

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013년 6월 13일 (13.06.2013)



(10) 국제공개번호
WO 2013/085281 A1

- (51) 국제특허분류:
G06F 21/20 (2006.01) *G06F 15/16* (2006.01)
H04L 9/32 (2006.01)
- (21) 국제출원번호: PCT/KR2012/010487
- (22) 국제출원일: 2012년 12월 5일 (05.12.2012)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2011-0129242 2011년 12월 5일 (05.12.2011) KR
- (71) 출원인: 인텔렉추얼디스커버리 주식회사 (IN-TELLCETUAL DISCOVERY CO., LTD.) [KR/KR];
135-090 서울시 강남구 삼성로 511, 10층, Seoul (KR).
- (72) 발명자: 허의남 (HUH, Eui Nam); 138-040 서울시 송파구 풍납동 388-7 우성아파트 2동 708호, Seoul (KR).
나상호 (NA, Sang Ho); 446-906 경기도 용인시 기흥구 서천동 1번지 전자정보대학 322호, Gyeonggi-do (KR).
박준영 (PARK, Jun Young); 446-906 경기도 용인시 기

흥구 서천동 1번지 전자정보대학 322호, Gyeonggi-do (KR). 김진택 (KIM, Jin Taek); 100-454 서울시 중구 신당4동 신당삼성아파트 113동 1404호, Seoul (KR).

(74) 대리인: 특허법인 무한 (MUHANN PATENT & LAW FIRM); 135-814 서울시 강남구 논현동 51-8 명림빌딩 2, 5, 6층, Seoul (KR).

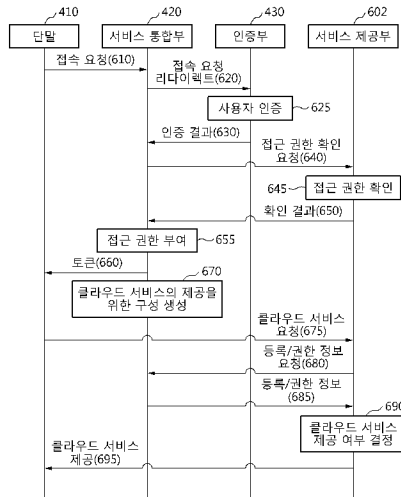
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG,

[다음 쪽 계속]

(54) Title: METHOD AND DEVICE FOR SECURITY IN CLOUDING COMPUTING SERVICE

(54) 발명의 명칭 : 클라우드 컴퓨팅 서비스에서의 보안을 위한 방법 및 장치



(57) Abstract: The present invention relates to a method and device for security in a clouding computing service. A service integrating unit provides various cloud services to a terminal through a virtual private network. An authenticating unit performs authentication on a user of the terminal through redirection at the integrating unit. The service integrating unit creates a virtual machine that provides a cloud service requested by the terminal onto a service providing unit. The service providing unit provides a cloud service to a terminal authenticated by the authenticating unit.

(57) 요약서: 클라우드 컴퓨팅 서비스에서의 보안을 위한 방법 및 장치가 제공된다. 서비스 통합부는 가상 개인 네트워크를 통해 다양한 클라우드 서비스들을 단말에게 제공한다. 인증부는 서비스 통합부에서의 리다이렉션을 통해 단말의 사용자에게 인증을 수행한다. 서비스 통합부는 서비스 제공부 상에 단말이 요청한 클라우드 서비스를 제공하는 가상 머신을 생성한다. 서비스 제공부는 인증부에 의해 인증된 단말에게 클라우드 서비스를 제공한다.

- 410 ... Terminal
420 ... Service integrating unit
430 ... Authenticating unit
602 ... Service providing unit
610 ... Connection request
620 ... Connection request redirection
625 ... Authenticate a user
630 ... Authenticated result
640 ... Access authorization verifying request
645 ... Verified result
655 ... Provide the access authorization
670 ... Create a configuration for providing a cloud service
675 ... Cloud service request
680 ... Registration/authorization information request
685 ... Registration/authorization information
690 ... Determine whether to provide the cloud service
695 ... Provide the cloud service

WO 2013/085281 A1



ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, **공개:**

TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 클라우딩 컴퓨팅 서비스에서의 보안을 위한 방법 및 장치

기술분야

- [1] 아래의 실시예들은 클라우드 컴퓨팅 서비스에서의 보안에 관한 것으로, 더욱 상세하게는 클라우드 컴퓨팅 보안 요소(element)를 통해 퍼스널 클라우드 서비스를 제공하는 보안 방법, 장치 및 시스템에 관한 것이다.

배경기술

- [2]클라우드 컴퓨팅은 가상화(visualization) 기술 및 분산 처리(distributed processing) 기술을 활용함으로써 대규모의 IT 자원을 제공하는 기술이다. 클라우드 컴퓨팅 서비스에 의해 사용자는 인터넷을 통해 컴퓨팅 자원에 대한 서비스를 제공받을 수 있다. 여기서, 컴퓨팅 자원은 메모리(memory) 자원, 중앙 처리 장치(Central Processing Unit; CPU) 자원, 네트워크 자원 및 스토리지(storage) 자원 등을 포함할 수 있다. 사용자는 자신이 사용한 컴퓨팅 자원에 상응하는 요금을 클라우드 컴퓨팅 서비스의 운영 주체에게 지불할 수 있다.
- [3]말하자면, 클라우드 컴퓨팅은 서로 상이한 물리적인 위치에 존재하는 컴퓨팅 자원들을 가상화 기술을 통해 하나의 컴퓨팅 자원으로 통합하고, 통합된 컴퓨팅 자원을 사용자들에게 제공하는 기술이다. 즉, 클라우딩 컴퓨팅은 '인터넷에 기반한 사용자 중심의 주문형 아웃소싱 서비스 기술'로 간주될 수 있다.
- [4]인터넷이 제공된다면, 사용자는 클라우드 컴퓨팅 서비스를 통해 자신만의 컴퓨팅 환경을 시간 및 장소에 무관하게 사용할 수 있다. 클라우딩 컴퓨팅 서비스는 사용자에게 상기의 사용자가 사용한 자원만큼의 요금을 부과한다. 또한, 사용자는 클라우드 컴퓨팅 서비스의 컴퓨팅 환경을 통해, 하드웨어 서비스, 소프트웨어 서비스 및 사후 서비스 등과 같은 모든 서비스를 제공받을 수 있다. 따라서, 시스템의 유지 및 보수 비용이 절감될 수 있고, 하드웨어 및 소프트웨어의 구매 비용이 절감될 수 있고, 컴퓨팅 처리를 위해 사용되는 에너지가 절감될 수 있다.
- [5]클라우드 컴퓨팅 서비스가 주목을 받음에 따라, IT 대기업들의 주도 하에 클라우드 컴퓨팅 서비스가 널리 보급되고 있다. 클라우드 컴퓨팅 서비스에 있어서, 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud) 등과 같은 4가지의 클라우드 컴퓨팅 서비스 타입이 존재한다.
- [6]퍼블릭 클라우드 서비스는 불특정된 다수의 사용자들에게 인터넷을 통해 클라우드 서비스를 제공한다. 퍼블릭 클라우드 서비스는 무상의 서비스 제공을 의미하는 것은 아니며, 서비스에 관련된 데이터 및 소스의 공개(open)을 의미하는 것 또한 아니다. 퍼블릭 클라우드 서비스에서도, 사용자 접근

제어(access control) 및 과금 등과 같은 서비스가 제공될 수 있다. 퍼블릭 클라우드 서비스 하에서는, 서비스의 제공자가 사용자의 정보를 관리하고, 모든 클라우드 컴퓨팅 서비스의 리소스들이 공유된다. 따라서, 퍼블릭 클라우드 서비스는 사용자의 개인 정보의 보호에 있어서, 취약점을 갖는다.

- [7] 프라이빗 클라우드 서비스는 퍼블릭 클라우드 서비스에서와 같은 컴퓨팅 환경을 제공한다. 프라이빗 클라우드 서비스는 특정한 기업 또는 기관에서 클라우드 컴퓨팅 서비스, 데이터 및 프로세스를 직접 관리하는 클라우드 서비스를 의미한다. 말하자면, 프라이빗 클라우드 서비스는 보안을 위해서 외부로부터의 접근을 회피하고, 인증된 사용자들만의 접근을 허용하는 폐쇄적인 클라우드 서비스 타입이다.
- [8] 커뮤니케이션 클라우드 서비스는 특정한 사용자들의 집단을 위한 클라우드 컴퓨팅 서비스이다. 커뮤니케이션 클라우드 서비스는 특정한 집단의 구성원들에게만 접근 권한을 부여한다. 집단의 구성원들은 커뮤니케이션 클라우드 서비스를 통해 서로 간에 데이터 및 어플리케이션 등을 공유한다.
- [9] 하이브리드 클라우드 서비스는 퍼블릭 클라우드 서비스 및 프라이빗 클라우드 서비스가 결합된 서비스이다. 하이브리드 클라우드 서비스는 기본적으로 퍼블릭 클라우드 서비스를 제공하며 사용자가 공유를 원치 않는 데이터 및 서비스에 대해서는 프라이빗 클라우드 서비스의 정책을 따른다.
- [10] 클라우드 컴퓨팅 서비스의 구조는 인프라형 서비스 구조, 플랫폼형 서비스 구조 및 소프트웨어 서비스 구조로 분류될 수 있다. 인프라형 서비스 구조는 사용자의 요구에 맞춰 사용자만의 컴퓨팅 환경을 제공한다. 플랫폼형 서비스 구조는 사용자의 컴퓨팅 목적에 맞게 사용자가 플랫폼을 선택하고, 선택된 플랫폼을 사용할 수 있는 환경을 제공한다. 소프트웨어 서비스 구조는 사용자가 사용 목적에 맞는 소프트웨어를 선택하여 사용할 수 있는 환경을 제공한다.
- [11] 클라우드 컴퓨팅 서비스를 위해, 강력하고 체계적인 접근 제어 및 권한 부여 정책이 요구된다. 퍼스널 클라우드 서비스는 서로 상이한 서비스 제공자들 간의 협업을 통해 클라우드 서비스를 제공한다. 따라서, 퍼스널 클라우드 서비스의 특징에 맞는 강력하고 체계적인 보안 시스템 또는 보안 인프라가 요구된다.
- [12] 클라우드 컴퓨팅 서비스의 모델은 클라우드 서비스 제공자가 단일하다는 것을 가정할 수 있다. 그러나, 다양한 사업자들 간의 협업을 통해 다양한 클라우드 서비스들이 조합된 새로운 사용자 주문형 클라우드 서비스가 대두할 것으로 기대될 수 있다.
- [13] 일반적으로, 인터넷은 호스트-클라이언트 구조를 갖는다. 말하자면, 사용자의 단말은 인터넷을 통해 서버에 접속하며, 단말은 인터넷을 통해 서버로부터 서비스를 제공받는다. 상기의 구조에 있어서, 신뢰될 수 있는 부분 및 신뢰될 수 없는 부분으로 구분되는 보안 경계가 존재한다. 사용자 로컬에 존재하는 컴퓨터, 스토리지, 방화벽 등처럼 사용자가 직접 관리 및 제어가 가능한 영역은 신뢰할 수 있는 부분이며, 네트워크, 서버, 웹스토리지와 같이 사용자가 직접 볼 수 없고

제어가 불가능한 영역은 신뢰할 수 없는 부분으로 구분된다.

- [14] 아웃소싱이 이루어지는 클라우드 컴퓨팅 환경에서는, 클라우드 서비스의 제공을 위한 클라우드 컴퓨팅 구성 요소들 간의 보안 경계가 불분명해진다. 클라우드 컴퓨팅 구성 요소들은 단말 및 클라우드 서비스의 제공자를 포함할 수 있다. 특히, 다중의 클라우드 서비스 제공자들 간의 협업에 기반하는 클라우드 서비스가 제공되기 위해서는, 클라우드 서비스의 사용자의 정보가 서비스 제공자들 간에서 전달, 가공 및 처리되어야 한다.
- [15] 사용자 중심의 주문형 아웃소싱 컴퓨팅 서비스에 있어서, 사용자 인증, 이용 요금 청구 및 사용자의 서비스 성향 등에 대한 사용자 정보의 보호가 요구된다. 말하자면, 협업에 기반하는 클라우드 컴퓨팅 서비스 환경을 고려하는 사용자 중심의 주문형 컴퓨팅 서비스만의 새로운 보안 서비스와 시스템이 요구된다.
- [16] 기업을 위한 클라우드 컴퓨팅뿐만 아니라 개인화된 퍼스널 클라우드 컴퓨팅 제공을 위한 다양한 서비스가 준비된다는 점을 고려하였을 때, 클라우드 서비스들 간에서 사용자의 정보가 안전하게 전달될 수 있는 클라우드 보안 시스템 및 방법이 요구된다. 사용자의 정보는 개인 정보 및 서비스 관련 정보를 포함할 수 있다. 말하자면, 클라우드 컴퓨팅이 발전함에 따라, 클라우드 컴퓨팅의 신뢰성, 보안성, 법적 쟁점, 개인 정보 보호 및 표준화 등 제반 문제에 대한 해결이 요구된다.

발명의 상세한 설명

기술적 과제

- [17] 일 실시예는 클라우드 컴퓨팅 환경을 제공하기 위한 강력하고 체계적인 보안 시스템 및 보안 방법을 제공할 수 있다.
- [18] 일 실시예는 가상화 환경을 제공하기 위해 가상 머신, 가상 자원 공유 및 가상 네트워크를 고려하는 보안 시스템 및 보안 방법을 제공할 수 있다.
- [19] 일 실시예는 클라우드 컴퓨팅의 특징인 가상화, 분산 컴퓨팅 및 협업 서비스 모델을 고려하는 클라우드 환경에 적합한 보안 시스템 및 보안 방법을 제공할 수 있다.

과제 해결 수단

- [20] 일 측에 따르면, 사용자의 단말로부터 클라우드 서비스로의 접속의 요청을 수신하는 단계, 상기 사용자의 상기 클라우드 서비스에 대한 접근 권한의 확인을 상기 클라우드 서비스를 제공하는 서비스 제공부에게 요청하는 단계, 상기 서비스 제공부로부터 상기 확인의 결과를 수신하는 단계 및 상기 결과가 상기 사용자가 상기 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우 상기 사용자의 토큰에 상기 클라우드 서비스에 대한 접근 권한을 부여하는 단계를 포함하는, 클라우드 서비스 방법이 제공될 수 있다.
- [21] 상기 클라우드 서비스 방법은, 상기 단말의 식별자를 인증부로 전송하는 단계 및 상기 인증부로부터 상기 식별자에 기반한 상기 사용자에 대한 인증의 결과를

수신하는 단계를 더 포함할 수 있다.

[22] 상기 클라우드 서비스 방법은, 상기 사용자의 토큰을 상기 단말로 전송하는 단계를 더 포함할 수 있다.

[23] 상기 클라우드 서비스 방법은, 상기 서비스 제공부로부터 상기 클라우드 서비스의 등록 정보 및 상기 사용자의 권한 정보의 요청을 수신하는 단계 및 상기 서비스 제공부로 상기 등록 정보 및 상기 권한 정보를 전송하는 단계를 더 포함할 수 있다.

[24] 상기 클라우드 서비스 방법은, 상기 서비스 제공부 상에 상기 클라우드 서비스를 제공하기 위한 구성을 생성하는 단계를 더 포함할 수 있다.

[25] 상기 클라우드 서비스를 제공하기 위한 상기 구성은 상기 서비스 제공부 상에서 수행되는 가상 머신일 수 있다.

[26] 상기 클라우드 서비스는 가상 네트워크를 통해 상기 서비스 제공부에 의해 상기 단말에게 제공될 수 있다.

[27] 상기 클라우드 서비스는 복수 개일 수 있다.

[28] 상기 접근 권한은 상기 서비스 제공부의 상기 클라우드 서비스에 대한 정책에 기반하여 상기 토큰에게 부여될 수 있다.

[29] 다른 일 측에 따르면, 사용자의 단말로부터 클라우드 서비스로의 접속의 요청을 수신하고, 상기 사용자의 상기 클라우드 서비스에 대한 접근 권한의 확인을 상기 클라우드 서비스를 제공하는 서비스 제공부에게 요청하고, 상기 서비스 제공부로부터 상기 확인의 결과를 수신하고, 상기 결과가 상기 사용자가 상기 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우 상기 사용자의 토큰에 상기 클라우드 서비스에 대한 접근 권한을 부여하는 접근 제어부 및 상기 서비스 제공부 상에 상기 클라우드 서비스를 제공하기 위한 구성을 생성하는 서비스 구성부를 포함하는, 클라우드 서비스 통합 서버가 제공될 수 있다.

[30] 상기 접근 제어부는 상기 단말의 식별자를 인증부로 전송할 수 있고, 상기 인증부로부터 상기 식별자에 기반한 상기 사용자에 대한 인증의 결과를 수신할 수 있다.

[31] 상기 접근 제어부는 상기 사용자의 토큰을 상기 단말로 전송할 수 있다.

[32] 상기 접근 제어부는 상기 서비스 제공부로부터 상기 클라우드 서비스의 등록 정보 및 상기 사용자의 권한 정보의 요청을 수신할 수 있고, 상기 서비스 제공부로 상기 등록 정보 및 상기 권한 정보를 전송할 수 있다.

발명의 효과

[33] 퍼스널 클라우드 서비스의 특징에 맞는 접근 제어 방법, 권한 위임 및 권한 부여 정책을 사용하는 보안 시스템 및 보안 방법이 제공된다.

도면의 간단한 설명

[34] 도 1은 CSA 클라우드의 15 개의 보안 도메인들을 도시한다.

- [35] 도 2는 클라우드 서비스 모델을 설명한다.
- [36] 도 3는 클라우드 서비스에 대한 보안 위협을 설명한다.
- [37] 도 4는 일 실시예에 따른 클라우드 컴퓨팅 서비스 시스템이다.
- [38] 도 5는 일 실시예에 따른 서비스 통합부의 구조도이다.
- [39] 도 6은 일 실시예에 따른 클라우드 서비스 방법의 흐름도이다.
- [40] 도 7은 일 실시예에 따른 클라우드 컴퓨팅 서비스 시스템이다.
- [41] 도 8은 일 실시예에 따른 사용자가 ISP에 회원으로서 가입하는 절차를 도시한다.
- [42] 도 9는 일 실시예에 따른 MCSP의 구조도이다.
- [43] 도 10은 일 실시예에 따른 사용자의 개인 정보 위임 및 로그인 과정을 설명한다.
- [44] 도 11은 일 실시예에 따른 사용자 서비스 구성 과정을 설명한다.
- [45] 도 12는 일 실시예에 따른 MCSP 회원 가입 및 MCSP 이용 절차를 설명한다.

발명의 실시를 위한 형태

- [46] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [47] 이하에서, 용어 "유일 자원 지시기(Uniform Resource Locator; URL)" 및 "통합 자원 식별자(Uniform Resource Identifier; URI)"는 동일한 의미로 사용되며, 상호 대체될 수 있다.
- [48] 하기에서, 실시예에 결합될 수 있는 다양한 클라우드 컴퓨팅 서비스의 보안 방법들이 설명된다.
- [49] 아마존의 일래스틱 컴퓨트 클라우드(Elastic Compute Cloud; EC2)의 보안
- [50] 아마존의 EC2는 사용자 클라이언트가 원하는 서비스를 위한 가상 머신 (Virtual Machine; VM)을 제공하는 인프라형 서비스(Infrastructure as a Service; IaaS) 클라우드일 수 있다.. 클라이언트 소프트웨어는 가상 머신 내에 존재할 수 있다. 따라서, 아마존은 인프라 서비스를 제외한 가상 머신 안에서 실행되는 서비스에 대한 책임을 갖지 않을 수 있다.
- [51] 아마존은 일회성(one-time) 토큰(token) 장치와 같은 강력한 보안 장치를 제공할 수 있다. 일반적으로 일회성 토큰 장치와 같은 보안 장치를 사용하는 기업들은 모니터링 및 관리 톨을 사용할 수 있다. 모니터링 및 관리 톨은 통합 식별자(identifier; ID)관리, 액티브 트래킹(active tracking) 및 인증(authentication) 시스템의 원격 제어 등의 기능을 제공할 수 있다. 사용된 토큰의 폐지 방법은 보안 문제에 있어서의 핵심일 수 있다.
- [52] 일반적으로, 보안 서비스는 아마존이 소유하는 인프라 내에서만 제공될 수 있다. 따라서, EC2 클라이언트는 전적으로 가상 서버 내부의 데이터 및 프로그램의 보호에 대한 책임을 질 수 있다. 그러나, 데이터 및 소프트웨어는 서비스 내부에서 암호화 되어야 하기 때문에 보안 정책의 수정이 매우 어려울 수 있다.

[53] 구글의 앱 엔진(App Engine) 보안

[54] 구글에서 제공하는 코드 배치 문서(code deployment documentation) 내에는 앱 엔진의 보안 서비스에 대한 내용이 기술되어 있다. 서비스에 대한 보안을 위해, 보안 관련 정보는 서비스가 앱 엔진에 로드(load)될 때 사용된 XML 구성 파일(XML configuration file) 내에 상세하게 기술될 수 있다. 상술된 것과 같은 앱 엔진 보안 솔루션의 문제점은 오직 구글 계정 서비스와 연계된 인증 서비스만을 제공할 수 있다는 것일 수 있다. 구글 계정은 간단한 사용자 명칭 및 패스워드를 사용한 인증 방식을 사용하기 때문에 보안에 있어서 매우 취약할 수 있다.

[55] 또한, 앱 엔진의 보안 서비스는 오직 앱 엔진에 의해 제공되는 서비스 단위로만 수행될 수 있다. 서비스 기능 중 선택된 요소 별 클라이언트 접근 제어 방식은 명확하지 못한 보안 서비스 구조를 가질 수 있다. 앱 엔진 서비스를 통해 제공되는 자원들에 대해서는 서비스가 자체적으로 보안을 보장해야 할 수 있다. 그러나, 서비스 자원에 대한 보안에 대하여 명시된 내용은 없을 수 있다.

[56] 마이크로 소프트(Microsoft; MS)의 애저(Azure) 보안

[57] 애저가 제공하는 보안 서비스는 다른 클라우드의 보안 서비스에 비해 상대적으로 뛰어난 것으로 간주될 수 있다. 클라우드 서비스의 클라이언트 또는 제공자는 플랫폼 형 서비스(Platform as a Service; PasS)인 애저를 이용함으로써 서비스의 생성, 제공 및 관리를 할 수 있다. 서비스의 생성, 제공 및 관리를 위해, 애저는 보안 행사 마크업 언어(Secure Assertions Markup Language; SAMP)에 기반하는 보안 메커니즘을 제공할 수 있다. SAMP는 클라우드 서비스의 제공자가 서비스의 이용자들에 대한 접근 제어를 할 수 있게 할 수 있다.

[58] 클라이언트 또는 서비스 요청자는 서비스 접근의 요청 시 자신에 대한 인증을 가능하게 하는 자격 증명을 제시할 수 있다. 제시된 자격 증명은 신원 제공자(Identity Provider, IP)에 의해 발급된 것일 수 있다. 자격 증명은 신원 제공자에 의해 서명될 수 있다. 상기의 서명을 통해 클라이언트 또는 서비스 요청자가 인증될 수 있다. 서로 상이한 신원 제공자들의 자격 증명들 간의 호환성을 위해, 애저는 자격 증명 변환 서비스를 제공할 수 있다. 애저를 이용하기 위해, 클라이언트 또는 서비스 요청자는 우선적으로 자격 증명에 대한 인증 과정을 거칠 수 있다. 전술된 인증 과정을 통해, 인증된 사용자 요청만이 처리될 수 있다. 애저의 보안 시스템에서, 자격 증명 확인 프로세스는 단점으로 지적될 수 있다. 애저 서비스는 애저의 접근 제어 서비스로의 요청 기능 및 자격 증명 확인 기능을 구현할 수 있다. 따라서, 애저에 의해 보안 서비스가 제공되지만, 애저 서비스의 개발자가 수동으로 보안 정책을 결정해야 할 수 있다.

[59] 하기에서, 실시예에 결합될 수 있는 보안 솔루션의 이슈들이 설명된다.

[60] 리소스 보호

[61] 클라우드의 리소스는 클라우드 서비스를 통해서만 제공될 수 있다. 따라서, 리소스 보안이 필수적으로 요구될 수 있고, 리소스 보안을 위한 최적의 솔루션이

요구될 수 있다. 클라이언트가 클라우드 서비스에 접속할 때에는 리소스 보안이 보장된 후에 서비스가 실행될 수 있다.

[62] 리소스 보호는 하기의 방법들을 통해 구현될 수 있다.

[63] 1) 재량(discretionary) 시스템 : 클라우드 서비스 제공자에 의해 클라이언트의 리소스 접근 권한에 대한 승인 또는 거부가 이루어질 수 있다. 재량 시스템의 가장 큰 취약점은 저장된 데이터와 관련된 클라이언트 인증의 의미를 고려하지 않는 것일 수 있다.

[64] 2) 비-재량(non-discretionary) 시스템 : 리소스 접근 권한에 대한 승인 또는 거부는 클라이언트에 의한 분류 및 인증에 기반하여 이루어질 수 있다. 분류는 데이터 또는 어플리케이션에 대한 분류일 수 있다.

[65] 접근 제어 매트릭스(Access Control Matrix; ACM)

[66] ACM은 보안 접근법들 중 가장 일반적으로 사용되는 하나일 수 있다. ACM은 매트릭스를 사용하기 때문에 쉽게 접근 권한 승인, 폐지 및 결정을 할 수 있다. 그러나, ACM은 집중화된 분산 컴퓨팅 환경에서는 원활하게 작동하지 못할 수 있다. 접근 제어 매트릭스는 접근제어 목록(Access Control Lists; ACL)를 나타내는 행 및 자격인증(capabilities)을 나타내는 열로 구성될 수 있다. 시스템의 각 리소스는 서비스 목록을 가질 수 있다. 서비스 목록은 서비스들 각각 및 서비스들 각각의 실행 권한을 가질 수 있다. ACL은 리소스들 전체에 적용될 수 있다. 따라서, ACL의 프로세스 분류는 세부적이지 않을 수 있는 반면, ACL의 권한 관리는 용이하게 이루어질 수 있다. 반면, 자격인증을 이용하는 보안 시스템은 클라이언트 또는 클라이언트에 할당된 서비스에 권한을 할당할 수 있다. 일반적으로, 사용자 자격인증은 리소스 및 리소스에 대한 권한을 정의할 수 있다. 자격인증 및 ACL은 각각의 장점 및 단점에 있어서 상호 보완 관계를 가질 수 있다.

[67] 속성 기반 접근 제어(Attribute Based Access Control; ABAC)

[68] 또 다른 보안 모델은 ABAC이다. ABAC 및 ACM은 1) 서비스 및 리소스에 할당된 속성과 2) 정책을 통한 권리 부여 방식에 있어서 서로 상이할 수 있다. 서비스에게는 명칭(name) 및 역할(role) 등과 같은 속성이 할당될 수 있다. 리소스에게는 소유자 및 도메인이 할당될 수 있다. 서비스의 특정 기능은 정책 규칙(policy rule)을 만족시키는 범위 내에서 수행될 수 있다. 정책 규칙을 만족시키는 범위는 서비스의 각 속성 및 리소스의 각 속성을 서로 간에 비교함으로써 판별될 수 있다. ABAC에서는 속성의 사용에 따라 속성 증명에 대한 이슈가 있을 수 있다.

[69] 정보 흐름 제어(information flow control)

[70] 접근 권한은 저장된 기밀 데이터 및 사용자 승인에 따라서 권한 부여가 될 수 있다. 권한 부여에 있어서, 기능의 확장 및 ACL의 수정이 가능한 모델이 제안될 수 있다. 승인 기능(clearance capability)은 데이터 보호를 위한 추가적 기능을 포함한 신뢰하는 식별자일 수 있다. 승인 기능에는 특정 클래스의 정보 접근에

대한 클라이언트 승인을 제공하기 위한 보안 단계가 포함될 수 있다.

- [71] 승인 기능이 획득된 후에는 하기와 같은 다음과 같은 비교 절차가 수행될 수 있다. 첫 번째로, 승인 필드의 내용 및 요청된 자원의 분류가 비교될 수 있다. 승인 필드의 내용이 요청된 자원의 분류에 대응한다면, 보안 상태는 "안전(secure)"한 것으로 판별될 수 있다. 그렇지 않으면, 클라이언트가 요청한 접근은 거부될 수 있다. 보안 상태가 "안전(secure)"한 경우, 접근 권한 필드(access rights field) 및 요청된 작업이 비교될 수 있다. 접근 권한 필드가 요청된 작업에 대응할 경우, 클라이언트는 요청된 자원에 접근할 수 있다.

- [72] 하기에서, 실시예에 결합될 수 있는 통신 및 스토리지 보안 이슈에 대해 설명된다.

[73] 암호화의 비용

- [74] 클라우드 내부의 자원은 단순한 정보 저장에서부터 완벽한 비즈니스 워크플로우까지 변화할 수 있다. 공유된 환경에서의 데이터 보안은 모든 클라이언트를 식별해야 하기 때문에 복잡할 수 있다. 또한, 저장된 데이터의 보호를 위해 암호화가 제공될 수 있지만, 암호화된 데이터가 사용될 때마다 높은 비용이 발생할 수 있다.

[75] 데이터 통신의 안전성

- [76] 클라우드의 내부에서의 데이터 보안이 완벽하더라도, 클라이언트 및 클라우드 간의 통신과 클라우드 및 특정한 데이터 서비스 간의 통신은 반드시 보호되어야 할 수 있다. 또한, 데이터의 전송 동안, 기밀성 및 데이터 무결성은 반드시 보장되어야 할 수 있다. 전송 계층 보안(Transport Layer Security; TLS), 전송 계층 보안 프로세서, 보안 소켓 계층(Secure Sockets Layer; SSL) 및 HTTPS는 암호화 프로토콜로써 인터넷 또는 클라우드에 직접적으로 연결되는 네트워크의 통신 보안을 제공할 수 있다. 암호화 시스템은 대칭 암호화 방식 또는 비대칭 암호화 방식을 사용할 수 있다. 대칭 암호화 방식은 간단한 구조를 가질 수 있으나, 키 관리에 있어서 약점을 가질 수 있다. 비대칭 암호화 방식은 대칭 암호화 방식의 약점을 보완하여 데이터의 암호화 및 복호화에 있어서 각각 다른 키를 사용할 수 있다.

[77] 비대칭 암호화(Asymmetric Key Cryptosystem; AKC)

- [78] AKC는 개인 키(private key) 및 공개 키(public key)라는 두 개의 키들을 사용할 수 있다. 공개 키 또는 개인 키 중 하나의 키를 이용하여 데이터가 비대칭으로 암호화된 경우, 나머지 키가 데이터의 복호화에 사용될 수 있다. 비대칭 암호화에서, 두 개의 키들은 단방향성(One-way) 특성을 가질 수 있다. 공개 키는 누구에게나 공개되어 있을 수 있다. 따라서, 비대칭 암호화는 중간 공격자(Man In The Middle Attack; MITMA)에 취약할 수 있다. 비대칭 암호화가 MITMA에 취약하다는 문제는 자격 증명(CA, Certificate Authority)에 의해 해결될 수 있다.

[79] 인증(Authentication)

- [80] 클라우드에서 서비스, 서비스 공급자 및 클라우드 클라이언트의 인증은

필수적으로 요구될 수 있다. ID 및 패스워드(password)를 사용하는 단일-팩터 인증은 안전한 인증을 제공하기에는 충분하지 않을 수 있다. 따라서, 이중 인증이 제안될 수 있다. 이중 인증은 3 개의 제시된 인증 수단들 중 2 개의 인증 수단들 이용함으로써 클라이언트 인증을 수행하는 것일 수 있다. 예컨대, 3 개의 인증 수단들은 패스워드와 같은 "사용자가 아는 것(something you know)", 토큰 또는 스마트카드와 같은 "사용자가 가진 것(something you have)" 및 지문(fingerprint)과 같은 "사용자인 것(something you are)"일 수 있다. 상호 인증이 요구되는 경우 이중 인증의 구현은 어려울 수 있다. 상호 인증을 위해, 클라이언트는 클라우드 서비스에 대한 인증을 해야 할 수 있다. 또한, 워크플로우 상의 클라우드 서비스들은 서로에 대한 상호 인증을 해야 할 수 있다. 이러한 인증의 필요에 따라, 전자 서명과 같은 강력한 암호화 기반 인증이 요구될 수 있다. 메시지는 해쉬(hash) 함수에 의해 해쉬 값으로 변환될 수 있다. 해쉬 값에 개인 키를 적용함으로써 전자 서명이 생성될 수 있다. 전자 서명은 원본 메시지와 함께 전송될 수 있다. 메시지를 수신한 수신자는 원본 메시지를 제1 해쉬 값으로 변환할 수 있다. 또한, 수신자는 공개 키를 사용하여 전자 서명을 복호화함으로써 제2 해쉬 값을 생성할 수 있다. 수신자는 제1 해쉬 값 및 제2 해쉬 값을 비교할 수 있고, 제1 해쉬 값 및 제2 해쉬 값이 일치할 경우 원본 메시지가 변조되지 않은 것임을 확인할 수 있다.

[81] 커베로스(Kerberos)

[82] 커베로스는 사용자 ID 및 패스워드의 전송 없이 사용자를 인증할 수 있다. 커베로스는 비대칭 암호화 방식을 사용할 수 있다. 티켓(ticket)은 강력하게 암호화되고, 전자 서명된 토큰이다. 원격 도메인로부터의 서비스 접근에 대한 인증은 커베로스들 간의 키 공유를 통하여 수행될 수 있다. 커베로스는 매우 강력하고 안전한 인프라 환경을 제공할 수 있다. 커베로스는 분산 컴퓨팅 환경에서도 제공될 수 있다. 따라서, 커베로스는 클라우드 환경에서도 적용될 수 있다.

[83] 클라우드 컴퓨팅 보안 구조(cloud computing security architecture)

[84] 상술된 것과 같이, 클라이언트에게 제공되는 클라우드 서비스는 다양한 보안 문제들을 내포할 수 있다. 클라우드에서의 보안 위협, 도메인 및 보안 제어 방안에 대해 클라우드 보안 연맹(Cloud Security Alliance; CSA)의 클라우드 보안 백서(White Paper)가 적용될 수 있다.

[85] 하기에서 상세히 설명될 도 1 내지 도 3은 클라우드 서비스 모델을 설명한다. 3 개의 클라우드 서비스 모델들이 존재할 수 있다. 상기의 3 개의 클라우드 서비스 모델들과 관련하여 15 개의 보안 도메인들(security domains) 및 7 개의 주요 위협들(top threats)이 있을 수 있다.. 또한, 위협들을 해결하기 위한 10 가지의 보안 컨트롤 모델들 및 관련된 표준 기술들로 구성된 클라우드 컴퓨팅의 보안 구조가 제공될 수 있다.

[86] 도 1은 CSA 클라우드의 15 개의 보안 도메인들을 도시한다.

- [87] 도 1에서, 제1 도메인부터 제15 도메인까지 15 개의 도메인들의 명칭들이 도시되었다.
- [88] 클라우드 보안의 범위가 상당히 넓은 반면, 명확한 표준이 정의 되지 않았기 때문에, 클라우드 보안 분야는 아직 미성숙한(*immature*) 것일 수 있다. 따라서, 비즈니스 리스크에 대한 이해 및 클라우드의 이점에 대한 검토가 이루어져야 한다. 예컨대, 특정한 데이터베이스 서비스는 유연한 인증 및 세부적인 보안을 지원하지 않을 수 있다.
- [89] 보안 도메인에 있어서, 하기와 같은 이슈들이 고려될 수 있다.
- [90] 보안 제어(*security controls*)
- [91] 보안 제어는 보안 위협 및 도메인과 관련하여 요구되는 보안 제어 방안에 대한 정의 및 보안 요구사항에 대해서 설명할 수 있다.
- [92] 자원 관리(*asset management*)
- [93] 자원 관리는 클라우드 인프라를 구성하는 하드웨어, 네트워크 및 소프트웨어 자산을 모두 관리할 필요가 있다. 소프트웨어 자산은 물리적인 소프트웨어 자산 또는 가상의 소프트웨어 자산일 수 있다. 자원 관리에 있어서, 감사 및 규정 준수를 위해 자산의 물리적 기반 또는 네트워크 기반에 접근할 수 있는 계정이 포함될 수 있다.
- [94] 암호화(*cryptography*), 키 및 인증서 관리(*key and certificate management*)
- [95] 보안 시스템은 암호화 키 및 자격증명의 관리를 위해 인프라를 요구할 수 있다. 또한, 보안 시스템은 정보 보호를 위해 표준 기반의 암호화 기능 및 서비스를 포함할 수 있다.
- [96] 데이터/스토리지 보안(*data /storage security*)
- [97] 데이터 보안에 있어서, 데이터는 암호화되어 저장될 수 있다. 또한, 몇몇의 클라우드 서비스 사용자는 자신의 데이터 보호를 위해 다른 사용자와 다른 개별적인 공간에 데이터를 저장하기를 원할 수 있다.
- [98] 종단점 보안(*end-point security*)
- [99] 사용자들은 클라우드 서비스에서 종단점(*Endpoint*) 보안을 제공해야 할 수 있다. 네트워크 프로토콜과 디바이스 종류에 따라 제한적인 종단점 보안을 제공될 수 있다.
- [100] 이벤트 감사 및 리포팅(*event auditing and reporting*)
- [101] 사용자는 클라우드에서 발생하는 이벤트, 특히 시스템 에러 및 보안에 대한 데이터에 접근할 수 있다.
- [102] 식별, 역할들, 접근 제어 및 속성(*identity, roles, access control and attributes*)
- [103] 클라우드 기반의 자원에 대한, 효과적인 접근 제어의 구현 및 보안 정책의 시행을 위해서는 식별, 역할들, 권한부여 및 속성이 정의될 필요가 있다. 권한 부여는 위임에 대응할 수 있다. 속성은 사용자 및 서비스에 따라 결정된 것일 수 있다.
- [104] 네트워크 보안 (*Network Security*)

- [105] 스위치, 라우터 및 패킷 단의 네트워크 트래픽에 대한 보호가 요구될 수 있다. 아이피 스택에 대한 보안도 요구될 수 있다.
- [106] 보안 정책(security policies)
- [107] 보안 정책에 있어서, 접근 제어, 자원 할당 및 일관성 있는 결정 등에 대한 정책이 정의 및 결정될 수 있다. 또한, 보안 정책의 수행이 요구될 수 있다. 정책의 정의는 서비스 수준 협약(Service Level Alliance; SLA) 및 라이선스에 따라 자동적으로 수행될 수 있다.
- [108] 서비스 자동화 (Service Automation)
- [109] 보안 감사의 보안 제어 흐름은 자동화될 수 있다. 또한, 프로세스의 관리 및 분석은 자동화될 수 있다. 서비스 자동화는 사용자의 보안 정책 또는 라이선스에 대한 위배가 발생할 경우, 이벤트를 통해 관리자에게 상기의 위배가 통지될 수 있다.
- [110] 작업부하 및 서비스 관리(workload and service management)
- [111] 정의된 보안 정책 및 사용자 라이선스 동의에 따라 환경 설정, 운용 및 감시 서비스가 제공될 수 있다.
- [112] 도 2는 클라우드 서비스 모델을 설명한다.
- [113] 도 2에서, 상단의 숫자들을 도 1을 참조하여 전술된 15 개의 보안 도메인들을 나타낸다.
- [114] 좌측에 도시된 "보안 위협" 아래의 항목들은 클라우드 컴퓨팅에 존재하는 취약점에 기반하여 정의된 7 개의 위협들이다. 중간에 도시된 "보안 제어" 아래의 항목들은 보안 위협에 대응하는 보안 제어를 나타낸다. 우측에 도시된 "해당 표준 기술" 아래의 항목들은 보안 제어에 대응하는 표준 기술을 나타낸다.
- [115] 보안 제어들 각각에 대하여, 소프트웨어형 서비스(Software as a Service), 플랫폼형 서비스(Platform as a Service) 및 인프라형 서비스(Infrastructure as a Service; IaaS) 중 하나 이상이 적용될 수 있다.
- [116] 클라우드 컴퓨팅의 주요 위협들로서 하기의 항목들이 포함될 수 있다.
- [117] 제1 위협은 클라우드 컴퓨팅의 오용 및 비도덕적인 사용(abuse and nefarious use of cloud computing)일 수 있다. 악의적 목적으로 클라우드가 도입될 경우, 가상 공간 내에 정보가 존재하는 클라우드의 특성 때문에, 기존의 봇넷(botnet)에 비해 잠재적인 위협이 더 큰 것으로 간주될 수 있다.
- [118] 제2 위협은 불안정한 인터페이스 및 어플리케이션 프로그래밍 인터페이스(insecure interfaces and application programming interface)일 수 있다. 부가 가치의 제공을 위해, 기존 코드의 재사용 및 합성에 의해 어플리케이션이 구축될 경우, 복잡도 증가에 기인하여 보안 취약성이 발생할 수 있다.
- [119] 제3 위협은 악의적인 내부자(malicious insiders)일 수 있다. 클라우드 서비스를 위한 직원 채용에 있어서의 지침 또는 기준이 없을 수 있다. 해커, 조직 범죄 또는 기업 스파이 등 악의적 목적을 지닌 사람의 채용될 가능성이 증가함으로써, 클라우드 서비스 내의 데이터가 유출될 위험이 있을 수 있다.

- [120] 제4 위협은 기술 공유 문제(shared technology issues)일 수 있다. 인프라형 서비스는 공유 기술에 기반한 확장성을 제공할 수 있다. 제4 위협은 멀티-테넌트(Multi-Tenant) 아키텍처를 위한 효과적인 자원의 분리가 이루어지지 않을 경우에 존재할 수 있다.
- [121] 제5 위협은 데이터 유실 또는 유출(data loss or leakage)일 수 있다. 클라우드 환경의 구조적/운영적 특성에 의해 데이터 유출 위험이 증가할 수 있다. 제5 위협에 대한 다양한 원인이 존재할 수 있다.
- [122] 제6 위협은 계정 또는 서비스 하이재킹(account or service hijacking)일 수 있다. 클라우드 서비스에 있어서, 피싱, 사기 및 소프트웨어 취약성을 이용한 계정 접근은 일반적인 상황으로 간주될 수 있다. 클라우드 환경에서 계정 정보가 유출되는 것은 사용자의 모든 것이 노출되는 것과 동일한 위험이 될 수 있다.
- [123] 제7 위협은 알려지지 않은 위험 프로파일(unknown risk profile)일 수 있다. 소프트웨어 버전(version), 코드 업데이트, 취약성 프로파일, 침입 시도 및 보안 설계 등은 기업의 보안 현황 점검에 있어서 필수적인 요소로 간주될 수 있다.
- [124] 도 3는 클라우드 서비스에 대한 보안 위협을 설명한다.
- [125] 도 3에서 도시된 제1 위협 내지 제7 위협은 각각 도 2를 참조하여 전술된 제1 위협 내지 제7 위협 중 하나에 대응할 수 있다.
- [126] 제1 클라우드 서비스 제공자(310) 및 제2 클라우드 서비스 제공자(320) 내에는 하드웨어, 미들웨어, 데이터, 어플리케이션 및 API 등과 같은 개체(entity)가 존재할 수 있다. 하드웨어는 IaaS에 대응할 수 있다. 미들웨어는 PaaS에 대응할 수 있다. 데이터, 어플리케이션 및 API는 SaaS에 대응할 수 있다.
- [127] 위협으로부터 개체로의 화살표는 특정한 개체에 적용될 수 있는 위협을 나타낼 수 있다. 예컨대, 제2 위협은 특히 API에 적용될 수 있으며, 제6 위협은 클라이언트(330)에 적용될 수 있다.
- [128] 도 4는 일 실시예에 따른 클라우드 컴퓨팅 서비스 시스템이다.
- [129] 클라우드 컴퓨팅 서비스 시스템(400)은 단말(410), 서비스 통합부(420), 인증부(430)를 포함할 수 있다. 클라우드 컴퓨팅 서비스 시스템(400)은 하나 이상의 서비스 제공부들을 더 포함할 수 있다. 클라우드 컴퓨팅 서비스 시스템(400)은, 하나 이상의 서비스 제공부들로서, 제1 서비스 제공부(440) 및 제2 서비스 제공부(450)를 더 포함할 수 있다.
- [130] 클라우드 컴퓨팅 서비스 시스템(400)은 클라우드 컴퓨팅 서비스를 위한 보안 시스템일 수 있다.
- [131] 서비스 통합부(420), 인증부(430) 및 하나 이상의 서비스 제공부들은 동일한 물리적 장치 내의 구성요소들일 수 있다. 또는, 서비스 통합부(420), 인증부(430) 및 하나 이상의 서비스 제공부들은 각각 서로 상이한 물리적 장치일 수 있다. 말하자면, 클라우드 컴퓨팅 서비스 시스템(400)은 복수의 서버들로 구성될 수 있다. 예컨대, 서비스 통합부(420)는 클라우드 서비스 통합 서버일 수 있다. 인증부(430)는 인증 서버일 수 있다. 하나 이상의 서비스 제공부들은 하나 이상의

클라우드 서버들일 수 있다.

[132] 단말(410)은 단말(410)의 종류와는 무관하게 웹 브라우저와 같은 프로그램을 통해 사용자 주문형 서비스를 제공할 수 있다.

[133] 단말(410)은 다중 요인(multi-factor)을 이용함으로써 생성된 사용자의 토큰을 이용하여 사용자에 대한 인증을 요청할 수 있다. 사용자에 대한 인증은 사용자의 클라우드 서비스의 이용을 위한 인증일 수 있다. 다중 요인은 ID, 패스워드 X 509 증명 및 이메일 중 하나 이상일 수 있다.

[134] 단말(410)은 ID 및 패스워드를 사용하여 클라우드 서비스에 접근할 수 있다.

[135] 서비스 통합부(420)는 가상 개인 네트워크를 통해 다양한 클라우드 서비스들을 단말(410) 및 단말(410)의 사용자에게 제공하는 환경을 제공할 수 있다. 다양한 클라우드 서비스들은 융합 서비스로서 단말(410)에게 제공될 수 있다. 다양한 클라우드 서비스들이 융합됨에 따라 클라우드 서비스의 확장성이 향상될 수 있다.

[136] 서비스 통합부(420)는 접속을 요청한 단말(410)의 ID를 인증부(430)에게 제공할 수 있다. 서비스 통합부(420)는 인증부(430)로부터 단말(410)에 대한 승인 여부를 통보받을 수 있다. 단말(410)에 대한 승인은 단말(410)의 ID에 대한 승인일 수 있다.

[137] 인증부(430)는 서비스 통합부(420)의 운영 주체 및 하나 이상의 서비스 제공부들의 운영 주체가 아닌 제3의 운영 주체에 의해 운영될 수 있다. 인증부(430)는 공인된 운영 주체에 의해 운영될 수 있다.

[138] 인증부(430)는 단말(410)로부터 제공된 사용자의 정보를 관리할 수 있다. 단말(410)은 사용자의 개인 정보를 인증부(430)에게 제공할 수 있다. 인증부(430)는 사용자의 단말(410)을 통해 사용자의 개인 정보의 관리에 대한 인증을 받을 수 있다. 인증부(430)는 단말(410)로부터 제공된 사용자의 개인 정보를 관리할 수 있다.

[139] 인증부(430)는 사용자가 가입한 사이트 또는 사용자가 가입하고자 하는 사이트로부터 사용자에 대한 인증을 위임받을 수 있다. 인증부(430)는 위임에 따라 사용자에 대한 인증을 수행할 수 있다. 사용자가 가입한 사이트는 서비스 통합부(420) 또는 하나 이상의 서비스 제공부들일 수 있다.

[140] 단말(410)은 서비스 통합부(420)에게 클라우드 서비스에 대한 접근의 요청을 할 수 있다. 서비스 통합부(420)에서의 리다이렉션에 의해 인증부(430)가 사용자에 대한 인증을 수행할 수 있다.

[141] 인증부(430)는 다른 기관으로부터 요청된 사용자에 대한 인증을 수행할 수 있다.

[142] 인증부(430)는 정부 기관 또는 공인 인증 기관을 통해 사전에 가입한 사용자에게 대해서만 인증을 수행할 수도 있다. 인증부(430)는 사전에 가입한 사용자에게 임시 ID를 발급할 수 있다. 임시 ID의 발급을 통해, 인증부(430)는 사용자의 개인 정보의 노출 없이 사용자에 대한 인증을 수행할 수 있다.

- [143] 하나 이상의 서비스 제공부들은 가상 네트워크를 통해 인증부(430)에 의해 인증된 단말(410)에게 클라우드 서비스를 제공할 수 있다.
- [144] 하나 이상의 서비스 제공부들은 각각 사용자 또는 단말(410)의 클라우드 서비스에 대한 접근 권한을 확인할 수 있고, 접근 권한에 대응하는 클라우드 서비스를 제공할 수 있다.
- [145] 도 5는 일 실시예에 따른 서비스 통합부의 구조도이다.
- [146] 서비스 통합부(420)는 접근 제어부(510), 서비스 구성부(520) 및 침입 탐지부(530)를 포함할 수 있다.
- [147] 도 4를 참조하여 전술된 서비스 통합부(420)의 기능은 접근 제어부(510), 서비스 구성부(520) 및 침입 탐지부(530)에 분산하여 수행될 수 있다.
- [148] 접근 제어부(510)는 서비스 제공부의 서비스 정책에 기반하여 단말(410)의 토큰에게 접근 승인 및 사용 권한을 부여할 수 있다. 서비스 제공부는 도 4를 참조하여 전술된 하나 이상의 서비스 제공부들일 수 있다.
- [149] 사용자가 클라우드 서비스에 대한 접근을 요청할 때, 서비스 제공부로의 접근의 요청은 접근 제어부(510)에 의해 제어될 수 있다.
- [150] 접근 제어부(510)는 사용자의 단말(410)로부터 클라우드 서비스로의 접속의 요청을 수신할 수 있다.
- [151] 접근 제어부(510)는 단말(410)의 ID를 인증부(430)로 전송할 수 있다. 접근 제어부(510)는 인증부(430)로부터 ID에 기반한 사용자에 대한 인증의 결과를 수신할 수 있다.
- [152] 접근 제어부(510)는 사용자의 클라우드 서비스에 대한 접근 권한의 확인을 클라우드 서비스를 제공하는 서비스 제공부에게 요청할 수 있다.
- [153] 접근 제어부(510)는 서비스 제공부로부터 사용자의 클라우드 서비스에 대한 접근 권한의 확인의 결과를 수신할 수 있다. 접근 제어부(510)는 접근 권한의 확인의 결과가 사용자가 상기 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우 사용자의 토큰에 클라우드 서비스에 대한 접근 권한을 부여할 수 있다.
- [154] 접근 제어부(510)는 클라우드 서비스에 대한 접근 권한이 부여된 토큰을 단말(410)로 전송할 수 있다.
- [155] 접근 제어부(510)는 서비스 제공부로부터 클라우드 서비스의 등록 정보 및 사용자의 권한 정보의 요청을 수신할 수 있다. 접근 제어부(510)는 서비스 제공부로 등록 정보 및 권한 정보를 전송할 수 있다.
- [156] 서비스 구성부(520)는 서비스 제공부 상에 클라우드 서비스를 제공하기 위한 구성을 생성할 수 있다. 클라우드 서비스를 제공하기 위한 구성은 서비스 제공부 상에서 수행되는 가상 머신일 수 있다. 서비스 구성부(520)는 사용자가 요청한 클라우드 서비스에 관련된 모든 서비스들을 서비스 제공부 상에 구성할 수 있다.
- [157] 서비스 구성부(520)는 서비스 게이트웨이(gateway), 서비스 브로커, 가상 사설망 관리, 프라이버시 관리 및 감사 등의 기능을 수행할 수 있다.

- [158] 침입 탐지부(530)는 클라우드 컴퓨팅 서비스 시스템(400) 또는 서비스 통합부(420)에 대한 물리적 공격을 사전에 탐지하여 차단할 수 있다. 침입 탐지부(530)는 사전 탐지 및 차단을 통해 클라우드 컴퓨팅 서비스 시스템(400) 또는 서비스 통합부(420)의 가용성을 향상시킬 수 있다. 예컨대, 물리적 공격은 클라우드 컴퓨팅 서비스 시스템(400)의 외부 또는 내부에서의 트래픽 폭주를 이용한 네트워크 공격일 수 있다.
- [159] 침입 탐지부(530)는 서비스 제공부 내에 초급 탐지기를 설치할 수 있다. 초급 탐지기는 서비스 제공부 상의 가상 머신에 설치될 수 있다. 초급 탐지기는 가상 머신 상에서 동작하는 필수 프로그램으로서, 가상 머신이 생성될 때 설치될 수 있다.
- [160] 초급 탐지기는 네트워크 사용률 및 자원 사용률을 측정할 수 있다. 침입 탐지부(530)는 초급 탐지기에 의해 측정된 네트워크 사용률 및 자원 사용률에 기반하여 클라우드 컴퓨팅 서비스 시스템(400) 또는 서비스 통합부(420)에 대한 침입이 발생하였는지 여부를 판단할 수 있다. 침입 탐지부(530)는 침입이 발생한 것으로 판단한 경우, 침입이 발생한 것을 서비스 통합부(420)에게 통지할 수 있다.
- [161] 초급 탐지기는 클라우드 컴퓨팅 서비스 시스템(400) 내의 모든 가상 머신의 정보를 수집함으로써 침입이 발생하였는지 여부를 잘못 판단할 가능성을 낮출 수 있고, 긍정 오류(false positive)가 발생할 확률을 낮출 수 있다.
- [162] 경우에 따라, 침입 탐지부(530)는 서비스 제공부 내에 존재할 수 있으며, 인증부(430) 내에 존재할 수 있다. 말하자면, 침입 탐지부(530)는 서비스 통합부(420)에 종속되지 않을 수 있다.
- [163] 침입 탐지부(530)는 단말(410)에게 클라우드 서비스를 제공하기 위해 서비스 제공부 내에 가상 머신이 생성될 때부터 네트워크 정보 및 자원 사용 정보를 수집할 수 있다. 초급 탐지기는 협업 클라우드 컴퓨팅을 구성하는 모든 가상 머신의 정보를 수집할 수 있다. 침입 탐지부(530)는 수집된 정보에 기반하여 비정상적인 행위 패턴 등을 검출함으로써 침입 여부의 판단 및 공격 여부의 판단을 수행할 수 있다.
- [164] 도 6은 일 실시예에 따른 클라우드 서비스 방법의 흐름도이다.
- [165] 단계(610)에서, 사용자의 단말(410)은 서비스 통합부(420)에게 클라우드 서비스로의 접속의 요청을 전송할 수 있다. 서비스 통합부(420)는 단말(410)로부터 클라우드 서비스로의 접속의 요청을 수신할 수 있다. 클라우드 서비스로의 접속의 요청은 단말(410)의 ID를 포함할 수 있다.
- [166] 클라우드 서비스로의 접속의 요청은 토큰을 사용하여 수행될 수 있다. 단말(410)은 다중 요인을 사용함으로써 생성된 토큰을 서비스 통합부(420)로 전송할 수 있다. 토큰은 클라우드 서비스로의 접속의 요청을 나타낼 수 있다.
- [167] 클라우드 서비스로의 접속의 요청은 클라우드 서비스의 회원 가입일 수 있다. 클라우드 서비스로의 접속의 요청은 단말(410)의 사용자의 정보를 포함할 수

있다. 단말(410)의 사용자의 정보는 사용자의 개인 정보, 사용자의 ID 및 사용자의 패스워드 중 하나 이상을 포함할 수 있다. 예컨대, 사용자의 개인 정보, ID 및 패스워드가 서비스 통합부(420)에게 제공될 수 있다.

- [168] 단계(620)에서, 서비스 통합부(420)는 단말(410)의 ID 및 사용자의 정보를 인증부(430)로 전송할 수 있다. 단계(620)를 통해, 클라우드 서비스로의 접속의 요청은 서비스 통합부(420)로부터 인증부(430)로 리다이렉트(redirect)될 수 있다. 리다이렉션(redirection)에 의해, 인증부(430)가 단말(410)의 사용자에 대한 인증을 수행할 수 있다.
- [169] 단계(625)에서, 인증부(430)는 단말(410)의 ID에 기반하여 단말(410)의 사용자에 대한 인증을 수행할 수 있다.
- [170] 클라우드 서비스로의 접속의 요청이 클라우드 서비스의 회원 가입인 경우, 인증부(430)는 사용자에 대한 인증을 수행한 후, 사용자가 원하는 ID를 생성할 수 있다. 인증부(430)는 단말(410)에게 사용자가 원하는 ID를 발급해줄 수 있다. 인증부(430)는 발급된 ID를 단말(410)로 전송할 수 있다. 또는, 인증부(430)는 발급된 ID를 서비스 통합부(420)로 전송할 수 있고, 서비스 통합부(420)는 발급된 ID를 단말(410)로 전송할 수 있다. 회원 가입은 인증서, 공개ID(open ID), ID, 패스워드 및 이메일 등의 다양한 인증 수단에 의해 수행될 수 있다.
- [171] 인증부(430)는 사용자의 정보를 저장할 수 있다. 인증부(430)는 사용자의 정보를 암호화하여 저장할 수 있다.
- [172] 단계(630)에서, 인증부(430)는 단말(410)의 ID에 기반한 사용자에 대한 인증의 결과를 서비스 통합부(420)로 전송할 수 있다. 서비스 통합부(420)는 인증부(430)로부터 단말(410)의 ID에 기반한 사용자에 대한 인증의 결과를 수신할 수 있다.
- [173] 사용자에 대한 인증의 결과가 사용자가 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우, 하기의 단계들(640 내지 695)이 수행될 수 있다.
- [174] 단계(640)에서, 서비스 통합부(420)는 사용자의 클라우드 서비스에 대한 접근 권한의 확인을 클라우드 서비스를 제공하는 서비스 제공부(602)에게 요청할 수 있다. 서비스 제공부(602)는 도 4를 참조하여 전송된 제1 서비스 제공부(440) 또는 제2 서비스 제공부(450)에 대응할 수 있다. 서비스 제공부(602)는 서비스 통합부(420)로부터 사용자의 클라우드 서비스에 대한 접근 권한의 확인의 요청을 수신할 수 있다.
- [175] 단계(645)에서, 서비스 제공부(602)는 사용자의 클라우드 서비스에 대한 접근 권한을 확인할 수 있다.
- [176] 단계(650)에서, 서비스 제공부(602)는 사용자의 클라우드 서비스에 대한 접근 권한의 확인의 결과를 서비스 통합부(420)로 전송할 수 있다. 서비스 통합부(420)는 서비스 제공부(602)로부터 접근 권한의 확인의 결과를 수신할 수 있다.
- [177] 단계(655)에서, 접근 권한의 확인의 결과가 사용자가 클라우드 서비스에 대한

접근 권한을 가지고 있음을 나타내는 경우, 서비스 통합부(420)는 사용자의 토큰에게 클라우드 서비스에 대한 접근 권한을 부여할 수 있다.

- [178] 서비스 통합부(420)는 서비스 제공부(602)의 클라우드 서비스에 대한 정책에 기반하여 사용자의 토큰에게 접근 권한을 부여할 수 있다.
- [179] 상술된 클라우드 서비스는 복수일 수 있다. 또한, 복수의 클라우드 서비스들은 복수의 서비스 제공부(602)들에 의해 각각 제공될 수 있다. 사용자 또는 사용자의 단말(410)이 복수의 클라우드 서비스들을 동시에 사용할 경우, 서비스 통합부(420)는 복수의 클라우드 서비스들 각각에 대한 접근 권한들을 부여할 수 있다.
- [180] 단계(660)에서, 서비스 통합부(420)는 접근 권한이 부여된 토큰을 단말(410)로 전송할 수 있다. 단말(410)은 서비스 통합부(420)로부터 접근 권한이 부여된 토큰을 수신할 수 있다.
- [181] 하기의 단계들(670 내지 695)에서, 단말(410)에게 클라우드 서비스가 제공될 수 있다. 서비스 제공부(602)는 가상 네트워크를 통해 단말(410)에게 클라우드 서비스를 제공할 수 있다.
- [182] 단계(670)에서, 서비스 통합부(420)는 서비스 제공부(602) 상에 클라우드 서비스를 제공하기 위한 구성을 생성할 수 있다.
- [183] 클라우드 서비스를 제공하기 위한 구성은 서비스 제공부(602) 상에서 수행되는 가상 머신일 수 있다. 서비스 통합부(420)는 서비스 제공부(602) 상에서 단말(410)에게 클라우드 서비스를 제공하는 가상 머신을 생성할 수 있다.
- [184] 단계(675)에서, 단말(410)은 서비스 제공부(602)에게 클라우드 서비스를 요청할 수 있다. 단말(410)은 접근 권한이 부여된 토큰을 사용하여 서비스 제공부(602)에게 클라우드 서비스를 요청할 수 있다. 클라우드 서비스의 요청을 위해, 단말(410)은 접근 권한이 부여된 토큰을 서비스 제공부(602)로 전송할 수 있다.
- [185] 단계(680)에서, 서비스 제공부(602)는 클라우드 서비스의 등록 정보 및 단말(410)의 사용자의 권한 정보의 요청을 서비스 통합부(420)로 전송할 수 있다. 서비스 통합부(420)는 서비스 제공부(602)로부터 클라우드 서비스의 등록 정보 및 단말(410)의 사용자의 권한 정보의 요청을 수신할 수 있다.
- [186] 단계(685)에서, 서비스 통합부(420)는 클라우드 서비스의 등록 정보 및 단말(410)의 사용자의 권한 정보를 서비스 제공부(602)로 전송할 수 있다. 서비스 제공부(602)는 서비스 통합부(420)로부터 클라우드 서비스의 등록 정보 및 단말(410)의 사용자의 권한 정보를 수신할 수 있다.
- [187] 단계(690)에서, 서비스 제공부(602)는 클라우드 서비스의 등록 정보 및 단말(410)의 사용자의 권한 정보에 기반하여 단말(410)에게 클라우드 서비스를 제공할지 여부를 결정할 수 있다. 서비스 제공부(602)는 사용자의 권한 정보가 클라우드 서비스를 사용할 권한이 있다는 것을 나타내는 경우 단말(410)에게 클라우드 서비스를 제공할 것을 결정할 수 있다. 서비스 제공부(602)는 클라우드

서비스의 등록 정보를 사용하여 사용자의 권한 정보가 클라우드 서비스를 사용할 권한이 있다는 것을 나타내는지 여부를 판단할 수 있다.

[188] 단계(695)에서, 서비스 제공부(602)가 사용자의 권한 정보가 클라우드 서비스를 사용할 권한이 있다는 것을 나타낸다고 판단한 경우, 서비스 제공부(602)는 단말(410)에게 클라우드 서비스를 제공할 수 있다.

[189] 도 7은 일 실시예에 따른 클라우드 컴퓨팅 서비스 시스템이다.

[190] 클라우드 컴퓨팅 서비스 시스템(700)은 단말(710), 식별 서비스 제공부(Identification Service Provider; ISP)(720), 마켓 기반 클라우드 서비스 포털(Market-based Cloud Service Portal; MCSP)(730) 및 클라우드 서비스 제공부(Cloud Service Provider; CSP)(740)를 포함할 수 있다. 상술된 구성 이외에, 예컨대 도 4를 참조하여 전술된 클라우드 컴퓨팅 서비스 시스템(400)의 다른 구성요소가 클라우드 컴퓨팅 서비스 시스템(700)에 포함될 수 있다.

[191] CSP(740)는 복수 개일 수 있다. 복수의 CSP(740)들로서, 제1 CSP 내지 제n CSP가 도시되었다.

[192] 단말(710)은 도 4를 참조하여 전술된 단말(410)에 대응할 수 있다. ISP(720)는 도 4를 참조하여 전술된 인증부(430)에 대응할 수 있다. MCSP(730)는 도 4를 참조하여 전술된 서비스 통합부(420)에 대응할 수 있다. CSP(740)는 도 4를 참조하여 전술된 하나 이상의 서비스 제공부들에 대응할 수 있다.

[193] 사용자의 단말(710)은 사용자의 정보를 제 3의 공인된 ISP(720)에게 위임할 수 있다. 단말(710)은 단말(710)의 종류에 와는 무관하게 웹 브라우저와 같은 프로그램을 통해 사용자 주문형 서비스를 제공할 수 있다.

[194] ISP(720)는 공인된 제 3의 서비스 제공자 또는 공공 기관에 의해 운영될 수 있다. ISP(720)는 사용자의 정보를 위임받을 수 있다. ISP(720)는 위임받은 사용자의 정보를 관리할 수 있다. 단말(710)의 사용자는 인증서 또는 오픈 ID 등과 같은 다양한 인증 수단을 이용함으로써 ISP(720)에 가입할 수 있다. ISP(720)는 사용자가 가입하고자 하는 사이트로부터 인증의 위임의 요청을 받을 수 있다. ISP(720)는 사용자에 대한 인증의 결과를 사이트에게 통보할 수 있다.

[195] ISP(720)는 가입한 사용자의 정보를 사용자의 개인 키를 이용하여 암호화할 수 있다. ISP(720)는 암호화된 사용자의 정보를 관리할 수 있다. ISP(720)는 단말(710)의 요청에 따라 사용자의 정보의 무결성 및 기밀성 등에 대한 감사 기능을 제공할 수 있다.

[196] ISP(720)는 사용자 주문형 서비스 및 다양한 인터넷 기반 서비스들에 각각에 대한 가상 ID(Pseudo ID; PID)들을 관리할 수 있다. 상기의 관리를 위해 ISP(720)는 사용자가 특정한 서비스를 요청하면 요청된 서비스를 이용하기 위한 가상 ID를 생성할 수 있다. ISP(720)는 가입된 사용자와의 사전 협약에 따라 사용자의 공개 키를 배포할 수 있는 권한을 가질 수 있다.

[197] ISP(720)는 사용자의 요청에 따라 사용자가 서비스에 가입할 때 서비스 용 가상 ID를 생성할 수 있다. 예컨대, 개별적인 서비스 별로 서비스에 대한 가상 ID가

생성될 수 있다. 또한, ISP(720)는, 단말(710)이 MCSP(730)에서 특정한 클라우드 서비스 제공자의 서비스를 구매할 때, 단말(710)을 대신하여 클라우드 서비스 제공자에게 사용자에게 대한 인증을 제공할 수 있다. 또한, ISP(720)는 클라우드 서비스 제공자로부터 서비스를 제공받기 위해 서비스에 가입할 수 있다.

- [198] MCSP(730)는 다중 협업 클라우드 서비스의 브로커의 기능을 수행할 수 있다. MCSP(730)는 일종의 서비스 판매 중개업자로서 CSP(740)의 판매를 대행할 수 있다. MCSP(730)는 단말(710)이 구매한 CSP(740)의 서비스에 대한 구성, 관리 및 사용자 환경을 제공할 수 있다. 상기의 제공을 위해, MCSP(730) 및 CSP(740) 간의 계약 및 상호 인증이 요구될 수 있다.
- [199] 단말(710)이 MCSP(730)에게 클라우드 서비스의 구매를 요청할 경우, MCSP(730)는 웹 혹은 어플리케이션 형태의 사용자 인터페이스(User Interface; UI)를 단말(710)에게 제공할 수 있다. 예컨대, MCSP(730)는 CSP(740)가 제공하는 클라우드 서비스의 종류에 따라, UI 또는 단일 자원 지시기(Uniform Resource Locator; URL) 리다이렉션을 제공할 수 있다. 단말(710)의 사용자는 UI 또는 URL 리다이렉션을 통해 클라우드 서비스를 이용할 수 있다.
- [200] 도 8은 일 실시예에 따른 사용자가 ISP에 회원으로서 가입하는 절차를 도시한다.
- [201] 단계(810)에서, 단말(710)은 ISP(720)에 회원으로서 가입하기 위해 사용자의 정보, ID 및 패스워드를 ISP(720)로 전송할 수 있다. 상기의 ID는 사용자가 발급받기를 원하는 ID일 수 있다.
- [202] 단계(820)에서, ISP(720)는 ISP(720)에 회원으로서의 가입을 요청한 사용자에게 대한 인증을 수행할 수 있다. 사용자에게 대한 인증 후, ISP(720)는 사용자가 원하는 ID를 발급할 수 있다.
- [203] ISP(720)는 사용자의 정보를 암호화하여 저장할 수 있다. 또한, ISP(720)는 타 기관으로부터 요청된 사용자에게 대한 인증 과정을 수행할 수 있다.
- [204] ISP(720)는 가입의 승인을 나타내는 정보를 단말(710)로 전송할 수 있다.
- [205] 도 9는 일 실시예에 따른 MCSP의 구조도이다.
- [206] MCSP(730)는 보안부(900), 가상 사설 망(Virtual Private Network; VPN) 관리부(920), VPN(930), 서비스 브로커(940), 감시부(950), 서비스 구성부(960) 및 서비스 게이트웨이(970)를 포함할 수 있다.
- [207] 보안부(900)는 접근 제어부(910), 집행부(918) 및 키 관리부(919)를 포함할 수 있다. 접근 제어부(910)는 인증부(912), 허가부(914) 및 증명부(916)를 포함할 수 있다.
- [208] VPN(930)는 복수 개의 서비스들을 제공할 수 있다. 복수 개의 서비스들은 각각 클라우드 서비스일 수 있다. 복수 개의 서비스들로서, 제1 서비스 내지 제n 서비스가 도시되었다.
- [209] 서비스 구성부(960)는 정책 관리부(962), 서비스 제공부(964), 자원 관리부(966) 및 모니터링부(968)를 포함할 수 있다.

- [210] 단말(710)이 CSP(740)에 로그인할 때, 단말(710)은 단말(710)을 대신하여 위임된 인증을 수행할 ISP(720)의 주소 및 ISP(720)의 ID를 인증부(912)로 전송할 수 있다. 인증부(912)는 전송된 ISP(720)의 주소로의 리다이렉션을 수행할 수 있다. 리다이렉션을 통해, 인증부(912)는 ISP(720)에게 단말(710)의 사용자에게 대한 인증을 요청할 수 있다. 상기의 리다이렉션에서, 인증부(912)는 단말(710)의 ID를 ISP(720)로 전송할 수 있다. ISP(720)는 사용자의 입력에 기반하여 위임된 인증을 수행할 수 있다. 인증 후, ISP(720)는 사용자의 개인 키로 암호화된 ID를 MCSP(730)로 전송할 수 있다. 또한, ISP(720)는 사용자 정보를 포함한 공개 키를 암호화할 수 있고, 암호화된 공개 키를 MCSP(730)로 전송할 수 있다.
- [211] 허가부(914)는 ID 및 사용자의 정보에 기반하여, 사용자의 서비스에 대한 권한을 확인할 수 있고, 사용자가 구매한 주문형 서비스에 대한 내역 등을 확인할 수 있다. 허가부(914)는 XML을 이용하여 개인 서비스 프로파일(Personal Service Profile; PSP)를 작성할 수 있다. 허가부(914)는 PSP를 사용하여 서비스 구성부(960)에게 서비스 구성을 요청할 수 있다.
- [212] 증명부(916)는 ID 및 사용자의 정보를 전달된 공개 키를 이용하여 복호화할 수 있다. 증명부(916)는 복호화의 결과에 기반하여 사용자의 신원 증명을 확인할 수 있다.
- [213] 집행부(918)는 MCSP(730)의 보안 정책을 담당할 수 있다.
- [214] 키 관리부(919)는 서비스를 이용하고자 하는 단말(710) 또는 서비스에 맞는 키를 제공 및 관리할 수 있다.
- [215] VPN(930)은 단말(710)에게 서비스를 제공하기 위한 개인 네트워크를 구성할 수 있다. 단말(710)에게 제공되는 서비스들은 각각 VPN에 할당될 수 있으며, 상기의 할당을 통해 단말(710)에게 제공될 수 있다.
- [216] VPN 관리부(920)는 VPN을 위해 개인 네트워크를 생성 및 관리할 수 있다.
- [217] 서비스 브로커(940)는 다양한 사용자 서비스를 위한 VPN 세션을 관리할 수 있다. 서비스 브로커(940)는 VPN 관리부(920)를 통해 서비스 별 세션을 생성할 수 있다. 서비스 브로커(940)는 VPN 관리부(920)를 통해 서비스의 종료 시에 구성된 VPN(930) 및 VPN(930)에 관련된 사용자 데이터를 삭제할 수 있다. 사용자 데이터는 사용자의 정보 및 서비스의 캐쉬 데이터를 포함할 수 있다. 서비스 브로커(940)는 VPN 관리부(920)를 통해 일정 기간 동안 사용되지 않는 서비스를 종료시킬 수 있다. 말하자면, 서비스 브로커(940)는 서비스와 관련된 MCSP(730)의 전반적인 기능을 제어할 수 있다.
- [218] 감시부(950)는 단말(710)이 올바르게 서비스를 사용하는지 여부를 감시할 수 있다. 감시부(950)는 이상 트래픽 및 권한 침입을 감시할 수 있다. 감시부(950)는 MCSP(730)의 전반적인 보안 서비스를 감시할 수 있다.
- [219] 서비스 게이트웨이(970)는 MCSP(730) 및 CSP(740) 간의 안전한 통신을 제공할 수 있다. 서비스 게이트웨이(970)는 복수의 CSP(740)들 각각이 안전한 통신망을 위하여 VPN(930)과 통신하게 할 수 있다. 안전한 통신을 위해, 서비스

- 게이트웨이(970)는 복수의 CSP(740)들 각각과 안전한 통신 세션을 구성할 수 있다. 서비스 게이트웨이(970)는 구성된 통신 세션을 제어할 수 있다.
- [220] 서비스 구성부(960)는 접근 제어부(910)로부터 PSP를 제공받을 수 있다. 서비스 구성부(960)는 PSP에 기반하여 서비스를 구성할 수 있다. 서비스 구성부(960)는 서비스 이용을 위해 CSP(740)와 통신할 때, CSP(740)가 제공하는 오픈 API를 이용할 수 있다.
- [221] 자원 관리부(966)는 서비스의 구성을 위하여 CSP(740)가 제공하는 서비스 자원을 관리할 수 있다. 자원 관리부(966)는 PSP에 기반하여 명시된 자원에 대한 정보를 관리할 수 있다. 자원에 대한 정보는 서비스 URL, 스토리지 및 CPU 등을 포함할 수 있다.
- [222] 자원 관리부(966)는 PSP 내에 명시된 CSP(740)들에게 각 CSP(740)의 서비스를 위한 서비스 프로파일(Service Profile; SP)를 요청할 수 있다. 자원 관리부(966)는 PSP 내에 명시된 CSP(740)들에게 CSP(740)들 간의 서비스 자원 공유 및 협업에 필요한 정보를 제공할 수 있다. 예컨대, 단말(710)은 A사의 어플리케이션 서비스를 이용할 수 있다. 단말(710)은 어플리케이션 서비스를 이용함에 따라 생성된 데이터를 B사의 스토리지 서비스에 저장할 수 있다. 이 때, A사의 서비스로부터 B사의 스토리지로의 접근이 발생한 경우, A사의 어플리케이션은 자원 관리부(966)로부터 B사의 스토리지에 접근하기 위해 요구되는 정보를 획득할 수 있다. 스토리지에 접근하기 위해 요구되는 정보는 URP, IP 주소 및 사용자의 ID 등을 포함할 수 있다. A사의 어플리케이션은 획득된 정보를 사용하여 B사의 스토리지에 접근할 수 있다.
- [223] 자원 관리부(966)는 자원의 사용 현황 정보 등을 각 CSP에서 수집하여 업데이트 및 관리하며, 필요로 하는 구성요소로 제공한다.
- [224] 서비스 제공부(964)는 서비스의 제공을 위해 VPN 관리부(328)에게 서비스 세션의 생성을 요청할 수 있다. 서비스 제공부(964)는 서비스의 제공을 위한 환경을 구성할 수 있다.
- [225] 정책 관리부(962)는 서비스 별 또는 사용자 별로 보안 정책을 관리할 수 있다.
- [226] 모니터링부(968)는 서비스 오류에 대한 감시를 수행할 수 있으며, 정확한 서비스를 제공하기 위한 지속적인 서비스 감시를 수행할 수 있다.
- [227] 도 10은 일 실시예에 따른 사용자의 개인 정보 위임 및 로그인 과정을 설명한다.
- [228] 하기에서, 단말(710)이 사용자의 개인 정보를 ISP(720)에게 위임하는 과정 및 단말(710)이 MCSP(730)에 로그인하는 과정이 설명된다.
- [229] 단계(1010)에서, 단말(710)은 ISP(720)에게 회원 가입을 요청할 수 있다. 단말(710)은 ISP(720)에게 회원 가입과 함께 개인 정보의 위임을 요청할 수 있다.
- [230] 단계(1020)에서, 단말(710)은 MCSP(730)에 로그인할 수 있다. 단말(710)은 웹 브라우저를 통해 MCSP(730)에 로그인할 수 있다. 단말(710)은 사용자의 ID 및 ISP(720)의 주소를 사용하여 MCSP(730)에 로그인할 수 있다. 로그인을 통해 사용자의 ID 및 ISP(720)의 주소가 MCSP(730)로 전송될 수 있다.

- [231] 단계(1030)에서, MCSP(730)는 ISP(720)에게 ID에 대한 승인을 요청할 수 있다. ID에 대한 승인은 ID가 나타내는 단말(710)에 대한 서비스의 제공의 승인일 수 있다. MCSP(730)는 ISP(720)의 주소를 사용하여 ISP(720)에게 ID에 대한 승인을 요청할 수 있다. 상기의 요청과 함께, MCSP(730)는 승인의 결과를 제공받을 MCSP(730)의 주소를 ISP(720)로 전송할 수 있다.
- [232] 단계(1040)에서, ISP(720)는 ID에 대한 승인의 결과를 MCSP(730)에 통보할 수 있다. ISP(720)는 ID에 대한 승인의 결과를 ISP(720)에게 제공된 MCSP(730)의 주소로 전송할 수 있다.
- [233] 단계(1050)에서, 승인의 결과를 제공받은 MCSP(730)는 사용자에게 서비스 구성할 수 있다. MCSP(730)는 ISP(720)에 의해 제공된 서비스들 각각에 대해, 각 서비스를 위해 사용될 가상 ID를 이용하여 서비스를 구성할 수 있다.
- [234] 도 9를 참조하여 전송된 것처럼, 상술된 로그인 과정은 MCSP(730)의 접근 제어부(910)에 의해 수행될 수 있다.
- [235] 도 11은 일 실시예에 따른 사용자 서비스 구성 과정을 설명한다.
- [236] 단계(1110)에서, 서비스 구성부(960)는 접근 제어부(910)로부터 사용자의 PSP를 제공받을 수 있다. 서비스 구성부(960)는 사용자의 PSP에 기반하여 사용자를 위한 서비스를 구성할 수 있다.
- [237] 단계(1120)에서, 서비스 구성부(960)는 PSP를 자원 관리부(966)로 전달할 수 있다.
- [238] 단계(1130)에서, 자원 관리부(966)는 서비스 게이트웨이(970)와의 통신 세션을 생성할 수 있다.
- [239] 자원 관리부(966)는 서비스 구성부(960)로부터 제공된 서비스를 서비스 게이트웨이(970)에게 요청할 수 있다.
- [240] 단계(1140)에서, 서비스 게이트웨이(970)는 서비스를 제공하는 CSP(740)에게 서비스를 요청할 수 있다. 서비스 게이트웨이(970)는 CSP(740)가 제공하는 오픈 API를 이용하여 CSP(740)와 통신할 수 있다.
- [241] 단계(1150)에서, CSP(740)는 게이트웨이에 의해 요청된 서비스를 서비스 구성부(960)에게 제공할 수 있다.
- [242] 도 12는 일 실시예에 따른 MCSP 회원 가입 및 MCSP 이용 절차를 설명한다.
- [243] 단계(1200)에서, 사용자는 단말(710)을 통해 MCSP(730)에 회원 가입을 요청할 수 있다. 단말(710)은 CSP(740)의 서비스를 제공받기 위해서 MCSP(730)에 회원으로서 가입한 후 서비스를 구매해야 할 수 있다. 사용자에게 대한 인증은 단말(710), ISP(720) 및 MCSP(730)의 사이에서 이루어질 수 있다.
- [244] 단계(1202)에서, MCSP(730)는 ISP(720)에게 사용자에게 대한 인증을 요청할 수 있다. MCSP(730)는 사용자 로그인 시 입력된 ID 및 패스워드의 정보를 선택된 ISP(720)로 리다이렉션할 수 있다. 리다이렉션이 이용되기 때문에, MCSP(730) 내에는 ID 및 패스워드의 정보가 남지 않을 수 있다.
- [245] 단계(1204)에서, ISP(720)는 사용자에게 대한 인증을 수행한 후 MCSP(730)에

회원으로서 가입하기 위한 가상 ID(Pseudo ID, PID)를 발급할 수 있다. ISP(720)는 MCSP(730)에게만 PID 및 MCSP 요청 정보를 전달할 수 있다. PID 및 MCSP는 암호화될 수 있다. MCSP 요청 정보는 서비스와 관련된 사용자의 관심 및 취향에 대한 정보일 수 있다. ISP(720)는 사용자가 회원으로서 가입한 MCSP(730)에서 사용될 PID 및 서비스의 요청에 대한 정보를 XML 형태의 사용자 서비스 프로파일(User Service Profile; USP)로서 저장할 수 있다. USP는 암호화된 채 저장될 수 있다.

- [246] 단계(1206)에서, MCSP(730)는 ISP(720)로부터 전달받은 USP를 이용하여 XML 형태의 PSP를 생성할 수 있다. MCSP(730)는 단말(710)에게 인증의 결과를 전달할 수 있으며, 사용자의 회원 가입을 승인할 수 있다.
- [247] 단계(1208)에서, 단말(710)은 MCSP(730)를 통해 원하는 CSP(740)의 서비스를 구매할 수 있다. 구매를 위해, MCSP(730)는 서비스 이용을 위해 사용되는 서비스 가상 ID(Service Pseudo ID; SPID)를 생성할 수 있고, 생성된 SPID를 이용하여 CSP(740)에게 서비스의 가입을 요청할 수 있다.
- [248] 단계(1210)에서, CSP(740)는 MCSP(730)가 요청한 가입을 승인할 수 있다. 단말(710)은 MCSP(730)를 통해 원하는 CSP(740)의 서비스를 구매할 수 있다. 예컨대, MCSP(730)는 SPID를 이용하여 원하는 CSP(740)의 서비스를 구매 및 관리할 수 있다.
- [249] 단계(1212)에서, MCSP(730)는 PSP를 업데이트할 수 있다. MCSP(730)는 단말(710)이 구매한 서비스의 정보를 ISP(720)에 전달할 수 있다. 서비스의 정보는 SPID를 포함할 수 있다. MCSP(730)는 CSP(740)의 서비스를 위해 각 서비스 별로 SPID를 생성 및 관리할 수 있다. MCSP(730)는 서비스가 종료되는 시점에 PSP 및 관련된 데이터를 삭제할 수 있다.
- [250] 단말(710)이 특정한 CSP(740)의 서비스를 요청하면, MCSP(730)는 서비스의 구매 여부를 확인할 수 있다. MCSP(730)는 단말(710)이 요청된 서비스가 기존에 구매되지 않은 것이면, 새로운 SPID를 생성할 수 있고, 생성된 SPID를 사용하여 상술한 구매 절차를 수행할 수 있다.
- [251] CSP(740)는 단말(710)이 요청한 서비스를 제공할 수 있다. MCSP(730)는 변경된 서비스 정보인 PSP를 업데이트할 수 있다.
- [252] 단말(710)이 MCSP(730)에게 로그아웃을 요청하면, MCSP(730)는 서비스의 제공의 중단과 함께 최종적으로 업데이트된 PSP를 ISP(720)으로 전송할 수 있다. MCSP(730)는 서비스의 제공 중에 사용된 데이터 및 PID를 삭제할 수 있고, 로그아웃을 수행할 수 있다. ISP(720)는 MCSP(730)로부터 전송된 PSP를 이용하여 USP를 갱신할 수 있고, 갱신된 USP를 저장할 수 있다.
- [253] 상술된 것과 같이, 실시예에서는 계층 별로 상이한 ID가 사용될 수 있다. 예컨대, 단말(710) 및 ISP(720) 간에는 ISP ID가 사용될 수 있다. ISP(720) 및 MCSP(730) 간에는 PID가 사용될 수 있다. MCSP(730) 및 CSP(740) 간에는 SPID가 사용될 수 있다. 즉, 각 단계에 있어서, 서로 상이한 ID가 발급 및 사용될

수 있다.

- [254] 단말(710) 및 ISP(720) 간에는 제1 암호화 알고리즘을 이용하여 암호화된 정보가 송수신될 수 있다. ISP(720) 및 MCSP(730) 간에는 제2 암호화 알고리즘을 이용하여 암호화된 정보가 송수신될 수 있다. MCSP(730) 및 CSP(740) 간에는 제3 암호화 알고리즘을 이용하여 암호화된 정보를 송수신될 수 있다.
- [255] 상술된 것과 같이, 개인 정보의 보호를 위해서 단계 별로 서로 상이한 ID를 발급하거나, 서로 상이한 암호화 알고리즘을 이용함으로써, 해킹 등에 의해 사용자의 ID가 노출된 경우에서도, 사용자의 개인 정보 및 사용자가 어떤 데이터를 사용하는 지가 보호될 수 있다.
- [256] 클라우드 컴퓨팅 시스템은 단말(710) 및 ISP(720) 간에서 사용되는 제1 암호화 알고리즘, ISP(720) 및 MCSP(730) 간에서 사용되는 제2 암호화 알고리즘 및 MCSP(730)와 CSP(740) 간에서 사용되는 제3 암호화 알고리즘을 서로 상이하게 설정함으로써 다수의 보안 신뢰 구간들을 형성할 수 있다. 다수의 보안 신뢰 구간들을 통해 사용자의 정보가 효율적으로 보호될 수 있다.
- [257] 클라우드 컴퓨팅 시스템은 MCSP(730)가 다중의 CSP(740)들 간의 사용자의 정보 전달 및 자원 접근을 통제함에 따라 다중의 CSP(740)간의 사용자의 정보 전달, 가공 및 처리에 있어서 사용자 정보 보호가 이루어질 수 있다.
- [258] 클라우드 컴퓨팅 시스템은 단말(710) 및 ISP(720) 간에서 사용되는 제1 사용자 식별자, ISP(720) 및 MCSP(730) 간에서 사용되는 제2 사용자 식별자 및 MCSP(730) 및 CSP(740) 간에서 사용되는 제3 사용자 식별자를 서로 상이하게 설정함으로써 사용자 정보를 효율적으로 보호할 수 있다.
- [259] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [260] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정

및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[261] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

청구범위

- [청구항 1] 사용자의 단말로부터 클라우드 서비스로의 접속의 요청을 수신하는 단계;
상기 사용자의 상기 클라우드 서비스에 대한 접근 권한의 확인을 상기 클라우드 서비스를 제공하는 서비스 제공부에게 요청하는 단계;
상기 서비스 제공부로부터 상기 확인의 결과를 수신하는 단계;
상기 결과가 상기 사용자가 상기 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우 상기 사용자의 토큰에 상기 클라우드 서비스에 대한 접근 권한을 부여하는 단계를 포함하는, 클라우드 서비스 방법.
- [청구항 2] 제1항에 있어서,
상기 단말의 식별자를 인증부로 전송하는 단계; 및
상기 인증부로부터 상기 식별자에 기반한 상기 사용자에 대한 인증의 결과를 수신하는 단계를 더 포함하는, 클라우드 서비스 방법.
- [청구항 3] 제1항에 있어서,
상기 사용자의 토큰을 상기 단말로 전송하는 단계를 더 포함하는, 클라우드 서비스 방법.
- [청구항 4] 제1항에 있어서,
상기 서비스 제공부로부터 상기 클라우드 서비스의 등록 정보 및 상기 사용자의 권한 정보의 요청을 수신하는 단계; 및
상기 서비스 제공부로 상기 등록 정보 및 상기 권한 정보를 전송하는 단계를 더 포함하는, 클라우드 서비스 방법.
- [청구항 5] 제1항에 있어서,
상기 서비스 제공부 상에 상기 클라우드 서비스를 제공하기 위한 구성을 생성하는 단계를 더 포함하는, 클라우드 서비스 방법.
- [청구항 6] 제5항에 있어서,
상기 클라우드 서비스를 제공하기 위한 상기 구성은 상기 서비스 제공부 상에서 수행되는 가상 머신인, 클라우드 서비스 방법.
- [청구항 7] 제1항에 있어서,
상기 클라우드 서비스는 가상 네트워크를 통해 상기 서비스 제공부에 의해 상기 단말에게 제공되는, 클라우드 서비스 방법.
- [청구항 8] 제1항에 있어서,

- 상기 클라우드 서비스는 복수 개인, 클라우드 서비스 방법.
- [청구항 9] 제1항에 있어서,
상기 접근 권한은 상기 서비스 제공부의 상기 클라우드 서비스에 대한 정책에 기반하여 상기 토큰에게 부여되는, 클라우드 서비스 방법.
- [청구항 10] 제1항의 방법을 수행하는 프로그램을 수록한 컴퓨터 판독 가능 기록 매체.
- [청구항 11] 사용자의 단말로부터 클라우드 서비스로의 접속의 요청을 수신하고, 상기 사용자의 상기 클라우드 서비스에 대한 접근 권한의 확인을 상기 클라우드 서비스를 제공하는 서비스 제공부에게 요청하고, 상기 서비스 제공부로부터 상기 확인의 결과를 수신하고, 상기 결과가 상기 사용자가 상기 클라우드 서비스에 대한 접근 권한을 가지고 있음을 나타내는 경우 상기 사용자의 토큰에 상기 클라우드 서비스에 대한 접근 권한을 부여하는 접근 제어부; 및
상기 서비스 제공부 상에 상기 클라우드 서비스를 제공하기 위한 구성을 생성하는 서비스 구성부를 포함하는, 클라우드 서비스 통합 서버.
- [청구항 12] 제11항에 있어서,
상기 접근 제어부는 상기 단말의 식별자를 인증부로 전송하고, 상기 인증부로부터 상기 식별자에 기반한 상기 사용자에 대한 인증의 결과를 수신하는, 클라우드 서비스 통합 서버.
- [청구항 13] 제11항에 있어서,
상기 접근 제어부는 상기 사용자의 토큰을 상기 단말로 전송하는, 클라우드 서비스 통합 서버.
- [청구항 14] 제11항에 있어서,
상기 접근 제어부는 상기 서비스 제공부로부터 상기 클라우드 서비스의 등록 정보 및 상기 사용자의 권한 정보의 요청을 수신하고, 상기 서비스 제공부로 상기 등록 정보 및 상기 권한 정보를 전송하는, 클라우드 서비스 통합 서버.
- [청구항 15] 제11항에 있어서,
상기 클라우드 서비스를 제공하기 위한 상기 구성은 상기 서비스 제공부 상에서 수행되는 가상 머신인, 클라우드 서비스 통합 서버.
- [청구항 16] 제11항에 있어서,
상기 클라우드 서비스는 가상 네트워크를 통해 상기 서비스 제공부에 의해 상기 단말에게 제공되는, 클라우드 서비스 통합 서버.
- [청구항 17] 제11항에 있어서,

[청구항 18]

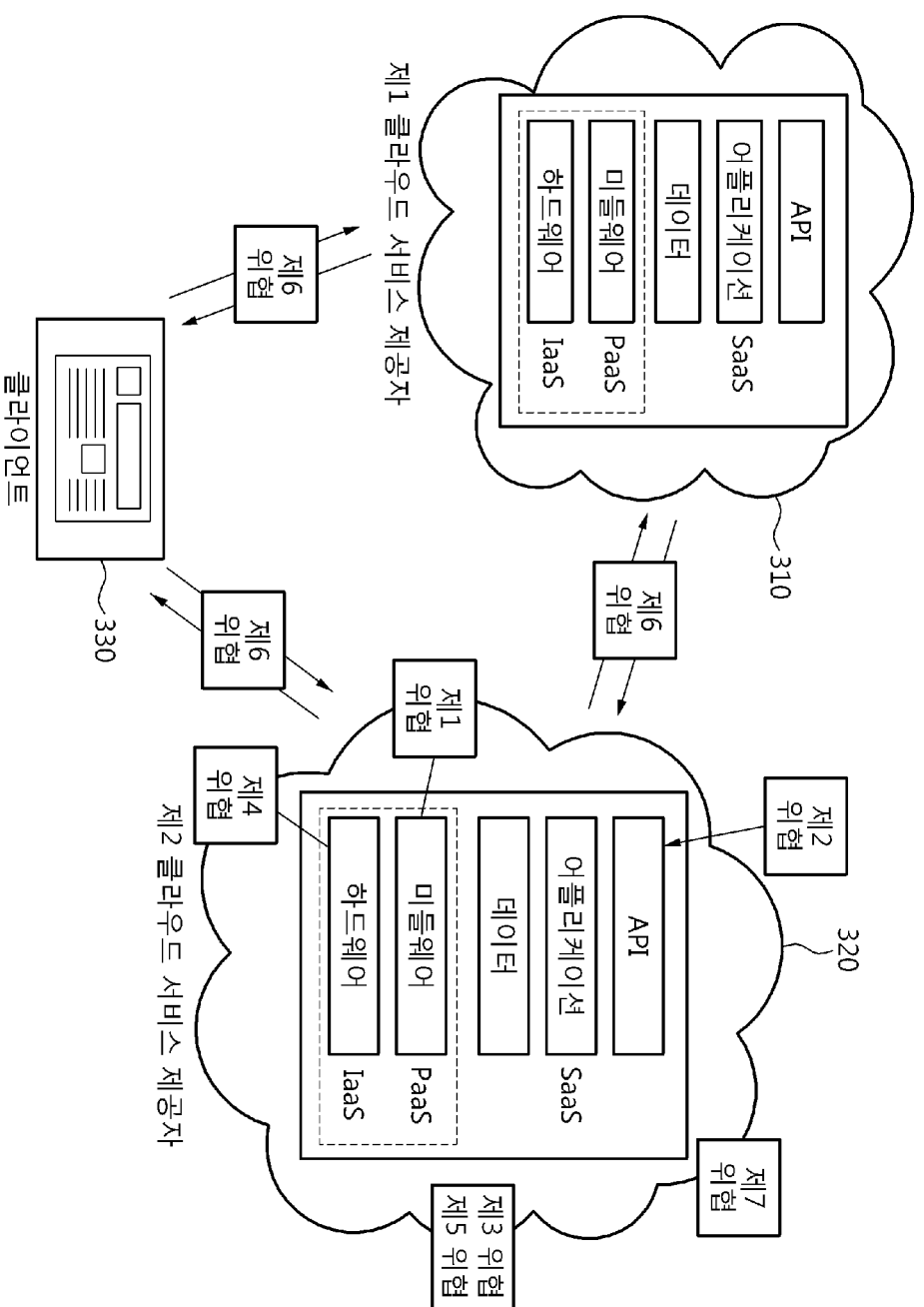
상기 클라우드 서비스는 복수 개인, 클라우드 서비스 통합 서버,
제11항에 있어서,
상기 접근 권한은 상기 서비스 제공부의 상기 클라우드 서비스에
대한 정책에 기반하여 상기 토큰에게 부여되는, 클라우드 서비스
통합 서버.

[Fig. 1]

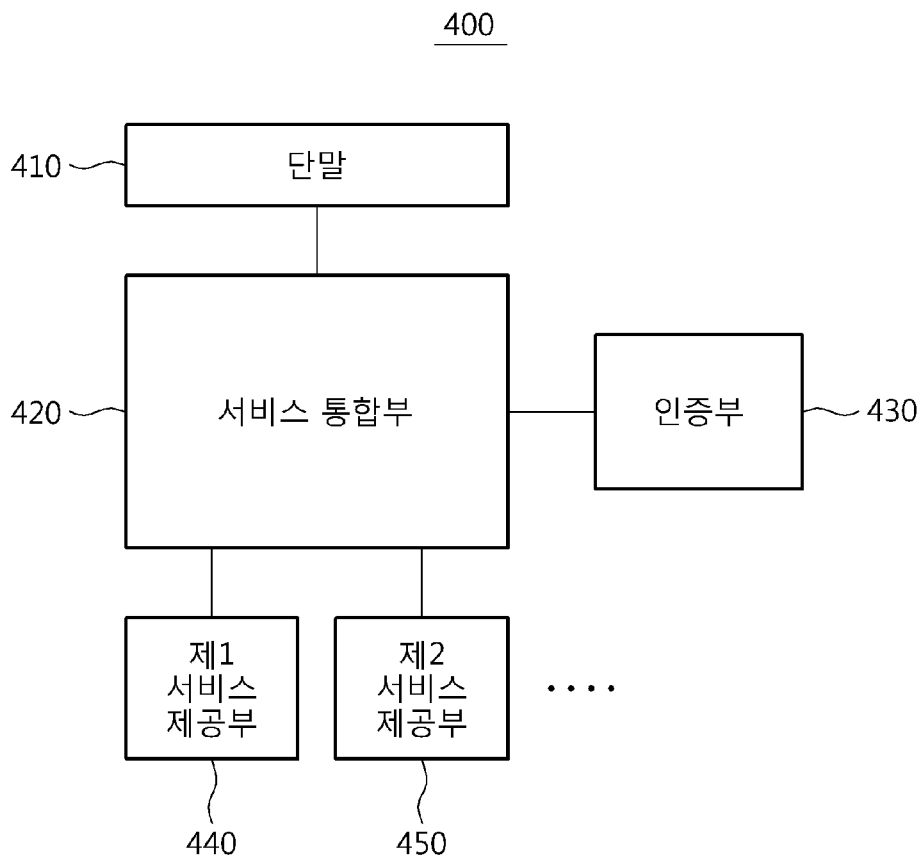
제1 도메인 : 클라우드 컴퓨팅 아키텍처 프레임워크
 제2 도메인 : 기업 위험 관리
 제3 도메인 : 법률
 제4 도메인 : 전자 증거 개시
 제5 도메인 : 준수 및 감사
 제6 도메인 : 정보 생명주기 관리
 제7 도메인 : 휴대성 및 상호 운용성
 제8 도메인 : 보안, 기밀 및 복구
 제9 도메인 : 데이터 센터 운용
 제10 도메인 : 빠른 응답, 통지 및 교정
 제11 도메인 : 어플리케이션 보안
 제12 도메인 : 암호화 및 키 관리
 제13 도메인 : 식별 및 접근 관리
 제14 도메인 : 스토리지
 제15 도메인 : 가상화

[Fig. 2]

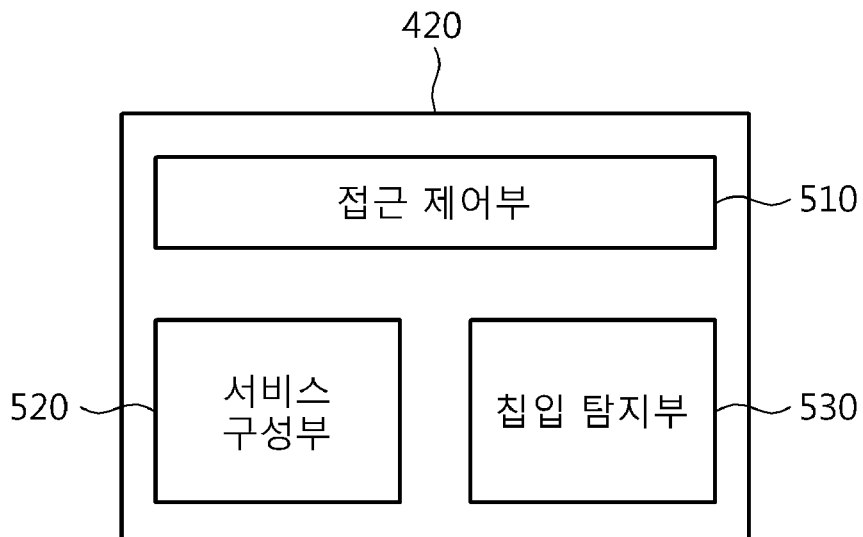
도메인	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
보안 위험	보안 제어										해당 표준 기술				
클라우드 컴퓨팅의 오용 및 비도덕 사용	지원 관리														
불안전한 인터페이스 및 API	암호화 : 키 및 인증서 관리										KMIP				
	데이터/스토리지 보안										IEEE P1619				
악의적인 내부자	종단점 보안														
	이벤트 감사 및 리포팅														
기술 공유 문제	식별, 규정, 접근 제어 및 속성										SAML, X, 509 인증				
데이터 유실 및 유출	네트워크 보안														
계정 또는 서비스 하이재킹	보안 정책										XACML				
	서비스 자동화														
알려지지 않은 위험 프로파일	작업 및 서비스 관리										SPML				



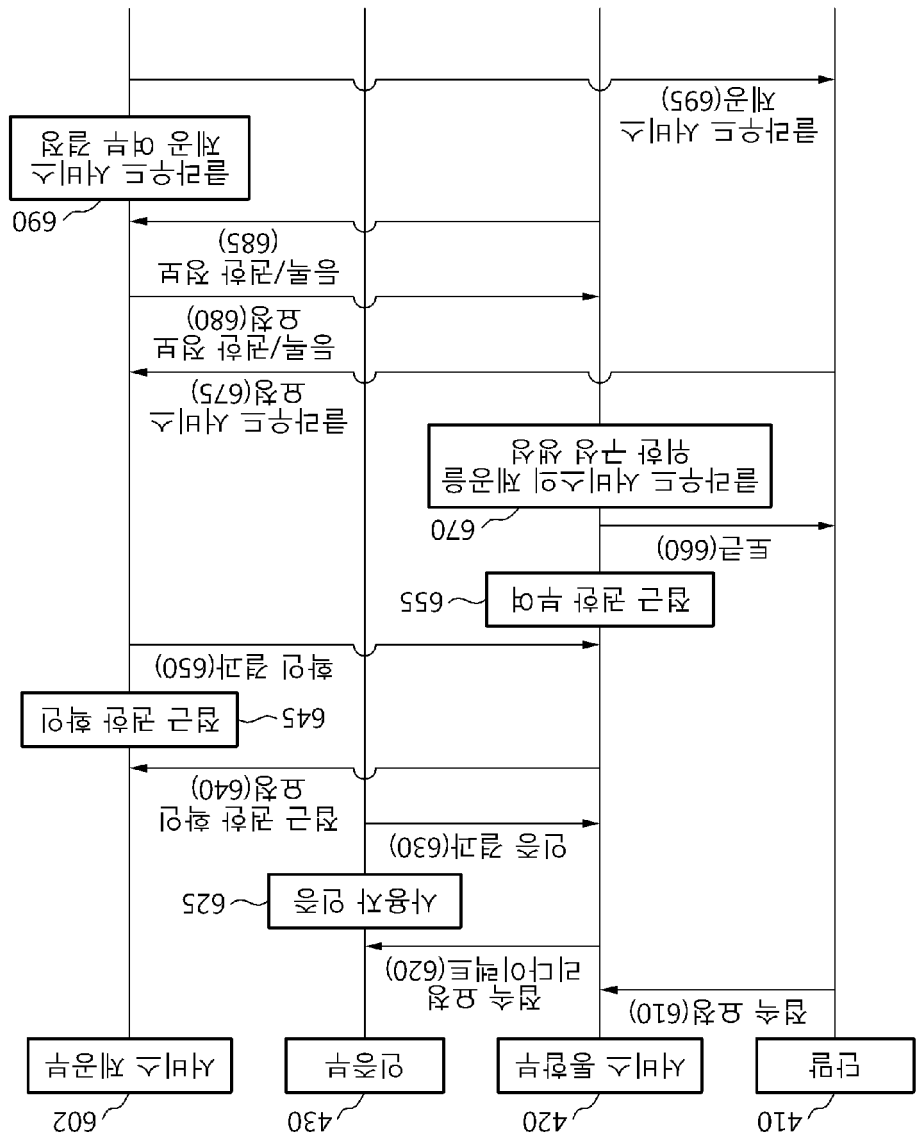
[Fig. 4]



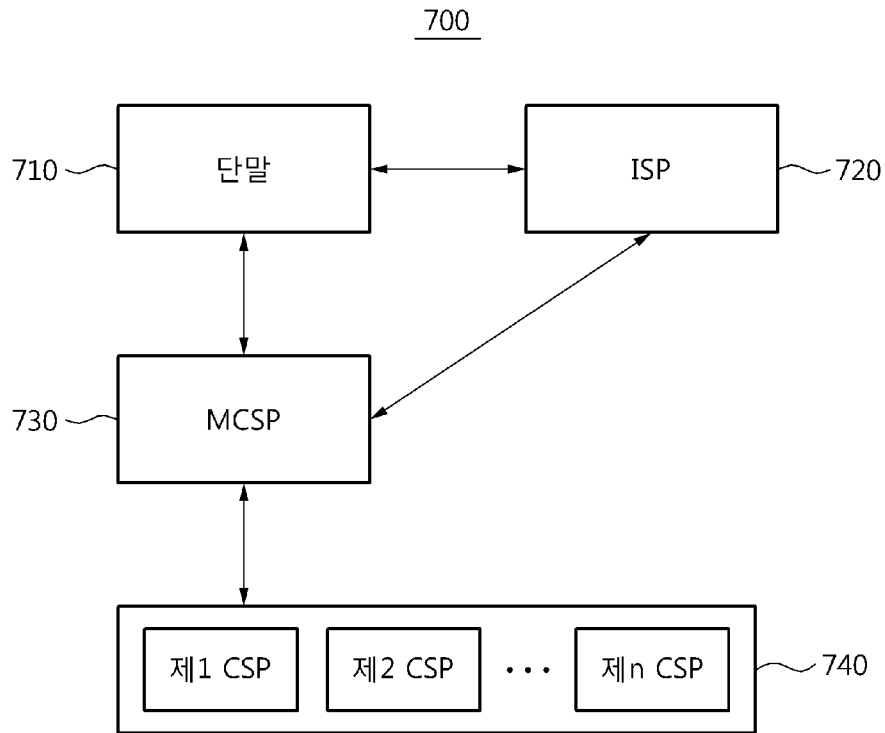
[Fig. 5]



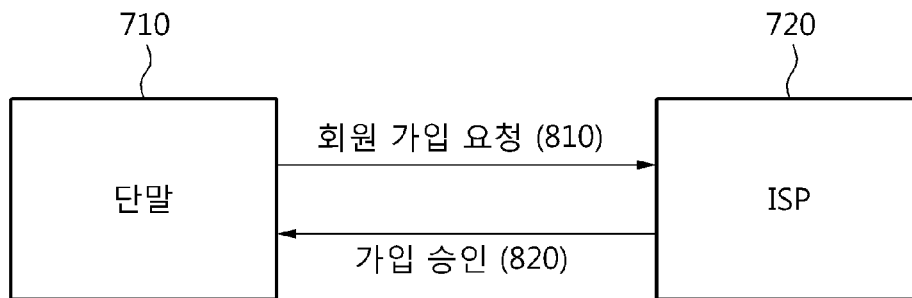
[Fig. 6]



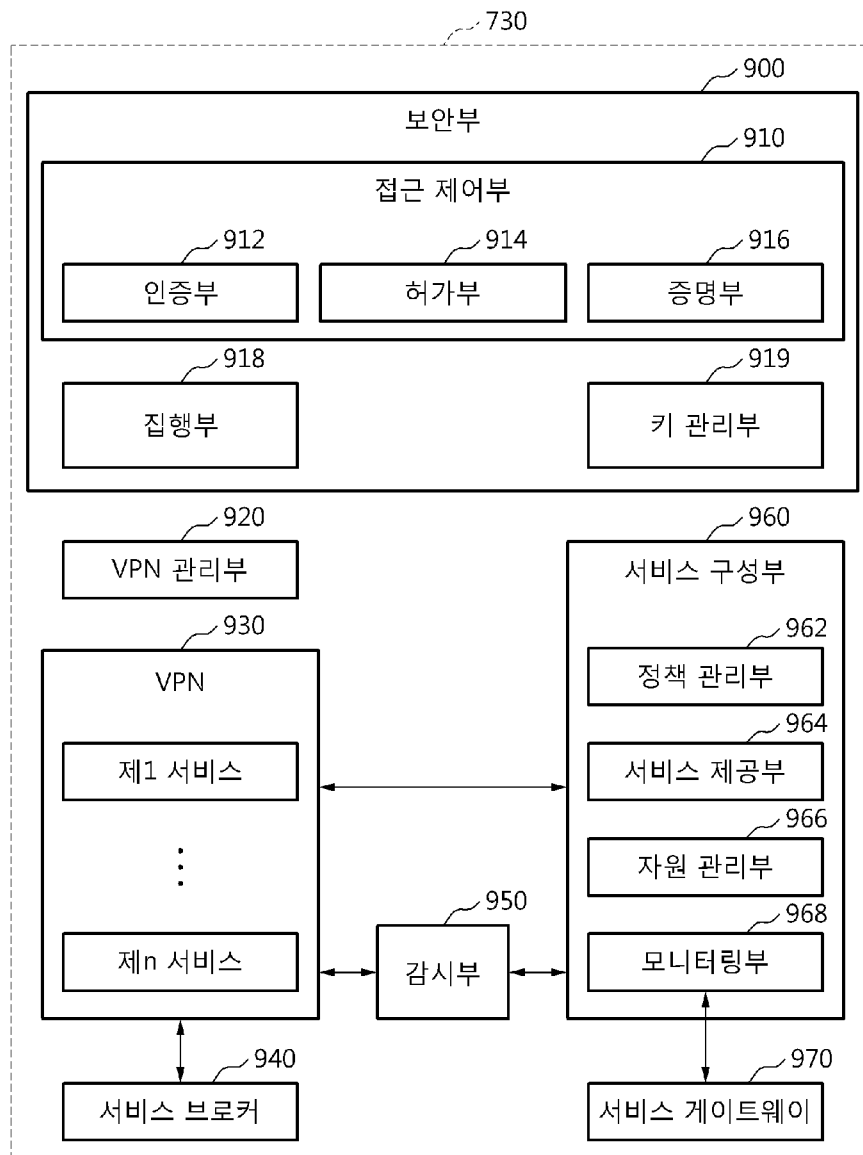
[Fig. 7]



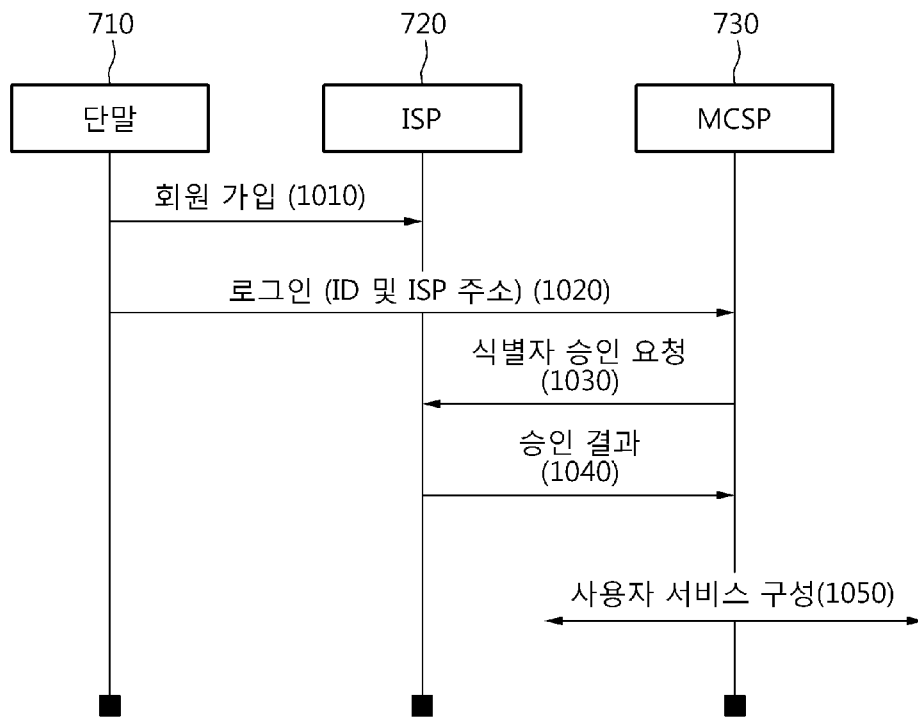
[Fig. 8]



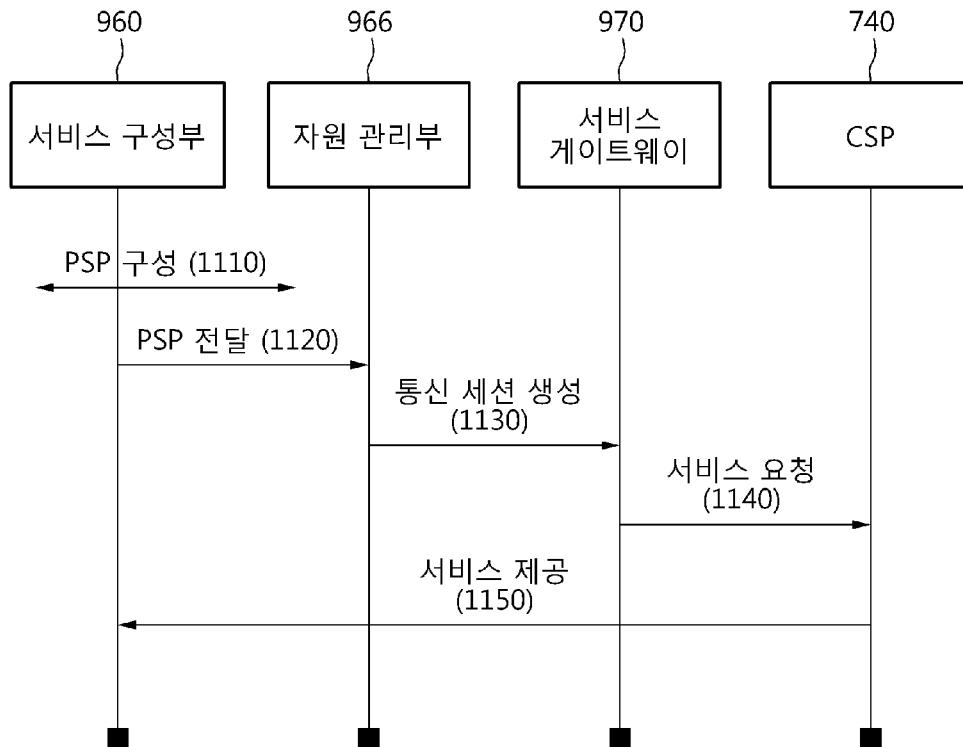
[Fig. 9]



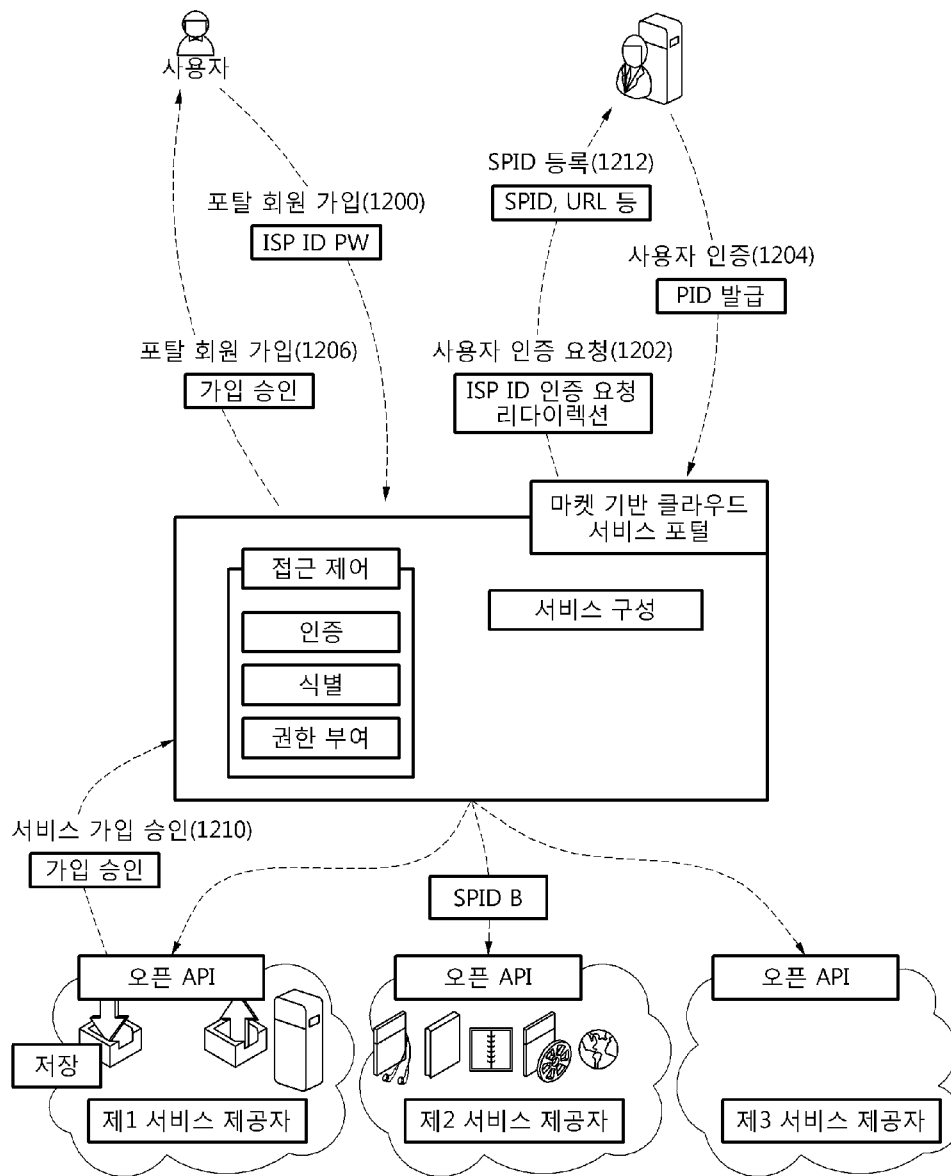
[Fig. 10]



[Fig. 11]



[Fig. 12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2012/010487**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/20(2006.01)i, H04L 9/32(2006.01)i, G06F 15/16(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/20; G06F 15/173; G06F 17/00; H04W 12/08; G06F 9/455; H04W 12/04; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: cloud, service, virtual machine, token, access, right, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2011-0002810 A (SAMSUNG ELECTRONICS CO., LTD.) 10 January 2011 See paragraphs 75, 77, 78, 80; and figure 6a.	1-18
A	KR 10-2010-0110816 A (MICROSOFT CORP.) 13 October 2010 See paragraphs 12, 14, 38, 40; and figure 2.	1-18
A	US 2011-0214176 A1 (LLOYD LEON BURCH et al.) 01 September 2011 See paragraphs 22-23; and figure 1.	1-18
A	US 2011-0265168 A1 (MARK LUCOVSKY et al.) 27 October 2011 See paragraph 25; claim 8; and figures 1, 4A, 4B.	1-18
A	US 2011-0126197 A1 (KAL A. LARSEN et al.) 26 May 2011 See paragraphs 116-127; claim 1; and figures 3, 4.	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

07 MARCH 2013 (07.03.2013)

Date of mailing of the international search report

08 MARCH 2013 (08.03.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2012/010487

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2011-0002810 A	10.01.2011	KR 10-2011-0002809 A	10.01.2011
		US 2010-0131590 A1	27.05.2010
		US 2010-0131592 A1	27.05.2010
		US 2010-0131966 A1	27.05.2010
		US 2011-0004574 A1	06.01.2011
		US 2011-0004916 A1	06.01.2011
		US 8239538 B2	07.08.2012
		WO 2010-058989 A1	27.05.2010
KR 10-2010-0110816 A	13.10.2010	CN 101911087 A	08.12.2010
		EP 2250608 A1	17.11.2010
		JP 2011-510539 A	31.03.2011
		US 2009-0183010 A1	16.07.2009
		WO 2009-091459 A1	23.07.2009
US 2011-0214176 A1	01.09.2011	NONE	
US 2011-0265168 A1	27.10.2011	NONE	
US 2011-0126197 A1	26.05.2011	US 2011-0125894 A1	26.05.2011
		US 2011-0125895 A1	26.05.2011
		US 2011-0126047 A1	26.05.2011
		US 2011-0126099 A1	26.05.2011
		US 2011-0126207 A1	26.05.2011
		US 2011-0126275 A1	26.05.2011

A. 발명이 속하는 기술분류(국제특허분류(IPC)) <i>G06F 21/20(2006.01)i, H04L 9/32(2006.01)i, G06F 15/16(2006.01)i</i>		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) G06F 21/20; G06F 15/173; G06F 17/00; H04W 12/08; G06F 9/455; H04W 12/04; G06F 21/00 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 클라우드, 서비스, 가상 머신, 토큰, 접근, 권한, 인증		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2011-0002810 A (삼성전자주식회사) 2011.01.10 단락 75, 77, 78, 80; 및 도면 6a 참조.	1-18
A	KR 10-2010-0110816 A (마이크로소프트 코퍼레이션) 2010.10.13 단락 12, 14, 38, 40; 및 도면 2 참조.	1-18
A	US 2011-0214176 A1 (LLOYD LEON BURCH 외 2명) 2011.09.01 단락 22-33; 및 도면 1 참조.	1-18
A	US 2011-0265168 A1 (MARK LUCOVSKY 외 4명) 2011.10.27 단락 25; 청구항 8; 및 도면 1, 4A, 4B 참조.	1-18
A	US 2011-0126197 A1 (KAL A. LARSEN 외 3명) 2011.05.26 단락 116-127; 청구항 1; 및 도면 3, 4 참조.	1-18
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2013년 03월 07일 (07.03.2013)		국제조사보고서 발송일 2013년 03월 08일 (08.03.2013)
ISA/KR의 명칭 및 우편주소  팩스 번호 82-42-472-7140		심사관 변성철 전화번호 82-42-481-8262 

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2011-0002810 A	2011.01.10	KR 10-2011-0002809 A US 2010-0131590 A1 US 2010-0131592 A1 US 2010-0131966 A1 US 2011-0004574 A1 US 2011-0004916 A1 US 8239538 B2 WO 2010-058989 A1	2011.01.10 2010.05.27 2010.05.27 2010.05.27 2011.01.06 2011.01.06 2012.08.07 2010.05.27
KR 10-2010-0110816 A	2010.10.13	CN 101911087 A EP 2250608 A1 JP 2011-510539 A US 2009-0183010 A1 WO 2009-091459 A1	2010.12.08 2010.11.17 2011.03.31 2009.07.16 2009.07.23
US 2011-0214176 A1	2011.09.01	없음	
US 2011-0265168 A1	2011.10.27	없음	
US 2011-0126197 A1	2011.05.26	US 2011-0125894 A1 US 2011-0125895 A1 US 2011-0126047 A1 US 2011-0126099 A1 US 2011-0126207 A1 US 2011-0126275 A1	2011.05.26 2011.05.26 2011.05.26 2011.05.26 2011.05.26 2011.05.26