【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I755951
【45】公告日： 中華民國 111 (2022) 年 02 月 21 日
【51】Int. Cl.：　*H04L29/08　(2006.01)*　　*H04W4/02　(2018.01)*
G06F15/163　(2006.01)

發明　　全 8 頁

【54】名　　稱：通訊系統及通訊方法

【21】申請案號：109142195　　【22】申請日： 中華民國 109 (2020) 年 12 月 01 日

【72】發 明 人： 林盈達 (TW) LIN, YING-DAR；張　德泰 (VN) TRUONG, DUC TAI；司德 (PK) ALI, ASAD；李奇育 (TW) LI, CHI-YU；賴源正 (TW) LAI, YUAN-CHENG
【71】申 請 人： 國立陽明交通大學
新竹市大學路 1001 號
【74】代 理 人： 蘇建太

【56】參考文獻：
TW　201807961A　　US　2014/0146673A1
US　2015/0271169A1

審查人員：黃偉倫

【57】申請專利範圍

1. 一種通訊系統，用於進行一邊界服務端(4)及一雲端服務端(3)之間的第三方認證，包含：一第一認證機制執行模組(21a)，設置於一代理伺服器(2)，用於執行一第一認證機制，並包含一虛擬歸屬用戶伺服器(virtual home subscriber server，V HSS)(211)及一虛擬使用者(virtual user equipment，vUSER)(212)，其中該虛擬歸屬用戶伺服器(211)用於與該邊界服務端(4)的一移動性管理實體(mobility management entity，MME)(410)進行通訊，該虛擬使用者(212)用於與該雲端服務端(3)進行通訊；其中，當該雲端服務端(3)的一帳戶欲使用該邊界服務端(4)的服務時，該第一認證機制執行模組(21a)執行該第一認證機制，其中該第一認證機制包含步驟：當該使用者設備(5)對該邊界服務端(4)發出一服務請求，且該雲端服務端(3)確認該使用者設備(5)的一國際移動用戶辨識碼合法時，藉由該虛擬使用者(212)接收該雲端服務端(3)提供的一認證向量，並由該虛擬歸屬用戶伺服器(211)、該移動性管理實體(410)及該使用者設備(5)根據該認證向量進行演進分組系統-認證密鑰協商協議(evolved packet system-authentication and key agreement，EPS-AKA)之證認。
2. 如請求項 1 所述的通訊系統，其中更包含一第二認證機制執行模組(21b)，設置於該代理伺服器(2)，用於執行一第二認證機制，並包含一虛擬使用者設備(virtual user equipment，vUE)(213)及一虛擬開放式身分提供者(virtual open ID provider，OP)(214)，該虛擬使用者設備(213)用於與該邊界服務端(4)的該移動性管理實體(410)進行通訊，該虛擬開放式身分提供者(214)用於與該雲端服務端(3)及一使用者設備(5)進行通訊，其中當該邊界服務端(4)的一帳戶欲使用該雲端服務端(3)的服務時，第二認證機制執行模組(21b)執行該第二認證機制，其中該第二認證機制包含步驟：當該使用者設備(5)對該雲端服務端(3)提出一服務請求，且該邊界服務端(4)的一歸屬用戶伺服器(420)確認該使用者設備(5)的一國際移動用戶辨識碼合法時，藉由該虛擬使用者設備(213)，經由該移動性管理實體(410)，接收該歸屬用戶伺服器(420)提供的一認證向量，並藉由該虛擬使用者設備(213)及該虛擬開放式身分提供者(214)將該認證向量傳送至傳送至該使用者設備(5)，使該使用者設備(5)對根據該認證向量計算出一挑戰回應參數(RES)，以及藉由該歸屬用戶伺服器(420)、該移動性

管理實體(410)及該虛擬使用者設備(213)及該使用者設備(5)，根據該認證向量及該挑戰回應參數(RES)進行進行 EPS-AKA 之認證，以及藉由該虛擬開放式身分提供者(214)、該雲端服務端(3)及該使用者設備(5)進行開放式身分連結(openID connect，OIDC)之認證；以及當 EPS-AKA 之認證完成時，藉由該虛擬開放式身分提供者(214)提供一權證(token)至使用者設備(5)，其中該雲端服務端(3)根據該權證提供服務。

3. 一種通訊方法，透過一通訊系統(1)執行，用於進行一邊界服務端(4)及一雲端服務端(3)之間的第三方認證，該通訊方法包含步驟：當該雲端服務端(3)的一帳戶欲使用該邊界服務端(4)的服務時，藉由設置於一代理伺服器(2)的一第一認證機制執行模組(21a)執行一第一認證機制，其中該第一認證機制執行模組(21a)包含一虛擬歸屬用戶伺服器(211)及一虛擬使用者(212)，該虛擬歸屬用戶伺服器(211)用於與該邊界服務端(4)的一移動性管理實體(410)進行通訊，該虛擬使用者(212)用於與該雲端服務端(3)進行通訊，其中該第一認證機制包含步驟：當該使用者設備(5)對該邊界服務端(4)發出一服務請求時，藉由該移動性管理實體(410)、該虛擬歸屬用戶伺服器(211)及該虛擬使用者(212)，將該使用者設備(5)的一國際移動用戶辨識碼傳送至該雲端服務端(3)進行校驗；以及當該使用者設備(5)對該邊界服務端(4)發出一服務請求，且該雲端服務端(3)確認該使用者設備(5)的一國際移動用戶辨識碼合法時，藉由該虛擬使用者(212)接收該雲端服務端(3)提供的一認證向量，並由該虛擬歸屬用戶伺服器(211)、該移動性管理實體(410)及該使用者設備(5)根據該認證向量進行演進分組系統-認證密鑰協商協議之證認。

4. 如請求項 3 所述的通訊方法，其更包含步驟：當該邊界服務端(4)的一帳戶欲使用該雲端服務端(3)的服務時，藉由設置於該代理伺服器(2)的一第二認證機制執行模組(21b)執行一第二認證機制，其中該第二認證機制執行模組(21b)包含一虛擬使用者設備(213)及一虛擬開放式身分提供者(214)，該虛擬使用者設備(213)用於與該邊界服務端(4)的該移動性管理實體(410)進行通訊，該虛擬開放式身分提供者(214)用於與該雲端服務端(3)及一使用者設備(5)進行通訊，其中該第二認證機制包含步驟：當該使用者設備(5)對該雲端服務端(3)提出一服務請求時，藉由該虛擬開放式身分提供者(214)、該虛擬使用者設備(213)及該移動性管理實體(410)，將該使用者設備(5)的一國際移動用戶辨識碼傳送至該歸屬用戶伺服器(420)進行校驗；當該使用者設備(5)對該雲端服務端(3)提出一服務請求，且該邊界服務端(4)的一歸屬用戶伺服器(420)確認該使用者設備(5)的一國際移動用戶辨識碼合法時，藉由該虛擬使用者設備(213)，經由該移動性管理實體(410)，接收該歸屬用戶伺服器(420)提供的一認證向量，並藉由該虛擬使用者設備(213)及該虛擬開放式身分提供者(214)將該認證向量傳送至傳送至該使用者設備(5)，使該使用者設備(5)對根據該認證向量計算出一挑戰回應參數(RES)，以及藉由該歸屬用戶伺服器(420)、該移動性管理實體(410)及該虛擬使用者設備(213)及該使用者設備(5)，根據該認證向量及該挑戰回應參數(RES)進行進行 EPS-AKA 之認證，以及藉由該虛擬開放式身分提供者(214)、該雲端服務端(3)及該使用者設備(5)進行開放式身分連結(openID connect，OIDC)之認證；以及當 EPS-AKA 之認證完成時，藉由該虛擬開放式身分提供者(214)提供一權證(token)至使用者設備(5)，其中該雲端服務端(3)根據該權證提供服務。

圖式簡單說明

圖 1 是本發明一實施例的通訊系統的系統架構圖。

圖 2(A)是本發明一實施例的通訊系統執行第一認證機制的訊號傳輸示意圖。

圖 2(B)是本發明一實施例的通訊方法(第一認證機制)的細部流程圖。

圖 3(A)為本發明一實施例的通訊系統執行第二認證機制的傳輸示意圖。

圖 3(B)是本發明一實施例的通訊方法(第二認證機制)的細部流程圖。

圖 4 是本發明另一實施例的通訊方法的細部流程圖。

圖 5(A)為本發明另一實施例的通訊系統的系統架構圖。

圖 5(B)為本發明又另一實施例的通訊系統的系統架構圖。

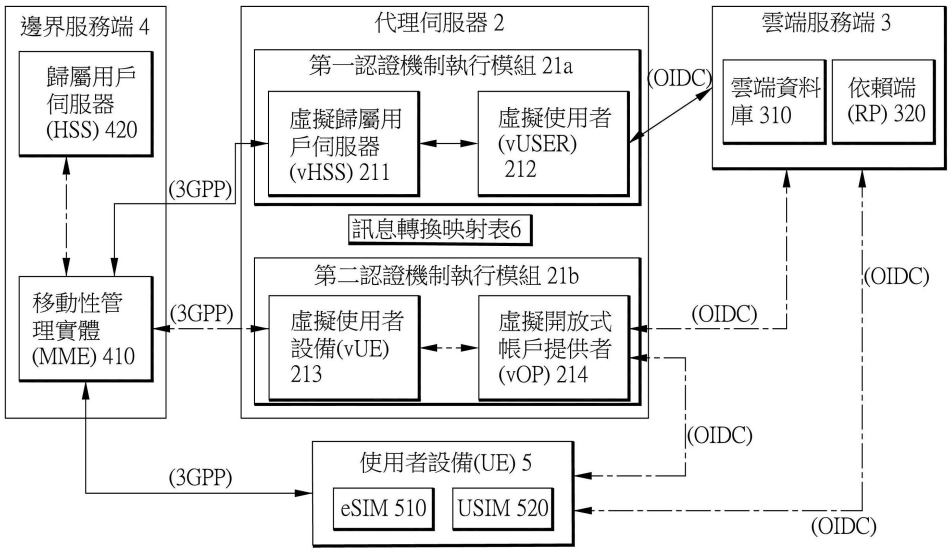

圖1

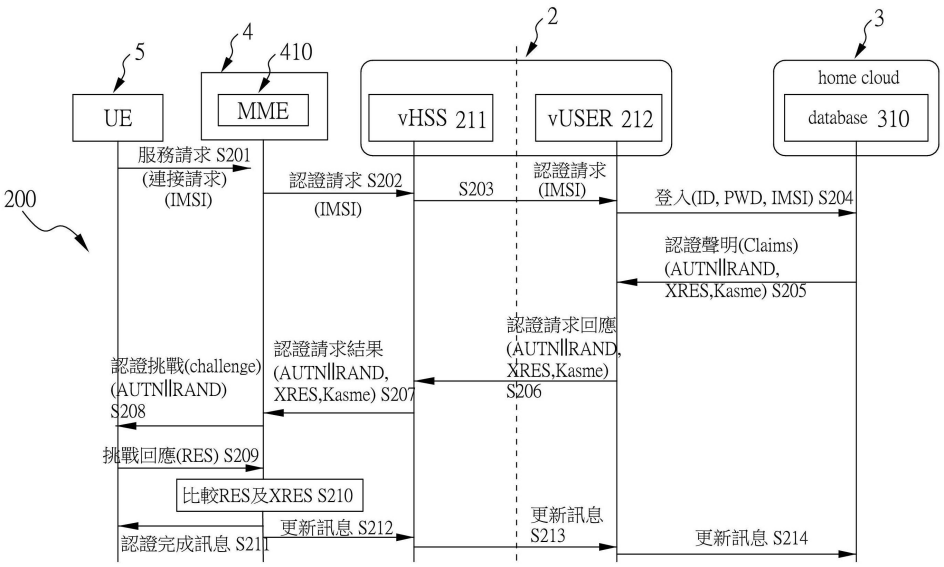

圖2(A)

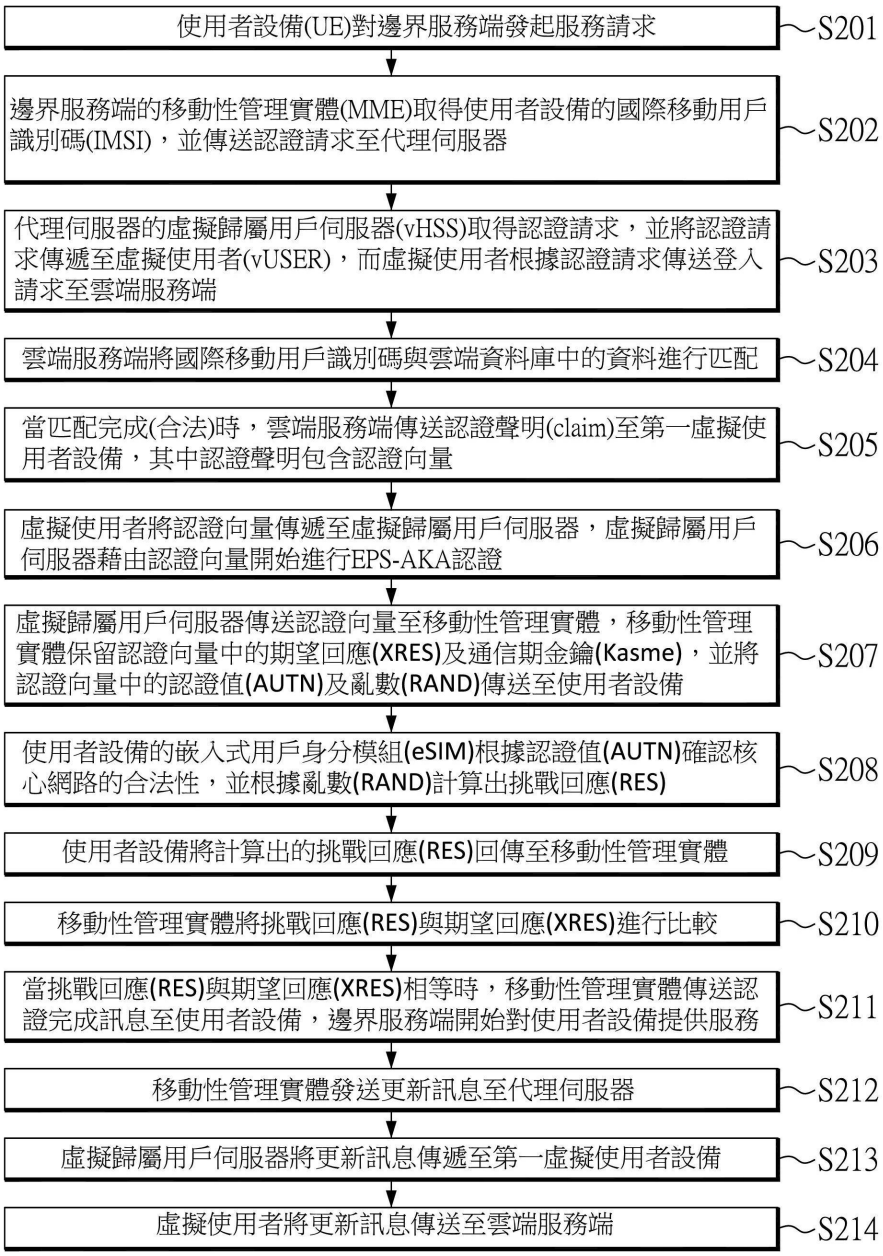
使用者設備(UE)對邊界服務端發起服務請求
S201
邊界服務端的移動性管理實體(MME)取得使用者設備的國際移動用戶識別碼(IMSI)，並傳送認證請求至代理伺服器
S202
代理伺服器的虛擬歸屬用戶伺服器(vHSS)取得認證請求，並將認證請求傳遞至虛擬使用者(vUSER)，而虛擬使用者根據認證請求傳送登入請求至雲端服務端
S203
雲端服務端將國際移動用戶識別碼與雲端資料庫中的資料進行匹配
S204
當匹配完成(合法)時，雲端服務端傳送認證聲明(claim)至第一虛擬使用者設備，其中認證聲明包含認證向量
S205
虛擬使用者將認證向量傳遞至虛擬歸屬用戶伺服器，虛擬歸屬用戶伺服器藉由認證向量開始進行EPS-AKA認證
S206
虛擬歸屬用戶伺服器傳送認證向量至移動性管理實體，移動性管理實體保留認證向量中的期望回應(XRES)及通信期金鑰(Kasme)，並將認證向量中的認證值(AUTN)及亂數(RAND)傳送至使用者設備
S207
使用者設備的嵌入式用戶身分模組(eSIM)根據認證值(AUTN)確認核心網路的合法性，並根據亂數(RAND)計算出挑戰回應(RES)
S208
使用者設備將計算出的挑戰回應(RES)回傳至移動性管理實體
S209
移動性管理實體將挑戰回應(RES)與期望回應(XRES)進行比較
S210
當挑戰回應(RES)與期望回應(XRES)相等時，移動性管理實體傳送認證完成訊息至使用者設備，邊界服務端開始對使用者設備提供服務
S211
移動性管理實體發送更新訊息至代理伺服器
S212
虛擬歸屬用戶伺服器將更新訊息傳遞至第一虛擬使用者設備
S213
虛擬使用者將更新訊息傳送至雲端服務端
S214

圖2(B)

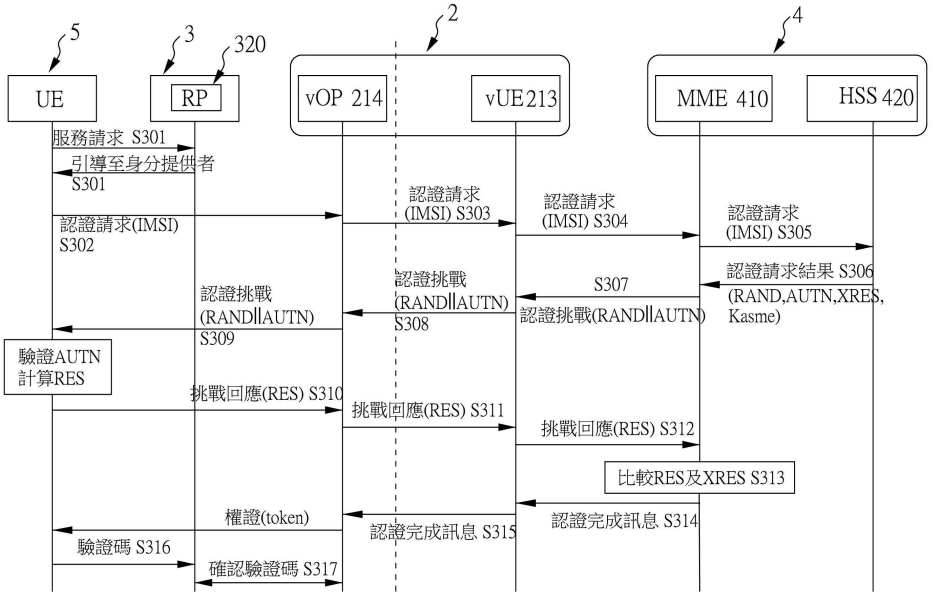
5
3
320
2
4
UE
RP
vOP 214
vUE213
MME 410
HSS 420
服務請求 S301
引導至身分提供者 S301
認證請求(IMSI) S302
認證請求 (IMSI) S303
認證請求 (IMSI) S304
認證請求 (IMSI) S305
認證請求結果 S306 (RAND,AUTN,XRES, Kasme)
S307
認證挑戰 (RAND||AUTN) S308
認證挑戰(RAND||AUTN)
認證挑戰 (RAND||AUTN) S309
驗證AUTN 計算RES
挑戰回應(RES) S310
挑戰回應(RES) S311
挑戰回應(RES) S312
比較RES及XRES S313
認證完成訊息 S314
認證完成訊息 S315
權證(token)
驗證碼 S316
確認驗證碼 S317

圖3(A)


使用者設備對雲端服務端發起服務請求
S301
使用者設備傳送認證請求至代理伺服器的虛擬開放式帳戶提供者(vOP)，其中認證請求包含國際移動用戶識別碼
S302
虛擬使用者設備自虛擬開放式帳戶提供者處取得認證請求
S303
虛擬使用者設備傳送認證請求至邊界服務端的移動性管理實體
S304
歸屬用戶伺服器(HSS)自移動性管理實體處取得國際移動用戶識別碼，並將國際移動用戶識別碼與資料庫中的用戶資料進行匹配
S305
當匹配完成(合法)時，歸屬用戶伺服器傳送認證請求結果至移動性管理實體，其中認證請求結果包含認證向量
S306
移動性管理實體保留認證向量的期望回應(XRES)，並傳送認證值(AUTN)及亂數(RAND)至代理伺服器的虛擬使用者設備
S307
虛擬開放式帳戶提供者自虛擬使用者設備處取得認證值(AUTN)及亂數(RAND)
S308
虛擬開放式帳戶提供者將認證值(AUTN)及亂數(RAND)傳送至使用者設備，使用者設備透過認證值(AUTN)確認核心網路已被認證，並透過亂數(RAND)計算出挑戰回應(RES)
S309
使用者設備回傳挑戰回應(RES)至虛擬開放式帳戶提供者
S310
虛擬使用者設備自虛擬開放式帳戶提供者處取得挑戰回應(RES)
S311
虛擬使用者設備將挑戰回應(RES)傳送至移動性管理實體
S312
移動性管理實體比較挑戰回應(RES)與期望回應(XRES)
S313
當兩者相等時，移動性管理實體將認證完成訊息傳送至虛擬使用者設備
S314
虛擬開放式帳戶提供者自虛擬使用者設備處取得認證完成訊息，並根據認證完成訊息傳送權證至使用者設備
S315
使用者設備根據權證傳送驗證碼至雲端服務端
S316
雲端服務端校驗驗證碼，並開始提供服務
S317

圖3(B)

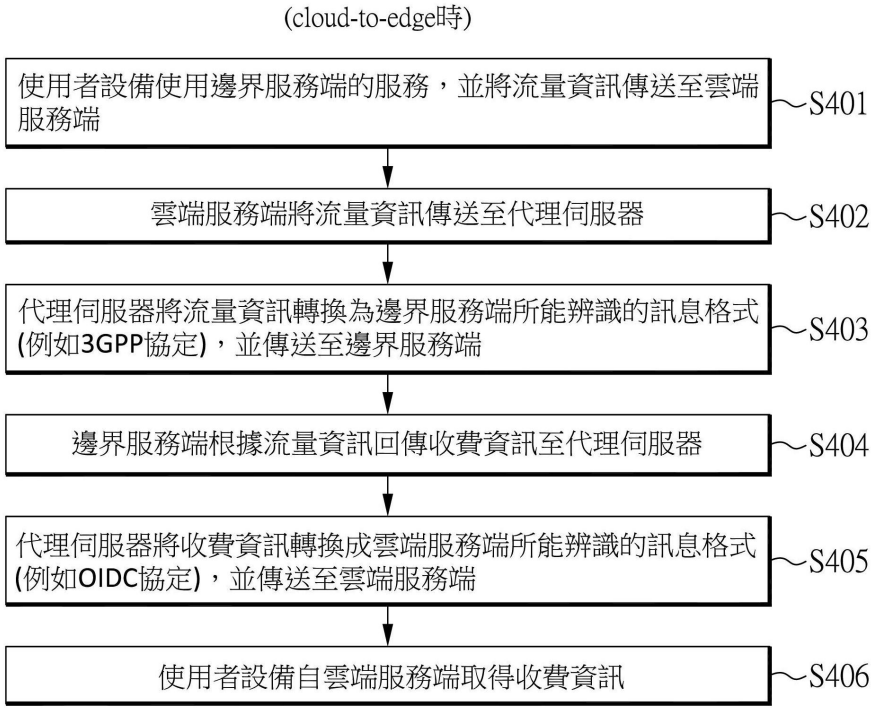
(cloud-to-edge時)
使用者設備使用邊界服務端的服務，並將流量資訊傳送至雲端服務端
S401
雲端服務端將流量資訊傳送至代理伺服器
S402
代理伺服器將流量資訊轉換為邊界服務端所能辨識的訊息格式(例如3GPP協定)，並傳送至邊界服務端
S403
邊界服務端根據流量資訊回傳收費資訊至代理伺服器
S404
代理伺服器將收費資訊轉換成雲端服務端所能辨識的訊息格式(例如OIDC協定)，並傳送至雲端服務端
S405
使用者設備自雲端服務端取得收費資訊
S406

圖4

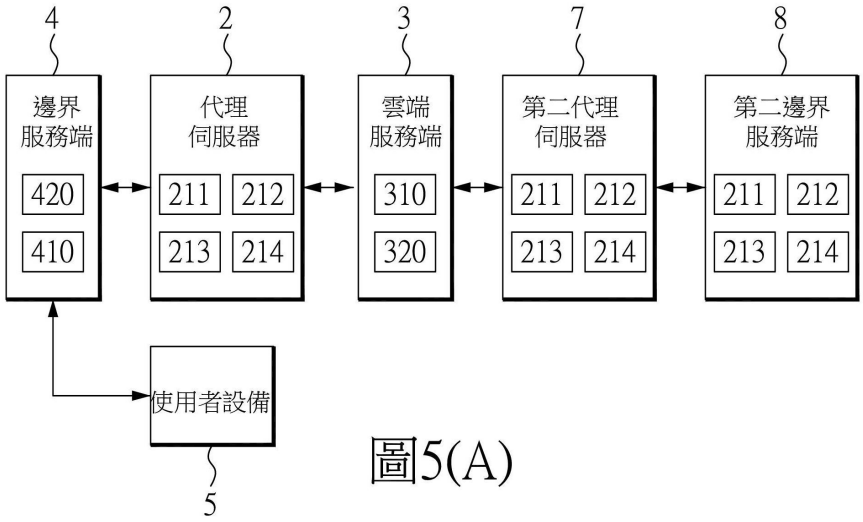
4
2
3
7
8
邊界服務端
420
410
代理伺服器
211
212
213
214
雲端服務端
310
320
第二代理伺服器
211
212
213
214
第二邊界服務端
211
212
213
214
使用者設備
5

圖5(A)

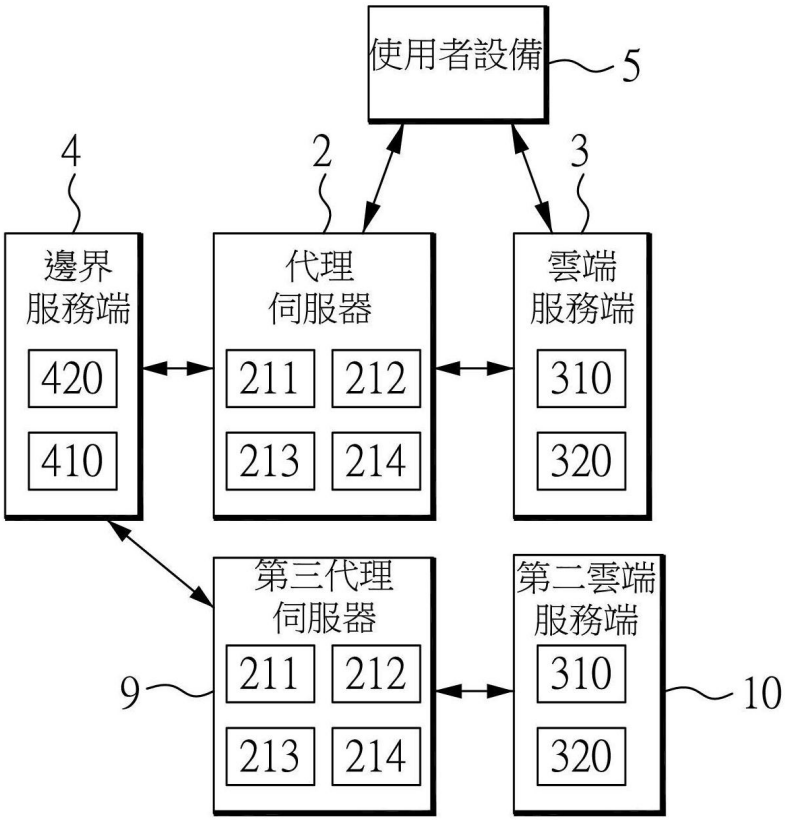
使用者設備
5
4
2
3
邊界
服務端
420
410
代理
伺服器
211
212
213
214
雲端
服務端
310
320
第三代理
伺服器
211
212
213
214
9
第二雲端
服務端
310
320
10

圖5(B)