and hybrid clouds. Vehicles or passengers can use public ownership. Cloud access to road conditions or mass transit information, private cloud part of the mass transit can access the current driving record, users can access the relevant information of the enterprise, hybrid cloud is the combination of public cloud and private cloud, whether in the cloud computing or VANETs All need cyber and information security protection. At present, many VANETs security research only deals with information communication. There is no information storage part. The cloud computing security research only focuses on information protection, and does not target user privacy and anonymity. This paper designs a network. It is confidential, certified, undeniable, conditional, and untrackable.

This article mainly needs to achieve 1. Identity verification mechanism, passengers and vehicles can verify each other's identity, and can be verified with a single check-in, 2. Keep the vehicle or user's privacy and anonymity, need to be able to change vehicles or use Anonymous ID and related parameters, 3. Private communication mechanism, any vehicle or user can conduct private communication, 4. Information security encryption method, allowing data to keep ciphertext on the cloud server, avoiding internal personnel or hackers Capture data.

Keywords: Internet of Vehicle、Cloud、Network security

1. Introduction

現今雲端計算已經是目前政府推動產業發展之一，目前民眾都持有智慧型手機無線上網，現在許多公共交通工具會逐漸設有車載無線通訊設備，這些車載無線通訊設備形成的網路稱為 VANET (Vehicular Ad Hoc Network)，VANET 近年來有許多議題在探討，目前許多車輛製造大廠以及企業也開始投入相關研發以及產品開發，VANET 主要是提供一個無線環境讓車輛或者乘客可以進行資訊交流[1] [2]，對於公共交通工具而言，可以透過車載無線裝置傳送行車相關等紀錄到伺服器，以方便交通公司掌握公車的路線以及載車數方便調度車輛，對於乘客而言，可以使用車載無線裝置傳遞郵件或者資訊服務存取加值服務[2]，不管對於交通工具或者乘客而言，網路存取行為形成雲端計算(Cloud Computing)的混合雲機制，大眾交通工具與使用者都可以存取公有雲的資訊，例如:天氣、新聞等，並且也可以存取私有雲的資訊，例如:車輛的載客數、車輛行車紀錄等，雲端計算中對於資訊與網路安全非常重視，資訊在網路傳送時需要注意使用者的匿名性、隱私以及身分的驗證等，這對於 VANETs 的網路安全性要求相符，本文規劃雲端計算技術使用在 VANETs 環境中，使用者可以透過車載裝置存取相關的應用服務，本文會提出一套網路安全應用到本文中，讓任何設備在雲端網路中傳遞資訊都可以保持匿名以及安全性。

美國電子電機工程師協會制定 VANET 的國際標準為 IEEE 1609/WAVE [3]以及 IEEE 802.11p [4]，其中 IEEE 1609/WAVE 制定通訊協定中各層標準，VANET 所使用的無線通訊標準為 IEEE 802.11P，802.11P 使用 5.9 GHz 波段並且共有七個 channel 可以使用[5]，其中一個頻道為控制頻道，二個公共安全專用頻道，四個公共安全/私用共享頻道，IEEE 802.11P 採用 Dedicated Short Range Communications (DSRC) [ASTM 2003]技術標準適合短距離高速傳輸，4G 無線通訊是由 LTE（Long Term Evolution）為 3GPP 聯盟所提出的技術，此聯盟由歐洲通訊大廠 Nokia、Ericsson 組成，改良至今的 LTE-advanced 能夠向下兼容 LTE，擁有理論值 1Gbps 的下載速度，上載速度也達 500Mbps；配合多種頻段，而不同地區選擇的頻段也大不相同，故目前 LTE 手機的使用還無法各處兼容。

本文主要是設計一套雲端應用在 VANETs 的網路安全機制，不管是車載無線通訊裝置或乘客手持通訊設備在雲端上資訊傳遞必須維持資訊在網路的安全性，如果在傳遞過程中遭到駭客惡意竄改或者惡意破壞等行為，會造成資料不完整或者被偽造，並且資料在雲端設備上也必須保持匿名性以及機密性，避免資訊被內部人員取得，本文不管車載無線裝置或者乘客本身都需要進行匿名以及隱私保護，本文主要設計目標如下: 1. 車載無線裝置所送出的資訊需要確保網路安全性，如: Confidentiality、Authentication、Non-repudiation、Conditional Anonymity、Conditional Untraceability，上述網路安全性會在以下會詳細說明。2. 車載無線裝置或者使用者手持裝置為了隱私以及匿名性，需要經常更換自己的相關金鑰參數以及匿名 ID，車載無線裝置或者使用者手持裝置需要自己產生相關金鑰參數以及匿名 ID，並且任何使用者都可以驗證是否為合法使用者。3. 雲 端 上的資訊安全，由於為了確保資訊在雲端伺服器上的隱私，需要將資訊進行加密保護，確保資訊在伺服器上的隱私。4. 資訊的可追蹤性，由於任何設備都會經常更換匿名 ID，

資訊傳遞到伺服器上會因為匿名 ID 的更換，會造成使用者的歷史資訊遺失，所以需要提出完整的安全機制可以追蹤使用者的每一筆資訊。5. 由於CA只有提供設備更換相關參數以及匿名 ID，車載無線裝置與使用者只是驗證是否為合法使用者，而使用者在雲端應用上的相關帳號與密碼會有不同，所以任何設備經由 CA 驗證後，是否可以導入單一簽入伺服器讓使用者選擇雲端的應用。

目前許多 VANET 網路安全研究主要是針對車輛之間訊息傳送的安全性，但由於交通訊息只是廣播讓週遭車輛避免車禍或雍塞等狀況，與一般雲端應用的資訊存取不同，因為這些資訊需要儲存到雲端伺服器，並且匿名 ID 在 VANETs 環境下不斷更換以維持車輛的匿名性，對於資訊存取而言是一大挑戰，在近年來 VANETs 網路安全研究中[6][7][8][9][10][11][12]中只探討廣播訊息驗證，但對於雲端資訊而言是需要私密性加密，對於近年來在雲端計算加解密方法[13][14]，並沒有討論到有關匿名性 ID 更換的方法，本文會結合單一簽入方法整合乘客的雲端應用的相關帳號密碼，目前 VANETs 環境中所以車輛都是互相進行身份驗證，驗證完畢後才能進行訊息溝通傳遞，但目前乘客或者大眾交通工具除了訊息傳遞外，另外還要考慮加值服務，因為現今許多應用程式供應商與大眾交通企業都有提供網路相關應用程式，但這些企業所提供的應用程式所使用的帳號與密碼皆不相同，所以本文提出單一簽入方法整合所有帳號密碼，讓乘客身份驗證後可以直接進入相關的雲端應用。

2. Related Work

文獻[6]中減輕了集中式 AAA 架構的長期驗證的延遲，本文獻主要在 VANETs 環境中保護車輛的隱私以及 portable electronic currency 的網路安全性，本文獻主要是利用 Bilinear Diffie-Hellman (BDH) problem 為基礎提出一套網路安全方法，但本文獻為了達到隱私，每輛車輛必須在每隔一段時間產生 key，每輛車輛需要事先產生 key，這對於車輛是一大負擔。

文獻[10]中利用基於 chameleon hashing 方法來提出一套網路安全機制，本文獻方法可以確保 VANETs 中的車輛隱私以及網路通訊安全，但由於 chameleon hashing 方法計算複雜度以及計算封包長度太大，對於 VANETs 是一大負擔。

文獻[11]中利用基於 Bilinear pairing 方法提出一套網路安全機制，本文獻雖然可以確保車輛在 VANETs 中網路通訊安全，但方法中沒有車輛之間的私密通訊，並且有關車輛更換相關參數還是需要向 TA 更新，這樣會有集中式驗證的問題。

文獻[12]在訊息簽章上使用橢圓曲線數位簽名演算法(Elliptic Curve Digital Signature Algorithm, ECDSA)，演算法是將車輛目前位置、匿名 ID 以及訊息進行簽章，本演算法只提供不需要第三方公正單位驗證，但本演算法沒有私密通訊的網路安全機制。

文獻[9]提出訊息批次驗證以及群組訊息簽章，利用群組簽章來確保訊息的匿名性以及安全性，車輛會自行與鄰近車輛形成群，每一群會自行組成一組相關金鑰，訊息會利用這一組相關金鑰將訊息進行加密，其他車輛無法從訊息追蹤到是由那台車輛所發出的，

所以可以確保車輛的隱私，但如果群中有惡意車輛發送惡意訊息，也無法追蹤到惡意車輛。

文獻[15]主要改善群組簽章演算法，文獻提高群組簽章演算法的效能，但演算法並沒有私密通訊的安全機制，並且沒有討論到車輛相關參數更新，車輛沒有定期更新參數很容易遭到追蹤。

文獻[14]提出雲端計算中的隱私問題以及共享資料匿名存取的改善方法，由於當使用者向其他使用要求要求存取雲端資料時，但如果使用者被拒絕時，拒絕訊息會顯示出來，這並沒有考量到使用者隱私的權力，所以使用者需要匿名顯示，只有被存取端才可以知道那些使用者存取資料。

文獻[13]主要對於雲端儲存的資料完整性，由於雲端儲存資料是儲存到雲端伺服器，資料的完整性是一件具有挑戰的議題，所以本文獻提出利用第三方驗證資料的完整性，並且也確保使用者的隱私以及資料的完整性。

文獻[16]提出雲端的隱私以及安全的問題，並且實際將現今雲端應用的安全問題提出，例如：Amazon's Elastic Compute Cloud (EC2)等，並且實際提出防禦方法抵抗目前雲端的安全性問題，本文獻可以作為本文實際網路安全設計的參考。

文獻[17]提出隱私、資料安全以及網路品質兼顧三方面的安全機制，本文獻利用雜訊加入到原本資料，讓加密資料在傳遞過程中，就算被擷取到也無法知道明文，並且加入雜訊後也不會增加原本資料的長度，文獻的方法可以確保資料的隱私。

文獻[18]提出在雲端環境中的安全架構，一般而言以公有雲的使用者眾多，相對會有潛在的安全性以及隱私問題，此外在操作系統方面也無法保證沒有任何系統漏洞，因此本文獻主要提出對於每一個使用者資料安全架構，確保使用者的資料安全性，並且使用者無法惡意攻擊雲端伺服器。

文獻[19]提出移動雲端運算的架構，主要是雲端情境感知車輛實體系統，情境感知系統可以提供道路實際情況，讓駕駛可以更清楚了解目前道路狀況，情境感知系統包含了駕駛行為檢測系統，可以通知周遭車輛駕駛要進行左轉或右轉以防止意外車禍發生，這些車輛自組形成車輛雲端，可以透過無線通訊系統來進行資料傳遞，提高車輛在道路上的安全。

從文獻探討中 VANETs 環境中的網路安全機制主要為廣播訊息的安全性，但 VANETs 環境下除了交通訊息外，最重要的是乘車與車輛的網路資訊服務，而這些網路資訊服務需要有私密性通訊外，也需要 Confidentiality、Authentication、Non-repudiation、Conditional Anonymity、Conditional Untraceability 要求，本文主要方向在車輛網路雲端計算，在文獻[19]中提出的架構主要適用於車輛網路，但文獻沒有提出相關網路安全機制，這對於資料傳遞上會有被截取或者偽造的風險，對於目前雲端計算的網路安全機制，因為尚未考慮到車輛的匿名 ID 以及隱私的要求，所以無法適用於 VANETs 環境下的雲端應用，本文主要提出一套在 VANETs 環境下雲端計算網路與資訊安全機制。

3. Background

3.1 Bilinear Pairings and Hard Problems

假設 G_1 為 prime order q 的加法群，G_2 為 prime order q 的乘法群，假設 P 為 G_1 的 generator，$\hat{e} = G_1 \times G_1 \to G_2$ bilinear mapping 有以下特性:

1. Bilinear:

   $\hat{e} = (aP, bQ) = \hat{e}(P, Q)^{ab}$

   $\hat{e} = (P_1 + P_2, Q) = \hat{e}(P_{1,} P)\hat{e}(P_{2,} P)$

   $\hat{e} = (P, Q_1 + Q_2) = \hat{e}(P, Q_1)\hat{e}(P, Q_2)$

   , for all $P,Q \in G_1$ and $a, b \in Z_q^*$.

2. Non-degeneracy: $\exists P, Q \in G_1$ such that $\hat{e}(P,Q) \neq 1$. That is, the mapping does not send all pairs in $G_1 \times G_1$ to the identity in G_2.

3. Computable: There exists an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P,Q \in G_1$.

雙線性映射 $\hat{e}$ 由[20] 以及[21]使用實現在橢圓曲線上， G_1 為 161 bits，order q 為 160 bits.

3.2 ID-based cryptosystem

ID-based cryptosystem (IBC)中，任何一個實體的公鑰可以是該實體的外在資訊推衍而得，例如該實體之 e-mail address，並且可以由第三單位 Private Key Generator 即 PKG 來為之產生私有金鑰，然而，該實體與 PKG 的協商會以非對稱式加密的方法來保密傳送內容，即以對方公鑰加密傳送資訊，接收者再自行以私鑰解開。

假設有兩位 User a 與 b，s 為主要金鑰，User a 的身分為 $ID_a \in \{0,1\}^*$，User a 的公開金鑰 $PU_a = H_1(ID_a)$、私密金鑰 $PR_a = s \cdot H_1(ID_a)$，User b 的身分為 $ID_b \in \{0,1\}^*$，User b 的公開金鑰 $PU_b = H_1(ID_b)$、私密金鑰 $PR_b = s \cdot H_1(ID_b)$，公開參數為 $Pub_b = s \cdot P$，User a 與 User b 建立共同金鑰($sk_{a,b}$)，User a 得知 User b 的 ID 就可計算出 User b 的公開金鑰，User a 就可以利用本身的私密金鑰計算出共同金鑰，計算如下:

$$\hat{e}\left(PR_a, PU_b\right) = \hat{e}\left(s \cdot PU_a, PU_b\right) = \hat{e}\left(PU_a, PU_b\right)^s = sk_{a,b} \quad \text{公式 1}$$

User b 與 User a 建立共同金鑰($sk_{b,a}$)，User b 得知 User a 的 ID 就可計算出 User a 的公開金鑰，User b 就可以利用本身的私密金鑰計算出共同金鑰，計算如下:

$$\hat{e}\left(PR_b, PU_a\right) = \hat{e}\left(s \cdot PU_b, PU_a\right) = \hat{e}\left(PU_b, PU_a\right)^s = sk_{b,a} \quad \text{公式 2}$$

所以 User a 與 User b 的共同金鑰相同，其他使用者無法得知 User b 與 User a 的共同金鑰。

3.3 單一簽入機制

使用者在存取每個網路應用程式時，需先經過帳號密碼驗證，而當存取不同伺服器的應用程式時，使用者需重新進行身份驗證動作，對使用者而言除了要記取不同應用程式的相關帳號密碼外，並且每次使用不同應用程式都要重新登入驗證，為了解決上述問題，則有單一簽入(Single Sign-On, SSO)機制的建置，可以省去需要多次登入的麻煩，並且可以將帳號與密碼整合為一組，單一簽入系統讓使用者只要登入一次，就可以存取多個系統而不需要重新進行身分驗證。單一簽入系統是指利用目前廣泛使用的標準瀏覽器，在不同的網站存取資料而不需要重複身分驗證的程序，單一簽入機制有以下角色:

1. 使用者: 對應用程式進行存取的角色。
2. 服務網站: 提供網路服務的角色。
3. 驗證伺服器(Authentication Server): 對使用者進行身分驗證並簽發相關的會議金鑰登入主機。

目前單一簽入分為兩種機制:1.代理人機制、2.重導機制，兩種模式介紹如下:

1.代理人機制:如圖 1 所示，使用者登入服務網站時，服務網站會將使用者的驗證資料給驗證伺服器進行身分驗證，在驗證伺服器確認使用者的驗證資料之後，回傳驗證的結果給使用者。代理人機制在服務伺服器端的設計上會比較複雜。

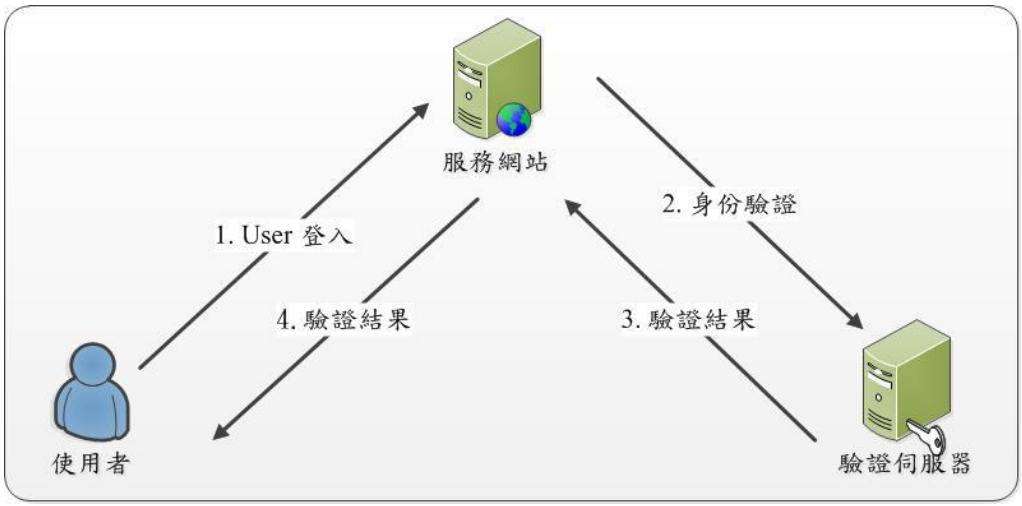

圖 1、代理人機制示意圖

2.重導機制: 如圖 2 所示，服務伺服器不會轉送使用者的驗證資料，使用者被重導到驗證伺服器，由使用者直接將資料送給驗證伺服器進行驗證，確認使用者的身分之後，再由驗證伺服器將使用者重導回服務伺服器繼續後續的活動。

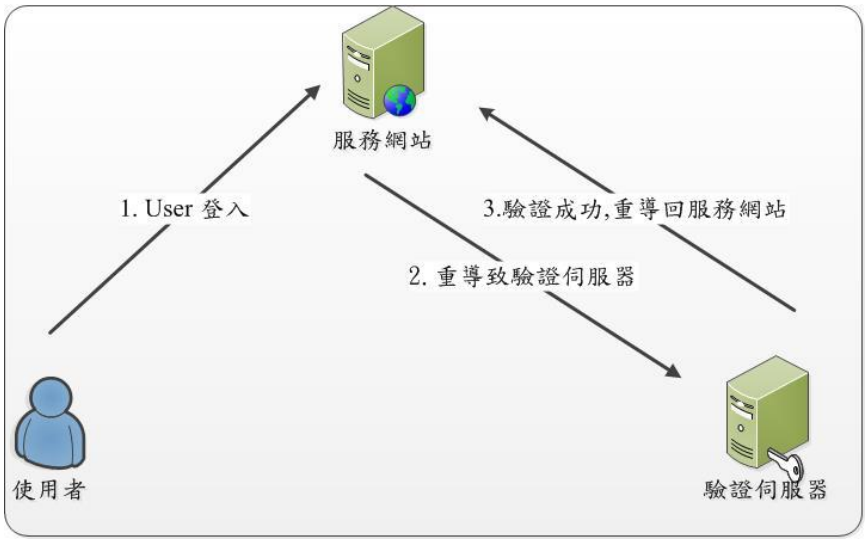

圖 2、重導機制示意圖

本文的安全機制是利用 Bilinear Pairings 技術建置，因為可以使用 IBC 建立雙方共同金鑰,並且使用共同金鑰將明文進行加密,確保不會遭到第三方惡意節點竊聽或竄改,在計算時間上，根據實驗結果 Pairing operation 為 4.5ms、Point Multiplication 為 0.6ms，Field Exponentiation 為 0.54ms，計算時間在可接受範圍內，每次使用訊息加密採用對稱式加密方法，對稱式加密方法的計算時間上小於 4.5ms，本文會採用重導機制的單一簽入，讓單一簽入驗證後再導入到應用程式，本文主要能夠在建置雲端計算在車輛網路環境下，並確保資訊傳遞以及資訊本身的安全性，

3.4 系統模型

如圖 3 為本文規劃的車載裝置雲端示意圖，C_1 至 C_4 為車輛、U_1 至 U_3 為乘客，Certificate Authority (CA)是具有法律的機構用來發送各個實體設備的相關資訊包含網路安全參數，S_1 為單一簽入伺服器用來記錄每個設備在不同雲的網路安全參數，R_1 為 RSU(Roadside Unit)為 3.5G 或 4G 的基地台，RSU 與 CA 之間通訊採用有線網路，車輛都裝有無線設備(On-Board Units,OBU)，乘客與車載裝置或者是車載裝置對 RSU 之間通訊採用無線通訊。

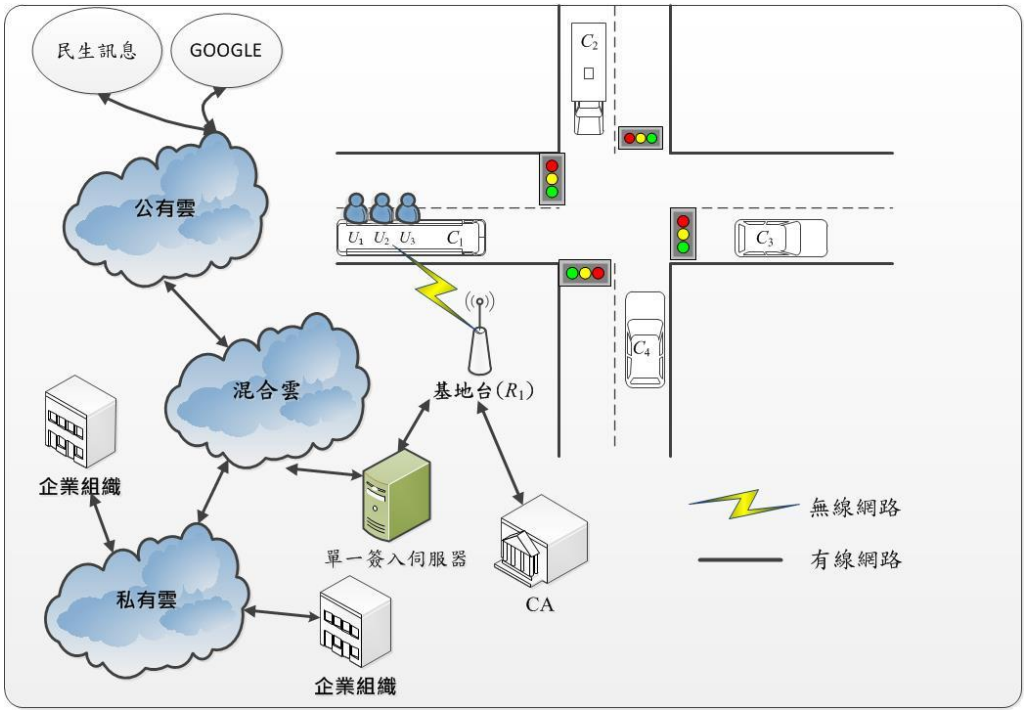

圖 3、車載裝置雲端示意圖

本文主要是在 VANETs 環境中建置雲端環境，以下三種雲端模式:

1. 公有雲: 公有雲是在網際網路上將服務公開給使用者使用，例如:google 雲端空間等，雖然可能是免費或者成本低廉，然而把資料放在「公有雲」上，卻有著資料機密性與安全性的疑慮。

2. 私有雲: 私有雲則通常是由組織內部管理，例如:公司相關報表等，是限制在公司的防火牆內使用，除了不受網路頻寬和潛在性的安全風險之外。

3. 混合雲: 混合雲是跨越公有雲和私有雲，由多個雲組成，可透過標準化的技術，在雲際間進行資料與訊息交換的工作。

4.本文提出的方法

4.1 訊息驗證技術

在訊息驗證技術上，本文主要達到 1.匿名 ID 需要唯一性，2.避免長時間觀察追蹤，3.結合第三代行動通訊 Hand-off 技術進行快速換手。

4.1.1. Bilinear Diffie-Hellman (BDH)訊息驗證介紹:

本文改寫 BHD 方法採用整數運算方式，使用者 i 挑選一個亂數 $h_i \in Z_q^*$ 當作 secret 值，使用者 i 會計算他的 public value (B_i) 並且公告給所有使用者，使用的符號如表 1，使用者 i 要廣播訊息 $M_{i,j}$，簽章流程如下:

1. 使用者 i 計算 $w_{i,j} = H(M_{i,j} \| T_j) \bmod p$ 。
2. 使用者 i 挑選一個亂數 $y_{i,j} \in Z_q^*$ 。
3. 計算 $h_i = y_{i,j} * w_{i,j} + r_{i,j}$ 。
4. 使用者 i 會公告 $\langle M_{i,j}, y_{i,j} \cdot P, ID_i, T_j, \hat{e}(P, r_{i,j} \cdot P) \rangle$ 。

當其他使用者收到訊息後，就可以自行驗證訊息，驗證如下:

1. 計算 $w_{i,j} = H(M_{i,j} \| T_j) \bmod p$ 。
2. 判斷 $\hat{e}(w_{i,j} \cdot P, y_{i,j} \cdot P) + \hat{e}(P, r_{i,j} \cdot P) = \hat{e}(P,P)^{h_i} \stackrel{?}{=} B_i$ ，如果是表示訊息正確。

表 1 Notations of the BDH

Symbol	Notation
h_i	使用者 i 選擇一個亂數 $h_i \in Z_q^*$ 當作 secret 值
B_i	$B_i = \hat{e}(h_i P, P)$
$y_{i,j}$	$y_{i,j} = \frac{h_i}{w_{i,j}}$
$w_{i,j}$	$w_{i,j} = H(M_{i,j} \| T_j) \bmod p$
$r_{i,j}$	餘數
T_j	時間戳記

4.1.2.系統初始化

一開始每個通訊設備的參數由 CA 進行產生，CA 會為 RSU 以及車輛進行參數初始化，每個設備產生的參數有公開金鑰、私密金鑰、Data Key 以及訊息簽章相關參數，CA 參數如下:

1. CA 選擇一個亂數 $h_{ID_{t,CA}} \in Z_q^*$ 當作 secret 值。
2. 本文使用 3 個 hash functions: $H: \{0,1\}^* \to Z_q^*$, $H_1: \{0,1\}^* \to G_1$, and $H_2: G_2 \to \{0,1\}^*$ 。
3. CA 計算 $B_{ID_{t,CA}} = \hat{e}(h_{ID_{t,CA}} P, P)$ 當作 public value。
4. CA 會設定 $D_{ID_{t,CA}} = h_{ID_{t,CA}} \cdot P$ 為 Data key。

5. CA 會設定 $PU_{ID_{t,CA}} = \mathrm{H}_1\left(ID_{t,CA}\right)$ 為公開金鑰，其中 $ID_{t,CA}$ 為 CA 的真實 ID。
6. CA 會設定 $PR_{ID_{t,CA}} = h_{ID_{t,CA}}\mathrm{H}_1\left(ID_{t,CA}\right)$ 為私密金鑰。

CA 會公告參數 $\left(ID_{t,CA}, B_{ID_{t,CA}}, D_{ID_{t,CA}}, \mathrm{H}, \mathrm{H}_1, \mathrm{H}_2\right)$，將 $h_{ID_{t,CA}}$ 保持秘密，CA 會設定每個 RSU 的參數，流程如下:

1. R_R 會選擇一個亂數 $h_{ID_{t,R_R}} \in Z_q^*$ 當作 secret 值。
2. R_R 計算 $B_{ID_{t,R_R}} = \hat{e}\left(h_{ID_{t,R_R}}P, P\right)$ 當作 public value。
3. R_R 計算 $D_{ID_{t,R_R}} = h_{ID_{t,R_R}} \cdot P$ 為 Data key。
4. R_R 計算 $PU_{ID_{t,R_R}} = \mathrm{H}_1\left(ID_{t,R_R}\right)$ 為公開金鑰，其中 ID_{t,R_R} 為 R_R 的基地台編號，基地台編號是唯一的。

以下參數為 CA 所設定:

1. CA 會設定 $PR_{ID_{t,R_R}} = h_{ID_{t,CA}}\mathrm{H}_1\left(ID_{t,R_R}\right)$ 為 R_R 的私密金鑰。
2. CA 挑選一個亂數 $y_{ID_{t,CA},j}$ 。
3. 計算 $y_{ID_{t,CA},j} = \dfrac{h_{ID_{t,CA}}}{w_{ID_{t,CA},j}}$ ， $w_{ID_{t,CA},j} = \mathrm{H}\left(\mathrm{H}_2\left(B_{ID_{t,R_R}}\right) \| ID_{t,R_R} \| T_{l,ID_{t,R_R}}\right) \bmod p$ 。

其中 $y_{ID_{t,CA},j} \cdot P$ 為 R_R 的簽章，R_R 的參數為 $\left(ID_{t,R_R}, B_{ID_{t,R_R}}, D_{ID_{t,R_R}}, x_{ID_{t,CA}}P, y_{ID_{t,CA}}P, e\left(r_{ID_{t,CA}}P, P\right), T_{l,ID_{t,R_R}}\right)$，其中 $T_{l,ID_{t,R_R}}$ 為參數的有效使用時間，CA 會設定每一台車輛的參數設定如下:

1. 車輛 V 挑選一個亂數 $h_{ID_{i,V}} \in Z_q^*$ 當作 secret 值。
2. 車輛 V 計算 $B_{ID_{i,V}} = \hat{e}\left(h_{ID_{i,V}}P, P\right)$ 當作 public value。
3. 車輛 V 計算 Data key 為 $D_{ID_{i,V}} = h_{ID_{i,V}} \cdot P$ 。
4. 車輛 V 計算匿名 ID($ID_{i,V}$)，$ID_{i,V}$ =H($ID_{t,V}$)，其中 $ID_{t,V}$ 為車輛出廠時引擎編號。
5. 計算公開金鑰為 $PU_{ID_{i,V}} = \mathrm{H}_1\left(ID_{i,V}\right)$ 。

以下參數為 CA 所設定:

1. CA 會設定車輛的私密金鑰($PR_{ID_{i,V}} = h_{ID_{t,CA}}\mathrm{H}_1\left(ID_{i,V}\right)$)。
2. CA 會挑選一個亂數 $y_{ID_{t,CA},j} \in Z_q^*$ 。
3. CA 會計算 $y_{ID_{t,CA},j} = \dfrac{h_{ID_{t,CA}}}{w_{ID_{t,CA},j}}$ ， $w_{ID_{t,CA},j} = \mathrm{H}\left(\mathrm{H}_2\left(B_{ID_{i,V}}\right) \| ID_{i,V} \| T_{l,ID_{i,V}}\right) \bmod p$ 。

其中 $y_{I_{t,}D_C} \cdot P$ 為車輛的簽章，車輛的參數為 $\left(ID_{i,V}, B_{ID_{i,V}}, D_{ID_{i,V}}, x_{ID_{t,CA},j}P, y_{ID_{t,CA},j}P, e\left(r_{ID_{t,CA},j}P, P\right), T_{l,ID_{i,V}}\right)$，其中 $T_{l,ID_{i,V}}$ 為參數的有效使用時間，CA 會記錄車輛的真實 ID、匿名 ID 以及 $y_{ID_{t,CA},j} \cdot P$，車輛會利用 CA 所產生的參數與 RSU 進行註冊，並且產生短期簽章以及相關參數。

4.1.3.車輛與 RSU 註冊

我們使用車輛 V_7 會與 R_3 利用 ID-based Cryptosystem 方法產生 common key，計算方法如下:

$$SK_{V_7-R_3}=\hat{e}\left(PR_{ID_{i,V_7}},PU_{ID_{t,R_3}}\right)=\hat{e}\left(PU_{ID_{i,V_7}},h_{ID_{t,TA}}PU_{ID_{t,R_3}}\right)=SK_{R_3-V_7} \quad \text{公式 3}$$

1. 車輛 V_t 計算短期的匿名 ID(ID_{p,V_7})， $ID_{p,V_7}=H\left(ID_{t,R_3}\|ID_{i,V_7}\right)$ 。
2. 車輛 V_t 計算新的 $B_{ID_{p,V_7}}$ 、 $D_{ID_{p,V_7}}$ 。
3. 車輛會利用 common key($SK_{V_7-R_3}$)使用對稱式加密(*SE*())方式將訊息傳送給 RSU 計算如下:

$$C=SE\left(ID_{p,V_7}\|B_{ID_{p,V_7}}\|D_{ID_{p,V_7}}\|T_j\right)_{SK_{V_7-R_3}} \quad \text{公式 4}$$

4. RSU 收到訊息後，利用 common key($SK_{R_R-V_7}$)將密文解開。
5. RSU 計算 $y_{ID_{t,R_3},j}=\dfrac{h_{ID_{t,R_3}}}{w_{ID_{t,R_3},j}}$ ， $w_{ID_{t,R_3},j}=\mathrm{H}\left(\mathrm{H}_2\left(B_{ID_{p,V_7}}\right)\|ID_{p,V_7}\|T_{l,ID_{p,V_7}}\right)\bmod p$ 。
6. RSU 計算車輛的私密金鑰 $PR_{ID_{p,V_7}}=h_{ID_{t,R_3}}\mathrm{H}_1\left(ID_{p,V_7}\right)$ 。
7. RSU 計算車輛 V_7 的私密金鑰並且利用 common key($SK_{V_7-R_3}$)使用對稱式加密(*SE*())方式將密文傳送給車輛，計算如下:

$$C=SE\left(ID_{p,V_7}\|y_{ID_{t,R_3},j}\cdot P\|e\left(r_{ID_{t,R_3},j}\cdot P,P\right)\|PR_{ID_{p,V_7}}\|T_j\right)_{SK_{R_3-V_7}} \quad \text{公式 5}$$

8. V_7 收到訊息後會將密文解密。
9. RSU 會將 V_7 新的參數公告 $\left(ID_{p,V_7},B_{ID_{p,V_7}},D_{ID_{p,V_7}},e\left(r_{ID_{t,R_3},j}P,P\right),y_{ID_{t,R_3},j}P,T_{l,ID_{p,V_7}}\right)$ 給通訊範圍內的車輛，並且記錄 V_7 的 $\left(ID_{i,V_7},ID_{p,V_7},B_{ID_{p,V_7}},D_{ID_{p,V_7}},y_{ID_{t,R_3},j},T_{l,ID_{p,V_7}}\right)$ 。

4.1.4.Hand-off 以及 Key 更新

本文結合第三代行動通訊的 Hand-off 機制進行車輛身分驗證以及 Key 的更新，車輛會定期偵測與 RSU 之間的訊號，當車輛進入到 RSU 的無線通訊邊緣時，車輛會開始與 RSU 進行 Hand-off 機制並且與鄰近 RSU 進行 Key 的更新，首先車輛 V_7 接近無線通訊邊緣時，車輛 V_7 向 R_3 要求進行 Hand-off 機制，R_3 得知 V_7 會進入下一個 RSU 範圍為 R_1，車輛 V_7 計算如下:

1. 車輛 V_7 先計算新的匿名 ID(ID_{p,V_7}')， $ID_{p,V_7}'=H\left(ID_{t,R_1}\|ID_{i,V_7}\right)$ 。
2. 車輛 V_7 計算 $B_{ID_{p,V_7}}$ 、 $D_{ID_{p,V_7}}$ 。
3. 車輛 V_7 利用與 R_3 的 common key($SK_{V_7-R_3}$)將訊息加密後傳送給 R_3，密文為 $C=SE\left(ID_{p,V_7}'\|B_{ID_{p\,V_7}}'\|D_{ID_{p\,V_7}}'\|T_j\right)_{SK_{V_7-R_3}}$ 。

R_3 收到密文後利用 $SK_{R_3-V_7}$ 解密，接下來 R_3 進行車輛 V_7 的 Hand-off 機制，過程如下:

1. R_3 利用與 R_1 的 common key($SK_{R_3-R_1}$)將訊息加密傳送給 R_1，密文為 $C=SE\left(ID_{p,V_7}'\|B_{ID_{p\,V_7}}'\|D_{ID_{p\,V_7,}}'\|T_j\right)_{SK_{R_3-R_1}}$ 。

2. R_1 收到密文後利用 $SK_{R_1-R_3}$ 解密，並且計算車輛 V_7 的 $PR_{ID_{p,V_7}}{}'$ 以及 $y_{ID_{t,R_1},j}P$，R_1 紀錄車輛 V_7 相關參數以及訊息發出的 RSU 的 ID，R_1 利用 $SK_{R_1-R_3}$ 將訊息加密傳送給 R_3，密文為 $C=SE\left(PR_{ID_{p,V_7}}{}' \| y_{ID_{t,R_1}}P \| e\left(r_{ID_{t,R_1}}P,P\right) \| T_j\right)_{SK_{R_1-R_3}}$。
3. R_3 收到密文後利用 $SK_{R_3-R_1}$ 解密，R_3 利用 $SK_{R_3-V_7}$ 將訊息加密後傳送給車輛 V_7，密文為 $C=SE\left(PR_{ID_{p,V_7}}{}' \| y_{ID_{t,R_1}}P \| e\left(r_{ID_{t,R_1}}P,P\right) \| T_j\right)_{SK_{R_1-R_3}}$。
4. 車輛 V_7 收到密文後利用 $SK_{V_7-R_3}$ 解密，車輛 V_7 將參數儲存到車載裝置內。
5. R_1 等待 ΔT 時間後再廣播公告車輛 V_7 參數給範圍內車輛，參數為 $\left(ID_{p,V_7}{}', B_{ID_{p,V_7}}{}', D_{ID_{p,V_7}}{}', e\left(r_{ID_{t,R_1},j}P,P\right), y_{ID_{t,R_1},j}P, T_{l,ID_{p,V_7}}{}'\right)$。

Hand-off 過程中車輛 V_7 沒有一直暴露長期匿名 ID(ID_{i,V_7})，並且當車輛 V_7 發生惡意事件時，RSU 可以從 ID_{p,V_7} 追蹤到 ID_{i,V_7} 最後由 TA 得知車輛真實身份，上述 Hand-off 機制的採用對稱加密方法，對稱加密金鑰都是事先已經建立，所以加解密計算時間很短可以加快 Hand-off 時間，並且 RSU 延遲時間廣播新進車輛參數，避免車輛遭到惡意節點長時間觀察追蹤。

4.2.一般車輛訊息傳遞模式

不管任何車輛都使用兩種無線網路通訊，訊息傳遞方式有兩種 1.訊息廣播模式，車輛或 RSU 透過廣播訊息提供相關資訊給鄰近車輛，2.one hop 訊息傳遞，車輛透過 one hop 方式將訊息傳送給指定的車輛或者 RSU，主要是用於車輛的私密訊息通訊，RSU 會定期廣播範圍內相關交通資訊給範圍內的車輛，交通資訊事件如:道路維修、車禍、道路封鎖、道路壅塞、車輛故障等，由於許多事件無法在短時間排除所以 RSU 需要定期傳送，廣播的 TE_{R_1} 為交通資訊的聚集，TE_{R_1}={事件 1,事件 1 經緯度,…,事件 n,事件 n 經緯度}，R_1 使用 BHD 方式將訊息簽章，簽章方式如下:

1. R_1 計算 $w_{ID_{t,R_1},j}=H\left(TE_{R_1} \| T_j\right) \bmod p$。
2. R_1 計算挑選一個亂數 $y_{ID_{t,R_1},j} \in Z_q^*$。
3. R_1 計算 $h_{ID_{t,R_1}}=y_{ID_{t,R_1},j} * w_{ID_{t,R_1},j}+r_{ID_{t,R_1},j}$。
4. R_1 會公告 $\left\langle H\left(TE_{R_1}\right), TE_{R_1}, y_{ID_{t,R_1},j}\cdot P, ID_{t,R_1}, T_j, \hat{e}\left(P, r_{ID_{t,R_1},j}\cdot P\right)\right\rangle$。

當車輛收到廣播訊息後，車輛會驗證是否 $H\left(TE_{R_1}\right)$ 與車載資訊內的資訊是否相同，如果相同表示交通資訊沒有異動則捨棄訊息，如果不相同則驗證訊息來源性以及完整性，驗證如下:

1. 車輛計算 $w_{ID_{t,R_1},j}=H\left(TE_{R_1} \| T_j\right) \bmod p$。
2. 車輛計算 $\hat{e}\left(w_{ID_{t,R_1},j}\cdot P, y_{ID_{t,R_1},j}\cdot P\right)+\hat{e}\left(P, r_{ID_{t,R_1},j}\cdot P\right)=\hat{e}(P,P)^{h_{ID_{t,R_1}}}$，如果相同則將訊息儲存到車載裝置。

車輛可以透過私密訊息通訊方式透過 RSU 下載或上傳資訊，由於本文考慮到封包路由問題，所以車輛在傳送距離較遠的封包則利用 3.5G 無線通訊避免封包遺失，車輛會定期傳送訊息給 RSU，假設車輛 V_6 與 R_1 建立 common key 進行私密通訊，

車輛 V_6 將所在位置以及匿名 ID 傳送給 R_1，R_1 也可以利用 common key 進行解密，V_6 與 R_1 的 common key 為 $SK_{V_6-R_1}=\hat{e}\left(PR_{ID_{p,V_6}},PU_{ID_{t,R_1}}\right)=\hat{e}\left(PU_{ID_{p,V_6}},h_{ID_{t,R_1}}PU_{ID_{t,R_1}}\right)=SK_{R_1-V_6}$ 。

車輛第二種無線通訊為 802.11P 無線通訊，由於 802.11P 屬於短距離無線通訊，並且如果要傳送距離較長的封包需要依靠車輛之間的傳送，車輛屬於高速移動並且會更換匿名 ID，所以很容易造成封包遺失情況，本文使用第二種無線通訊廣播訊息，主要是針對緊急事件廣播以及搜尋鄰近車輛所在位置，當車輛發生或發現事故時，車輛需發出廣播訊息警告鄰近車輛，簽章方法使用 BHD 技術，並且傳送私密訊息通訊給 RSU 紀錄交通資訊，因為從事故發生到結束都會影響道路安全以及行車效率，當訊息廣播送出後很快訊息就不會在延續傳送，所以需要固定 RSU 定期廣播訊息，讓新進車輛可以得知範圍內的交通資訊，車輛會定期廣播訊息告知自己所在位置給其他車輛，以方便車輛建立路由網路分享影音資訊。

4.3. 救援車輛訊息傳遞以及號誌時間調整

假設 RSU 可以控制通訊範圍內號誌的時間，RSU 內有範圍內的地圖資訊，所以可以得知範圍內的道路位置，雖然 RSU 可以從車輛上取得事故地點、施工地點等資訊，RSU 需要偵測道路雍塞情況，車輛會定期傳送 GPS 資訊給 RSU，GPS 包含經緯度、時間、速度以及行車方向，RSU 可以取得道路的綠燈時間，RSU 在某個區段時間內每條道路的綠燈時間收集車輛的速度，然後將收集後的速度平均就是道路平均速度，公式如下:

$$RS_{num,D}=\frac{Speed_{ID_{p,V_6}}+Speed_{ID_{p,V_7}}+...+Speed_{ID_{p,V_m}}}{n} \quad \text{公式 6}$$

$Speed_V$ 為車輛的速度、$RS_{num,D}$ 為道路的平均速度，接下來車輛可以由道路平均速度判斷車輛雍塞狀況。

當救援車輛取得救難任務目的地時，如圖 1 所示，救難車輛 EV_1 先向 CA 取得簽章流程如下:

1. 車輛建立與 CA 的 common key，
   $SK_{EV_1-CA}=\hat{e}\left(PR_{ID_{t,EV_1}},PU_{ID_{t,CA}}\right)=\hat{e}\left(PU_{ID_{t,EV_1}},h_{ID_{t,CA}}PU_{ID_{t,CA}}\right)=SK_{CA-EV_1}$ 。
2. 車輛利用 SK_{EV_1-CA} 將訊息加密，密文為 $C=SE\left(M_{ID_{t,EV_1}}\|T_j\right)_{SK_{EV_1-CA}}$，$M_{ID_{t,EV_1}}$ 為事件的經緯度以及事件內容。
3. CA 收到密文後使用 SK_{CA-EV_1} 解密，接下來 CA 為車輛 EV_1 進行簽章，並且 CA 將訊息儲存。
4. CA 計算 $w_{ID_{t,CA},j}=H\left(M_{ID_{t,CA},j}\|T_j\right)\bmod p$ 。
5. CA 計算 $h_{ID_{t,CA}}=y_{ID_{t,CA},j}*w_{ID_{t,CA},j}+r_{ID_{t,CA},j}$ 。
6. CA 使用 SK_{CA-EV_1} 加密，密文為 $C=SE\left(y_{ID_{t,CA},j}\cdot P\|e\left(r_{ID_{t,CA},j}\cdot P,P\right)\|T_j\right)_{SK_{CA-EV_1}}$ 。
7. 車輛收到密文解密後將簽章儲存。

救援車輛當進入 RSU 範圍時，需要 RSU 協助調整號誌時間讓救援車輛快速抵達目的地，首先車輛除了與 RSU 驗證身分外，另外傳送救援車輛行經道路資訊及

CA 簽章給 RSU，流程如下:

1. 車輛 EV_1 建立與 R_1 的 common key，
   $SK_{EV_1-R_1}=\hat{e}\left(PR_{ID_{t,EV_1}},PU_{ID_{t,R_1}}\right)=\hat{e}\left(PU_{ID_{t,EV_1}},h_{ID_{t,CA}}PU_{ID_{t,R_1}}\right)=SK_{R_1-EV_1}$ 。
2. 車輛 EV_1 利用 $SK_{EV_1-R_1}$ 將訊息加密，
   $C=SE\left(\text{map}_{ID_{t,EV_1}}\|M_{ID_{t,EV_1}}\|y_{ID_{t,CA},j}\cdot P\|e\left(r_{ID_{t,CA},j}\cdot P,P\right)\|T_j\right)_{SK_{EV_1-R_1}}$ 。

R_1 收到訊息後利用 $SK_{R_1-EV_1}$ 解密，會驗證簽章確認是否為 CA 所發出，驗證流程如下:

1. R_1 計算 $w_{ID_{t,CA},j}=H\left(M_{ID_{t,CA},j}\|T_j\right)\text{mod}\,p$ 。
2. R_1 計算 $\hat{e}\left(w_{ID_{t,CA},j}\cdot P,y_{ID_{t,CA},j}\cdot P\right)+\hat{e}\left(P,r_{ID_{t,CA},j}\cdot P\right)=\hat{e}\left(P,P\right)^{h_{ID_{t,CA}}}$ ，如果相同則將訊息儲存。

接下來救援車輛可以廣播 CA 簽章給周遭車輛，請周遭車輛進行讓道，救援車輛所廣播的訊息為 $M_{ID_{t,EV_1}}\|y_{ID_{t,CA},j}\cdot P\|e\left(r_{ID_{t,CA},j}\cdot P,P\right)\|T_j$ ，其他車輛可以驗證簽章是否合法，驗證流程如下:

1. 其他車輛計算 $w_{ID_{t,CA},j}=H\left(M_{ID_{t,CA},j}\|T_j\right)\text{mod}\,p$ 。
2. 其他車輛計算 $\hat{e}\left(w_{ID_{t,CA},j}\cdot P,y_{ID_{t,CA},j}\cdot P\right)+\hat{e}\left(P,r_{ID_{t,CA},j}\cdot P\right)=\hat{e}\left(P,P\right)^{h_{ID_{t,CA}}}$ ，如果相同則表示簽章合法。

假設每條道路都有綠燈最小門檻時間以及綠燈最大門檻時間，綠燈最小門檻時間為行人行走道路完成時間，設定最小門檻值避免車輛或行人行走時遭到碰撞，$Th_{g,\min}=\frac{ZC_{num}}{PV}$，其中 $Th_{g,min}$ 為最小門檻時間、ZC_{num} 為斑馬線的距離、PV 為行人行走的速度，綠燈最大門檻時間($Th_{g,max}$)假設為兩個紅燈的秒數時間，設定最大門檻時間避免車輛等待時間太長，RSU 控制號誌時間秒數，如圖 4 所示，流程如下:

1. RSU 利用上述道路平均行駛速率計算救援車輛到達十字路口時間。
2. 判斷救援車輛到達十字路口時是否為綠燈號誌，如果是不需要變動號誌時間，接下來計算救援車輛下一條道路時間從 1 開始計算，直到達到目的地。。
3. 如果不是為綠燈號誌，判斷車輛到達十字路口時間會不會超過綠燈最大門檻時間，如果不會超過最大門檻時間，則延長綠燈時間直到車輛離開十字路口時間為止，並且同步連接道路號誌綠燈時間，接下來計算救援車輛下一條道路時間從 1 開始計算，直到達到目的地。
4. 如果超過綠燈最大門檻時間，將縮短紅燈時間為最小紅燈時間(綠燈最小門檻時間=最小紅燈時間)，並且同步連接道路號誌時間，接下來計算救援車輛下一條道路時間從 1 開始計算，直到達到目的地。

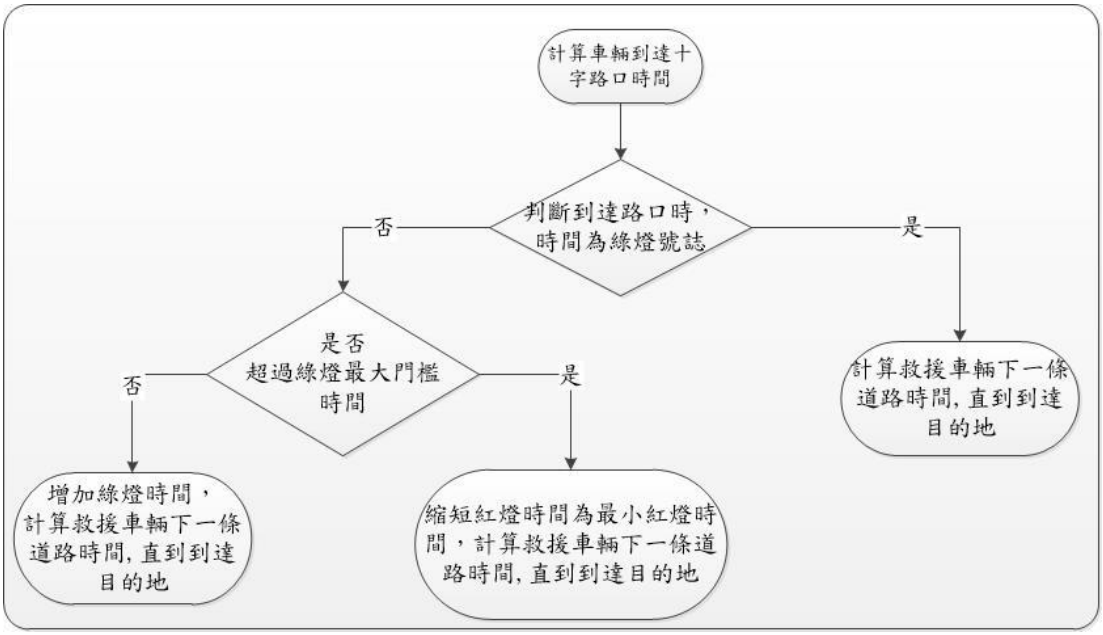

圖 4、RSU 控制號誌流程圖

4. Conclusion

本文主要是設計一套雲端應用在 VANETs 的網路安全機制，不管是車載無線通訊裝置或乘客手持通訊設備在雲端上資訊傳遞必須維持資訊在網路的安全性，如果在傳遞過程中遭到駭客惡意竄改或者惡意破壞等行為，會造成資料不完整或者被偽造，並且資料在雲端設備上也必須保持匿名性以及機密性，避免資訊被內部人員取得，本文不管車載無線裝置或者乘客本身都需要進行匿名以及隱私保護。

References

[1] U.S. Dept. Transp., " Nat. Highway Traffic Safety Admin.", Vehicle Safety Communications Project. 2006.

[2] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, " Secure incentives for commercial ad dissemination in vehicular networks", in Proc. ACM IntSymp. MobiHoc ,pp. 150-159, 2007.

[3] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services.IEEE 1609, 2006.

[4] IEEE P802.11p/D11.0, "Draft Amendment for Wireless Access in Vehicular Environments (WAVE)," IEEE 802.11 Working Group of the IEEE 802 Committee, Mar. 2010.

[5] Qing Wang, Supeng Leng, Huirong Fu, and Yan Zhang, "An IEEE 802.11p-Based Multichannel MAC Scheme With Channel Coordination for Vehicular Ad Hoc Networks", IEEE Transactions on Intelligent Transportation Systems, VOL. 13, NO. 2, JUNE 2012.

[6] Lo-Yao Yeh and Jiun-Long Huang, "PBS: A Portable Billing Scheme with Fine-Grained Access Control for Service-Oriented Vehicular Networks", IEEE Transactions on Mobile Computing, Vol. 13, No. 11, November 2014.

[7] Ming-Chin Chuang and Jeng-Farn Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks" , IEEE Systems Journal, Vol. 8, No. 3, September 2014.

[8] S. Biswas and J. Misic, "A cross-layer approach to privacypreserving authentication in WAVE-enabled VANETs," IEEE Transactions on Vehicular Technology, vol. 62, no. 5, pp. 2182– 2192, 2013.

[9] S.-J.Horng, S.-F. Tzeng, Y. Pan et al., "B-SPECS+: batch verification for secure pseudonymous authentication in VANET," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1860–1875, 2013.

[10] Song Guo, Deze Zeng and Yang Xiang, "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 11, November 2014.

[11] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," IEEE Transactions on Computers, vol. 63, no. 2, pp. 510–524, 2014.

[12] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 63, No. 2, February 2014.

[13] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren and Wenjing Lou, "Privacy-

Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, Vol. 62, No. 2, FEBRUARY 2013.

[14] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, JANUARY 2015.

[15] J. Zhang,W. Zhen, and M. Xu, "An efficient privacy-preserving authentication protocol in VANETs," in Proceedings of the 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Networks (MSN '13), pp. 272–277, December 2013.

[16] Zahir Tari," Security and Privacy in Cloud Computing Zahir Tari", IEEE Cloud Computing Published By The IEEE Computer Society 2014.

[17] YANG Pan, GUI Xiaolin, AN Jian, YAO Jing, LIN Jiancai and TIAN Feng, "A Retrievable Data Perturbation Method Used in Privacy-Preserving in Cloud Computing", Communications System Design 2014.

[18] Vijay Varadharajan, and Udaya Tupakula, "Security as a Service Model for Cloud Environment", IEEE Transactions on Network and Service Management, Vol. 11, No. 1, March 2014.

[19] Jiafu Wan, Daqiang Zhang, Shengjie Zhao, Laurence T. Yang, and Jaime Lloret, "Context-Aware Vehicular Cyber-Physical Systems with Cloud Support: Architecture, Challenges, and Solutions", Context-Aware Networking and Communications 2014.

[20] M. Scott, "Computing the tate pairing," in Proceedings of the International Conference on Topics in Cryptology, pp. 293–304, Springer, San Francisco, Calif, USA, 2005.

[21] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, Calif, USA, August 2001.