



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0100460

(43) 공개일자 2015년09월02일

(51) 국제특허분류(Int. Cl.)

G06F 21/50 (2013.01) G06F 17/00 (2006.01)

(21) 출원번호 10-2014-0083893

(22) 출원일자 2014년07월04일

심사청구일자 2014년07월04일

(30) 우선권주장

1020140021458 2014년02월24일 대한민국(KR)

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)

(72) 발명자

허의남

경기도 용인시 기흥구 서천로 27, 108동 201호 (서천동, 서천마을1단지)

나상호

경기도 용인시 기흥구 덕영대로 1732, 전자정보대학 331호 (서천동)

(74) 대리인

특허법인 신지

전체 청구항 수 : 총 13 항

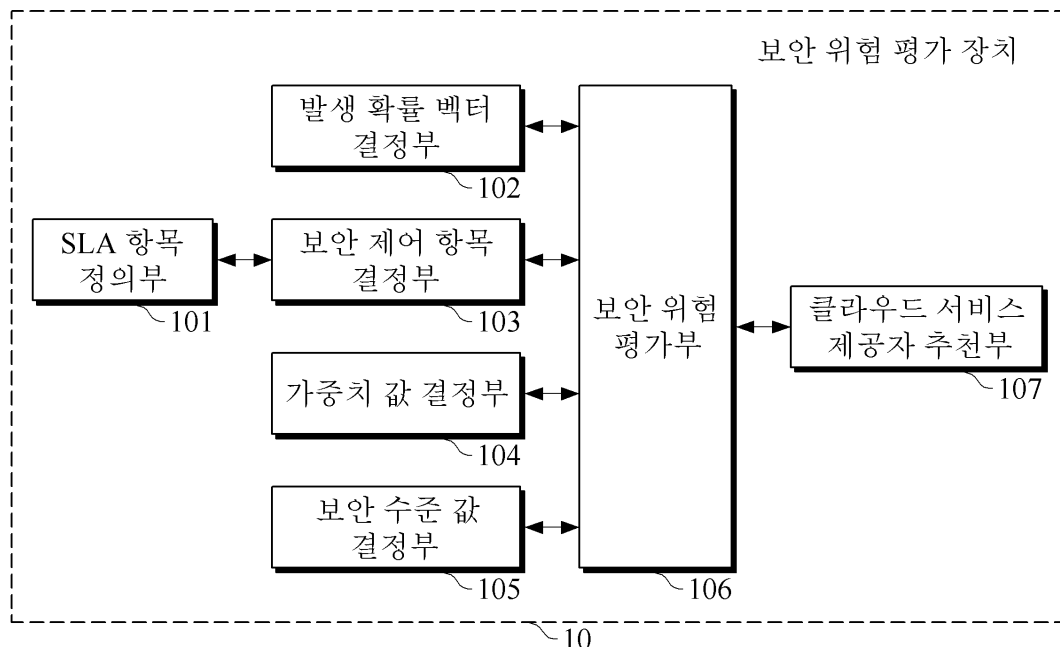
(54) 발명의 명칭 클라우드 컴퓨팅 환경에서의 보안 위험 평가 장치 및 평가 방법, 보안 위험 평가 결과를 이용한 클라우드 서비스 제공자 추천 방법

(57) 요약

클라우드 컴퓨팅 환경에서의 보안 위험 평가 장치 및 평가 방법, 보안 위험 평가 결과를 이용한 클라우드 서비스 제공자 추천 방법이 개시된다. 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위험 평가 장치는 클라우드 서비스에 있어서 보안 사고 발생 정도를 기반으로 정해지는 상기 클라우드 서비스의 보안 위험에 대한 발생 확률

(뒷면에 계속)

대표도 - 도2



벡터를 결정하는 발생 확률 벡터 결정부; 상기 클라우드 서비스의 유형에 따라 상기 클라우드 서비스의 보안 제어를 수행하는 물리적 방법인 하나 또는 그 이상의 보안 제어 항목을 결정하는 보안 제어 항목 결정부; 상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 가중치 값을 결정하는 가중치 값 결정부; 상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 보안 수준 값을 결정하는 보안 수준 값 결정부; 및 상기 발생 확률 벡터, 상기 하나 또는 그 이상의 보안 제어 항목, 상기 보안 제어 항목의 가중치 값 및 상기 보안 수준 값을 이용하여 상기 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위협을 정량적으로 평가하는 보안 위협 평가부를 포함한다.

이 발명을 지원한 국가연구개발사업

과제고유번호 1711014131

부처명 미래창조과학부

연구관리전문기관 한국정보통신산업진흥원

연구사업명 대학ICT 연구센터육성 지원사업

연구과제명 실시간 모바일 클라우드 서비스 플랫폼 연구개발

기 여 율 1/1

주관기관 경희대학교 산학협력단

연구기간 2014.01.01 ~ 2014.12.31

특허청구의 범위

청구항 1

클라우드 서비스에 있어서 보안 사고 발생 정도를 기반으로 정해지는 상기 클라우드 서비스의 보안 위협에 대한 발생 확률 벡터를 결정하는 발생 확률 벡터 결정부;

상기 클라우드 서비스의 유형에 따라 상기 클라우드 서비스의 보안 제어를 수행하는 물리적 방법인 하나 또는 그 이상의 보안 제어 항목을 결정하는 보안 제어 항목 결정부;

상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 가중치 값을 결정하는 가중치 값 결정부;

상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 보안 수준 값을 결정하는 보안 수준 값 결정부; 및

상기 발생 확률 벡터, 상기 하나 또는 그 이상의 보안 제어 항목, 상기 보안 제어 항목의 가중치 값 및 상기 보안 수준 값을 이용하여 상기 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위협을 정량적으로 평가하는 보안 위협 평가부;

를 포함하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

청구항 2

제1항에 있어서,

상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사·확인 및 준수(Audit·Verification and Compliance) 중 어느 하나 이상을 포함하는 그룹에서 상기 클라우드 서비스의 유형에 따라 선택되는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

청구항 3

제1항에 있어서,

상기 클라우드 서비스의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의하는 SLA 항목 정의부를 더 포함하고,

상기 보안 제어 항목 결정부는 상기 SLA 항목 정의부에서 정의된 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 이용하여 상기 하나 또는 그 이상의 보안 제어 항목을 결정하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

청구항 4

제1항에 있어서,

상기 보안 위협 평가부는 보안 위협에 대한 발생 확률 벡터, 상기 클라우드 서비스에 대하여 보안 위협과 관련된 보안 제어 항목의 가중치 벡터 및 보안 위협에 대한 평가 대상의 보안 위협 벡터를 이용하여 보안 위협을 평가하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

청구항 5

제1항에 있어서,

$$SR_T = P_T \times [W]_S \times [V]_T$$

상기 보안 위협 평가부는 . 을 이용하여 계산된 결과값을 총합하여 보안 위협을 평가하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

(여기서, SR_T 는 보안 위협 T에 대한 보안 위협, P_T 는 보안 위협 T에 대한 발생 확률 벡터, $[W]_S$ 는 클라우드 서버

스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목의 가중치 벡터, $[V]_T$ 는 보안 위협 T에 대한 평가 대상의 보안 위협 벡터)

청구항 6

제1항에 있어서,

상기 클라우드 서비스의 사용자가 이용하고자 하는 클라우드 서비스 유형 및 상기 클라우드 서비스의 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 작성한 협상 요청 메시지를 수신하면, 상기 수신한 협상요청 메시지에 따라 상기 보안 위협 평가부의 결과로부터 이용 가능한 상기 클라우드 서비스 제공자를 판단하여 상기 클라우드 서비스 사용자에게 제공하는 클라우드 서비스 제공자 추천부를 더 포함하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치.

청구항 7

클라우드 서비스에 있어서 보안 사고 발생 정도를 기반으로 정해지는 상기 클라우드 서비스의 보안 위협에 대한 발생 확률 벡터를 결정하는 단계;

상기 클라우드 서비스의 유형에 따라 상기 클라우드 서비스의 보안 제어를 수행하는 물리적 방법인 하나 또는 그 이상의 보안 제어 항목을 결정하는 단계;

상기 클라우드 서비스의 유형에 따라 상기 하나 또는 그 이상의 보안 제어 항목별로 상기 보안 제어 항목의 가중치 값을 결정하는 단계;

상기 클라우드 서비스의 제공자에 따라 상기 하나 또는 그 이상의 보안 제어 항목별로 상기 보안 제어 항목에 대한 보안 수준 값을 결정하는 단계; 및

상기 발생 가능성 벡터, 상기 하나 또는 그 이상의 보안 제어 항목, 상기 보안 제어 항목의 가중치 값 및 상기 보안 수준 값을 이용하여 상기 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위협을 정량적으로 평가하는 단계;

를 포함하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법.

청구항 8

제7항에 있어서,

상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사·확인 및 준수(Audit·Verification and Compliance) 중 어느 하나 이상을 포함하는 그룹에서 상기 클라우드 서비스의 유형에 따라 선택되는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법.

청구항 9

제7항에 있어서,

상기 발생 확률 벡터의 결정 단계 이전에 상기 클라우드 서비스의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의하는 단계를 더 포함하고,

상기 보안 제어 항목의 결정 단계에서는 상기 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 이용하여 상기 하나 또는 그 이상의 보안 제어 항목을 결정하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법.

청구항 10

제7항에 있어서,

상기 보안 위협을 정량적으로 평가하는 단계에서는 보안 위협에 대한 발생 확률 벡터, 상기 클라우드 서비스에 대하여 보안 위협과 관련된 보안 제어 항목의 가중치 벡터 및 보안 위협에 대한 평가 대상의 보안 위협 벡터를 이용하여 보안 위협을 평가하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법.

청구항 11

제7항에 있어서,

$$SR_T = P_T \times [W]_S \times [V]_T$$

상기 보안 위협을 정량적으로 평가하는 단계에서는, 을 이용하여 계산된 결과 값을 총합하여 보안 위협을 평가하는 것을 특징으로 하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법.

(여기서, SR_T 는 보안 위협 T에 대한 보안 위험, P_T 는 보안 위협 T에 대한 발생 확률 벡터, $[W]_S$ 는 클라우드 서비스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목의 가중치 벡터, $[V]_T$ 는 보안 위협 T에 대한 평가 대상의 보안 위험 벡터)

청구항 12

클라우드 서비스의 유형 및 상기 클라우드 서비스의 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 송신한 협상요청 메시지를 수신하는 단계;

상기 수신한 협상요청 메시지에 따라 클라우드 컴퓨팅 환경에서의 보안 위협 평가방법의 결과로부터 이용 가능한 상기 클라우드 서비스 제공자를 판단하는 단계; 및

상기 판단한 결과를 전송하는 단계

를 포함하는 클라우드 컴퓨팅 환경에서의 보안 위협 평가결과를 이용한 클라우드 서비스 제공자 추천 방법.

청구항 13

제7항 내지 제12항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명세서

기술분야

[0001]

본 발명은 컴퓨터 보안과 관련된 기술로서, 보다 상세하게는 클라우드 컴퓨팅 환경에서 클라우드 서비스 제공자의 보안 위협을 평가하는 기술에 관한 것이다.

배경기술

[0002]

클라우드 컴퓨팅이란 인터넷 기술을 활용하여 가상화된 IT 자원을 서비스 형태로 제공하는 컴퓨팅으로, 사용자는 IT 자원(예를 들어, 응용 서비스, 소프트웨어, 스토리지, 서버, 네트워크 등)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불한다. 즉, 클라우드 컴퓨팅은 인터넷 프로토콜 기반의 IT 서비스 제공 모델로서, IT 서비스 사용자는 클라우드 서비스를 제공하고 있는 시스템의 물리적인 위치와 구성에 상관없이 언제, 어디서든, 필요시에 인터넷을 통하여 IT 서비스를 제공받을 수 있다. 이와 같이, 클라우드 컴퓨팅 기술의 활성화에 따라 다양한 클라우드 서비스가 제공되고 있으나, 아웃소싱 리소스라는 특징으로 인하여 클라우드 컴퓨팅의 보안 문제점은 클라우드 컴퓨팅 기술의 성장에 있어서 장애물로 인식되고 있다.

[0003]

한편, 전통적인 IT 환경에서는 사용자의 요구사항을 반영한 서비스 수준 협약(Service Level Agreements)을 통하여 서비스 품질(Quality of Service)을 보장하기 위한 방법론들이 도입되었는데, 서비스 수준 협약(Service Level Agreements)은 서비스 사용자와 서비스 제공자 간의 일정한 서비스 제공 수준을 보장하기 위한 계약으로, 이는 클라우드 컴퓨팅에서도 동일하게 적용되고 있다. 그러나, 기존의 서비스 수준 협약은 보안 요소에 대한 측면은 고려하고 있지 않아 보안 서비스 수준 보장을 위한 연구가 중요한 이슈가 되고 있으며, 더욱이 클라우드 기반의 보안 서비스(아웃소싱 보안 서비스, Security as a Service)가 클라우드 컴퓨팅의 보안을 향상시켜 줄

수 있다는 전망 아래 다양한 연구가 진행되고 있다.

[0004] 또한, 전통적인 IT 환경에서 보안 서비스는 단순히 “제공되는(Offered)” 기반 기술로 여겨졌으나, 클라우드 기반의 보안 서비스의 등장으로 인해 “요구되는(On-Demand)” 서비스로의 인식의 변화가 진행되고 있다. 클라우드 컴퓨팅 기술 활성화와 스마트 모바일 디바이스 보급의 증가에 따라 모바일 클라우드로 정의되는 복잡한 서비스 환경 속에서 사용자는 다양한 보안 서비스 수준을 보장 받을 수 있는 환경이 마련되어야 한다.

[0005] 그러나, 종래의 보안 서비스 수준 평가는 정성적인 방식으로 평가하고 있어 사용자가 구체적인 평가 내용을 알 수 없는 문제점이 있다. 또한, 클라우드 서비스의 보안 위협은 각 클라우드 서비스의 특성과 사용자 환경에 따라 그 보안 위협의 종류와 위협 정도가 상이한데, 기존의 보안 평가는 이러한 특성을 반영하지 못하는 문제점이 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 하나의 과제는 클라우드 서비스 제공자 측면에서 클라우드 서비스의 보안 위협을 정량적으로 평가할 수 있는 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치 및 평가 방법을 제공하는 것이다.

[0007] 본 발명이 해결하고자 하는 다른 하나의 과제는 클라우드 서비스의 보안 위협 평가 결과를 기반으로 클라우드 서비스 제공자 간의 비교를 통하여 클라우드 서비스 사용자의 보안 요구사항에 가장 부합하는 클라우드 서비스 제공자를 추천하는 클라우드 서비스 환경에서의 보안 위협 평가 결과를 이용한 클라우드 서비스 제공자 추천 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치는 클라우드 서비스에 있어서 보안 사고 발생 정도를 기반으로 정해지는 상기 클라우드 서비스의 보안 위협에 대한 발생 확률 벡터를 결정하는 발생 확률 벡터 결정부; 상기 클라우드 서비스의 유형에 따라 상기 클라우드 서비스의 보안 제어를 수행하는 물리적 방법인 하나 또는 그 이상의 보안 제어 항목을 결정하는 보안 제어 항목 결정부; 상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 가중치 값을 결정하는 가중치 값 결정부; 상기 결정된 보안 제어 항목별로 상기 보안 제어 항목에 대한 보안 수준 값을 결정하는 보안 수준 값 결정부; 및 상기 발생 확률 벡터, 상기 하나 또는 그 이상의 보안 제어 항목, 상기 보안 제어 항목의 가중치 값 및 상기 보안 수준 값을 이용하여 상기 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위협을 정량적으로 평가하는 보안 위협 평가부를 포함한다.

[0009] 상기 실시예의 일 측면에 의하면, 상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사·확인 및 준수(Audit·Verification and Compliance) 중 어느 하나 이상을 포함하는 그룹에서 상기 클라우드 서비스의 유형에 따라 선택될 수 있다.

[0010] 상기 실시예의 다른 측면에 의하면, 상기 클라우드 서비스의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의하는 SLA 항목 정의부를 더 포함하고, 상기 보안 제어 항목 결정부는 상기 SLA 항목 정의부에서 정의된 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 이용하여 상기 하나 또는 그 이상의 보안 제어 항목을 결정할 수 있다.

[0011] 상기 실시예의 또 다른 측면에 의하면, 상기 보안 위협 평가부는 보안 위협에 대한 발생 확률 벡터, 상기 클라우드 서비스에 대하여 보안 위협과 관련된 보안 제어 항목의 가중치 벡터 및 보안 위협에 대한 평가 대상의 보안 위협 벡터를 이용하여 보안 위협을 평가할 수 있다.

[0012] 상기 실시예의 또 다른 측면에 의하면, 상기 보안 위협 평가부는 $SR_T = P_T \times [W]_S \times [V]_T$ 을 이용하여 계산된 결과값을 총합하여 보안 위협을 평가할 수 있다. (여기서, SR_T 는 보안 위협 T에 대한 보안 위협, P_T 는 보안 위협 T에 대한 발생 확률 벡터, $[W]_S$ 는 클라우드 서비스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목

의 가중치 벡터, $[V]_T$ 는 보안 위협 T에 대한 평가 대상의 보안 위협 벡터)

- [0013] 상기 실시예의 또 다른 측면에 의하면, 상기 클라우드 서비스의 사용자가 이용하고자 하는 클라우드 서비스 유형 및 상기 클라우드 서비스의 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 작성한 협상 요청 메시지를 수신하면, 상기 수신한 협상요청 메시지에 따라 상기 보안 위협 평가부의 결과로부터 이용 가능한 상기 클라우드 서비스 제공자를 판단하여 상기 클라우드 서비스 사용자에게 제공하는 클라우드 서비스 제공자 추천부를 더 포함할 수 있다.
- [0014] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법은 클라우드 서비스에 있어서 보안 사고 발생 정도를 기반으로 정해지는 상기 클라우드 서비스의 보안 위협에 대한 발생 확률 벡터를 결정하는 단계; 상기 클라우드 서비스의 유형에 따라 상기 클라우드 서비스의 보안 제어를 수행하는 물리적 방법인 하나 또는 그 이상의 보안 제어 항목을 결정하는 단계; 상기 클라우드 서비스의 유형에 따라 상기 하나 또는 그 이상의 보안 제어 항목별로 상기 보안 제어 항목의 가중치 값을 결정하는 단계; 상기 클라우드 서비스의 제공자에 따라 상기 하나 또는 그 이상의 보안 제어 항목별로 상기 보안 제어 항목에 대한 보안 수준 값을 결정하는 단계; 및 상기 발생 가능성 벡터, 상기 하나 또는 그 이상의 보안 제어 항목, 상기 보안 제어 항목의 가중치 값 및 상기 보안 수준 값을 이용하여 상기 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위협을 정량적으로 평가하는 단계를 포함한다.
- [0015] 상기 실시예의 일 측면에 의하면, 상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사·확인 및 준수(Audit·Verification and Compliance) 중 어느 하나 이상을 포함하는 그룹에서 상기 클라우드 서비스의 유형에 따라 선택될 수 있다.
- [0016] 상기 실시예의 다른 측면에 의하면, 상기 발생 확률 벡터의 결정 단계 이전에 상기 클라우드 서비스의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의하는 단계를 더 포함하고, 상기 보안 제어 항목의 결정 단계에서는 상기 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 이용하여 상기 하나 또는 그 이상의 보안 제어 항목을 결정할 수 있다.
- [0017] 상기 실시예의 또 다른 측면에 의하면, 상기 보안 위협을 정량적으로 평가하는 단계에서는 보안 위협에 대한 발생 확률 벡터, 상기 클라우드 서비스에 대하여 보안 위협과 관련된 보안 제어 항목의 가중치 벡터 및 보안 위협에 대한 평가 대상의 보안 위협 벡터를 이용하여 보안 위협을 평가할 수 있다.
- [0018] 상기 실시예의 또 다른 측면에 의하면, 상기 보안 위협을 정량적으로 평가하는 단계는 $SR_T = P_T \times [W]_S \times [V]_T$ 을 이용하여 계산된 결과값을 총합하여 보안 위협을 평가할 수 있다. (여기서, SR_T 는 보안 위협 T에 대한 보안 위협, P_T 는 보안 위협 T에 대한 발생 확률 벡터, $[W]_S$ 는 클라우드 서비스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목의 가중치 벡터, $[V]_T$ 는 보안 위협 T에 대한 평가 대상의 보안 위협 벡터)
- [0019] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위협 평가결과를 이용한 클라우드 서비스 제공자 추천 방법은 클라우드 서비스의 유형 및 상기 클라우드 서비스의 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 송신한 협상요청 메시지를 수신하는 단계; 상기 수신한 협상요청 메시지에 따라 클라우드 컴퓨팅 환경에서의 보안 위협 평가방법의 결과로부터 이용 가능한 상기 클라우드 서비스 제공자를 판단하는 단계; 및 상기 판단한 결과를 전송하는 단계를 포함한다.
- [0020] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 컴퓨터 판독가능한 기록매체는 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위협 평가 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된다.

발명의 효과

- [0021] 이상과 같이 본 발명의 일 실시예에 따르면, 클라우드 서비스 사용자와 클라우드 서비스 제공자 간의 협의된 보안 레벨을 기반으로 클라우드 서비스의 보안 위협을 평가할 수 있는 효과가 있다.
- [0022] 그리고 본 발명의 일 실시예에 따르면, 클라우드 서비스 제공자의 서비스 특성과 클라우드 서비스 사용자의 환

경 등을 고려하여 클라우드 서비스의 보안 위험을 정량적으로 평가할 수 있는 효과가 있다.

[0023] 그리고 본 발명의 일 실시예에 따르면, 클라우드 서비스의 보안 평가 결과를 기반으로 클라우드 서비스 제공자 간의 비교를 통하여 클라우드 서비스 사용자의 보안 요구사항에 가장 부합하는 클라우드 서비스 제공자를 추천해 줄 수 있는 효과가 있다.

[0024] 즉, 각 클라우드 서비스의 보안 평가 결과를 통하여 클라우드 서비스 사용자가 이용 중인 클라우드 서비스의 안전성을 보안 서비스 수준 협약을 통하여 보장함으로써, 클라우드 서비스에 대한 신뢰도를 향상시키고 클라우드 서비스 이용을 활성화할 수 있다. 또한, 객관적인 보안 평가 지표는 클라우드 서비스 제공자들의 보안 서비스에 대한 인식 제고를 통해 자발적인 보안 기술에 대한 투자 및 기술 개발을 이끌어 낼 수 있다.

[0025] 또한, 본 발명은 다음과 같은 분야에 적용이 가능하다. 첫 번째로, 안전한 클라우드 서비스 제공자의 추천 서비스를 제공할 수 있다. 클라우드 서비스 제공자의 독립적인 보안 서비스 수준 협약을 통한 보안 서비스 및 클라우드 브로커 기반의 보안 평가 서비스를 통하여 클라우드 서비스 제공자의 보안 서비스에 대하여 객관적으로 평가를 하고, 이를 바탕으로 클라우드 서비스 사용자에게 가격 대비 안전한 클라우드 제공자 추천 서비스를 제공할 수 있다. 두 번째로, 클라우드 서비스에 대한 보안 지도를 제공할 수 있다. 국내 공인 기관의 참여를 통하여 국내?외 클라우드 서비스에 대한 보안 지도를 작성하고, 이를 바탕으로 클라우드 서비스 제공자를 선택하기 위한 가이드라인을 제공할 수 있다. 세 번째로, 보안 평가 시스템 기반의 SECaaS(Security as a Service)를 제공할 수 있다. 클라우드 서비스 제공자의 보안 평가를 기반으로 사용자가 선택한 클라우드 서비스를 보다 안전하게 사용하기 위한 SECaaS 추천 서비스에 적용할 수 있다.

도면의 간단한 설명

[0026] 도1은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 브로커 기반의 보안 위험 평가 및 클라우드 서비스 제공자 추천 시스템의 구성도이다.

도 2는 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위험 평가 장치의 개략적인 구성을 보여주는 블록도이다.

도 3은 본 발명의 일 실시예에 따른 클라우드 서비스 유형에 따른 보안 위험과 관련된 보안 제어 항목의 가중치 값의 비교 결과를 나타내는 그래프이다.

도 4는 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 보안 위험을 평가하는 방법을 보여주는 흐름도이다.

도 5 및 도 6은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 클라우드 서비스 제공자를 추천하는 방법을 보여주는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 그러나 이러한 도면은 본 발명의 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 본 발명의 기술적 범위가 한정되거나 변경되는 것은 아니다. 또한 이러한 예시에 기초하여 본 발명의 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 통상의 기술자에게는 당연할 것이다.

[0028] 또한, 본 명세서에서 사용되는 용어 및 단어들은 실시예에서의 기능을 고려하여 선택된 용어들로서, 그 용어의 의미는 발명의 의도 또는 관례 등에 따라 달라질 수 있다. 따라서 후술하는 실시예에서 사용된 용어는, 본 명세서에 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우는 통상의 기술자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.

[0029] 본 발명을 설명하기에 앞서, 명세서 전반에 걸쳐 사용되는 용어들을 정의한다.

[0030] 본 발명에서 사용되는 ‘보안 서비스 수준 협약(Security Service Level Agreements)’이라 함은 클라우드 컴퓨팅 환경에서 클라우드 서비스의 보안을 서비스로 제공하기 위한 클라우드 서비스 제공자와 클라우드 서비스 사용자 간의 계약을 의미한다. 명시적으로 보안 서비스 수준의 협약이라는 명칭이 아니더라도 클라우드 서비스 제

공자와 클라우드 서비스 사용자 간에 클라우드 서비스의 보안을 서비스로 제공하기 위한 일정한 계약이 이루어진다면 이에 해당할 수 있다.

[0031]

본 발명에서 사용되는 ‘보안 위협’이라 함은 클라우드 서비스에 존재할 수 있는 여러 가지의 보안 위협을 의미한다. ‘보안 위협 벡터’라 함은 클라우드 서비스에 존재할 수 있는 여러 가지의 보안 위협들이 실제로 발생되게 만드는 물리적 방법들을 의미한다. 클라우드 서비스의 보안 위협에 대한 보고서는 NIST, Garter, CSA 등 국내·외 보안 전문기관, 관련 협회나 학계 등에서 다양한 형태로 발표되고 있다. 예를 들어, 가상화 인프라 보안 영역에서는 가상화 시스템 내부 경로를 통한 신규 악성코드 감염 및 확산, 하이퍼바이저 루트킷 등 가상화 시스템에 특화된 새로운 유형의 해킹 공격, 물리적 시스템 대비 상대적으로 보안 관리가 미흡한 가상화 환경 등이 있다. 데이터 보안 영역에서는 정보를 위탁 관리하는 클라우드 서비스 제공자에 의한 정보 유출 가능, 데이터의 물리적 위치 통제 및 데이터 유통 히스토리 파악 어려움 등이 있다. 접근 제어 영역에서는 다중 임대, 가상머신 동적 재배치로 인증 또는 접근 제어 복잡도 상승, 개인용 스마트폰 등 사용자 및 모바일 단말 접근통제 한계 등이 있다. 보안 관리 영역에서는 정보 위탁의 특징에 의해 보안 제어를 위한 위협평가 및 관리 복잡, 서비스 장애 원인의 빠른 파악과 복구 어려움, 기존 네트워크 기반 공격 및 악성코드 등에 대한 취약성, 클라우드 서비스의 SLA 기준 부족 등이 있다. 침해사고 대응 영역에서는 클라우드 침해사고시 정보 수집, 교환 및 대응에 대한 규정 부족 등이 있다. 법규 및 규제 영역에서는 정보 유출 및 손실시 책임소재 불분명, 해외서버 사용시 국내법과 해당국 법과의 상충으로 인한 분쟁 발생 가능성, 클라우드 점검을 위한 보안 점검 및 규제 항목 부재 등이 있다.

[0032]

이하에서, 본 발명의 실시예에 따른 보안 위협 평가 장치 및 평가 방법과 보안 위협 평가 결과를 이용한 클라우드 서비스 제공자 추천 방법에 대하여 하기 도면들을 참조하여 자세히 살펴본다.

[0033]

먼저, 도1은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 브로커 기반의 보안 위협 평가 및 클라우드 서비스 제공자 추천 시스템의 구성도이다.

[0034]

도1을 참조하면, 클라우드 컴퓨팅 환경에서 브로커 기반의 보안 위협 평가 및 클라우드 서비스 제공자 추천 시스템에는 클라우드 서비스 사용자(20), 클라우드 서비스 제공자(30, 40, 50) 및 브로커(10)를 포함한다. 여기서, ‘브로커(10)’라 함은 클라우드 서비스의 보안 위협을 평가하는 기능을 제공하거나, 또는 이와 함께 클라우드 서비스 사용자에게 클라우드 서비스 제공자를 추천하는 기능을 제공하는 물건을 의미한다. 즉, 브로커(10)는 복수의 클라우드 서비스 제공자 사이에서 클라우드 서비스 사용자의 요구사항에 부합하는 클라우드 서비스를 평가하고 클라우드 서비스 제공자를 중개해주는 역할로서 시스템 또는 제3의 서비스 제공자일 수 있으나, 여기에만 한정되는 것은 아니다. 이하에서, 브로커 역할을 하는 보안 위협 평가 장치에 대하여 도 2를 참고하여 상세히 설명한다.

[0035]

한편, 클라우드 서비스 사용자(20)는 이용하고자 하는 클라우드 서비스 제공자(30, 40, 50)를 직접 선택하는 것이 아니라, 브로커(10)를 통하여 보안 서비스 수준 협약(Security Service Level Agreements)을 기초로 하여 클라우드 서비스 제공자를 선택할 수 있다. 클라우드 서비스 제공자(30, 40, 50)는 브로커(10)의 보안 위협 평가를 통하여 자신의 보안 역량을 평가받고, 브로커(10)는 평가 결과를 기반으로 클라우드 서비스 사용자(20)의 보안 요구사항이 충족되는 클라우드 서비스 제공자(30, 40, 50)를 추천해 줄 수 있다.

[0036]

도 2는 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서의 보안 위협 평가 장치의 개략적인 구성을 보여주는 블록도이다.

[0037]

도 2를 참조하면, 보안 위협 평가 장치(10)는 SLA 항목 정의부(101), 발생 확률 벡터 결정부(102), 보안 제어 항목 결정부(103), 가중치 값 결정부(104), 보안 수준 값 결정부(105), 보안 위협 평가부(106) 및 클라우드 서비스 제공자 추천부(107)를 포함할 수 있다. 그리고, 도 2에 도시되어 있는 보안 위협 평가 장치(10)의 구성은 예시적인 것으로서, 보안 위협 평가 장치(10)는 도 2에 개시되어 있는 모듈들의 일부만을 구비하거나 및/또는 그 동작을 위하여 필수적인 다른 모듈들을 추가로 구비할 수도 있다.

[0038]

SLA 항목 정의부(101)는 클라우드 서비스 제공자의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의하는 기능을 제공한다. 이러한 보안 서비스 수준 협약의 항목 정의는 클라우드 서비스 사용자로부터의 입력에 기초하여 정의될 수 있다. 또는, 클라우드 브로커의 자체적인 연구 결과 또는 관련 업계 보안 전문가들과의 논의를 통해 정의할 수 있다. 예를 들어, 일반적

인 클라우드 서비스에서 서비스 수준 협약의 경우, CPU, 스토리지, 메모리 등을 서비스 수준 협약의 항목으로 이용하듯이, 보안 서비스 수준 협약의 경우 계약이나 협약을 통해 제공할 수 있는 암호화 서비스, 다중 요소 로그인 서비스 등 보안 서비스의 종류 등을 보안 서비스 수준 협약의 항목으로 이용할 수 있다. 또한, 클라우드 서비스 제공자가 요청하여 보안 서비스 수준 협약의 항목을 수정하거나 보완할 수도 있다. 예를 들어, 사용자가 온라인 스토리지 서비스를 이용하기 위하여 ‘안전한 로그인’을 SLA 항목으로 정의할 수 있다. 또는, 온라인 스토리지 서비스를 제공하는 클라우드 서비스 제공자는 ‘데이터 암호화’를 SLA 항목으로 보완하도록 요청할 수 있다. 그 결과, ‘안전한 로그인’과 ‘데이터 암호화’가 SLA 항목으로 정의될 수 있다.

[0039] 발생 확률 벡터 결정부(102)는 보안 위협에 대한 발생 확률 벡터를 결정하는 기능을 제공한다. 예를 들어, 보안 사고가 발생하였을 때의 정보를 수치화 또는 계량화한 통계값을 이용하여 발생 확률 벡터를 결정할 수 있다. 즉, 발생 확률 벡터는 보안 사고 발생 정도를 기반으로 하여 결정될 수 있다.

[0040] 보안 제어 항목 결정부(103)는 클라우드 서비스에 대한 보안 서비스를 제공하기 위해서 각 보안 서비스를 제공하기 위한 실질적인 보안 기술을 결정하는 기능을 제공한다. 이 경우에, 보안 제어 항목은 SLA 항목 정의부에 의하여 정의된 보안 서비스 수준 협약의 항목을 이용하여 결정할 수 있다. 또는 보안 서비스 수준 협약의 항목과 클라우드 서비스의 유형에 따라서 결정할 수도 있으나, 여기에만 한정되는 것은 아니다.

[0041] 여기서, ‘보안 제어 항목’이라 함은 보안 제어를 수행하는 물리적인 방법을 의미한다. 보안 제어 항목은 분류 방법에 따라 달라질 수 있다. 예를 들어, 본 발명의 실시예에서 보안 제어 항목은 ‘보안 저장(Secure Storage)’, ‘보안 처리(Secure Processing)’, ‘네트워크(Network)’, ‘접근 제어(Access Control)’, ‘감사·확인 및 준수(Audit·Verification and Compliance)’ 등으로 분류하였다.

[0042] 그리고, 보안 서비스를 제공하기 위해서는 각 보안 서비스를 제공하기 위한 실질적인 보안 기술이 결정되어야 한다. 보안 제어 항목의 각 항목은 관련 있는 보안 기술의 집합을 의미한다. 상기 예에서, 보안 제어 항목 중 ‘보안 저장(Secure Storage)’ 항목에서는 관련 있는 보안 기술로서 ‘데이터 암호화’, ‘데이터 접근 제어’ 등이 있을 수 있다.

[0043] 가중치 값 결정부(104)는 클라우드 서비스 유형에 따라 클라우드 서비스 제공자의 보안 제어 항목 간의 가중치 값을 결정하는 기능을 제공한다. 이 경우에, 클라우드 서비스 제공자의 보안 취약점을 분석한 결과를 이용하여 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 특성에 따라 보안 제어 항목 간의 가중치 값을 결정할 수 있다.

[0044] 여기서, ‘보안 제어 항목의 가중치’라 함은 보안 제어 항목 간의 상대적 중요도를 의미한다. 가중치 값은 클라우드 서비스 제공자가 결정할 수 있으나, 시장 참여자 간 논의를 통하여 결정할 수도 있고, 가중치 값의 결정 방식은 여기에만 한정되는 것은 아니다.

[0045] 한편, 가중치 값을 두는 이유는 클라우드 서비스의 유형에 따라 요구되는 보안 제어 항목이 달라질 수 있기 때문이다. 즉, 보안 제어 항목은 각 클라우드 서비스의 유형에 따른 특성에 의하여 중요도가 달라질 수 있기 때문에 보안 위협을 평가할 경우 보안 제어 항목에 포함된 보안 기술들이 가지는 의미가 달라질 수 있다. 예를 들어, 클라우드 서비스의 한 유형인 웹 기반 원격 데스크톱 서비스의 경우, 보안 저장(Secure Storage)의 가중치는 0.058, 보안 처리(Secure Processing)의 가중치는 0.124, 네트워크(Network)의 가중치는 0.417, 접근 제어(Access Control)의 가중치는 0.203, 감사·확인 및 준수(Audit·Verification and Compliance)의 가중치는 0.107로 정의할 수 있다. 즉, 웹 기반 원격 데스크톱 서비스(WebTop)의 경우 네트워크(N: Network) 항목이 중요하므로 다른 보안 제어 항목에 비해 가중치 값이 높게 정의되었다. 그리고, 각 벡터의 각 합은 1이다.

[0046] 보안 수준 값 결정부(105)는 보안 위협에 대한 클라우드 서비스 제공자의 대응 가능한 보안 제어 항목에 따라 보안 수준 값을 결정하는 기능을 제공한다. 따라서, 클라우드 서비스 제공자에 따라 보안 수준 값은 달라질 수 있다.

[0047] 여기서, ‘보안 수준 항목’이라 함은 클라우드 서비스의 보안 서비스 품질을 보장하기 위한 보안 서비스 수준 협약(Security Service Level Agreements)으로 보안 수준을 수치로 결정할 수 있는 세부 항목을 의미한다. 본 발명의 실시예에서 보안 수준은 표 1과 같은 항목에 의해 결정되나, 보안 수준을 결정하기 위한 항목은 다양한 형태로 구성될 수 있으며, 보안 수준 결정 방법론 또한 다양하게 적용 가능하다.

표 1

보안 수준 항목	내용
접근성(Access Vector : AV)	서비스 네트워크 접근성 (공용, 사설, 권한 관리 등)
접근 복잡성 (Access Complexity : AC)	서비스 시스템 접근성 (시스템 접근을 위해 추가적인 정보 필요 여부)
인증(Authentication : AU)	인증의 복잡성 (서비스 접근을 위한 인증의 복잡성)
기밀성(Confidentiality : C)	기밀성 보장 여부 (암호화 기술 적용 여부 등)
무결성(Integrity : I)	무결성 보장 여부 (메시지 인증 코드 사용 여부 등)
가용성(Availability : A)	가용성 보장 (백업 서버, Replica 존재 여부 등)

[0048]

[0049]

예를 들어, 상기 표 1의 ‘인증의 복잡성’ 항목으로 ‘안전한 로그인’이라는 보안 서비스 수준 협약의 항목이 존재하고, 안전한 로그인에 대한 보안 제어 항목은 클라우드 브로커에서 (접근 제어, 감사)라고 정의되어 있다고 가정하면, (안전한 로그인)={ (접근 제어, 감사), (클라우드 서비스 제공자의 보안 수준)}으로 안전한 로그인에 대한 보안 서비스 수준이 결정될 수 있다. 그리고, 클라우드 브로커에서 (접근 제어, 감사)라는 보안 제어 항목에 대하여, (접근 제어, 감사)={ (아이디, 패스워드)=0.1, (일회용 패스워드(OTP, One Time Password))=0.3, (다중 접근 제어)=0.7}이라고 보안 기술별로 보안 수준이 결정되어 있다고 가정하면, 임의의 클라우드 서비스 제공자 A가 (접근제어, 감사)라는 보안 제어 항목에 대하여 현재 클라우드 서비스 제공자 A가 제공하는 서비스에 적용된 기술이 오직 ‘아이디, 패스워드’ 라면, 클라우드 서비스 제공자 A가 클라우드 서비스 사용자에게 제공할 수 있는 보안 수준은 0.1로 결정될 수 있다.

[0050]

(안전한 로그인)클라우드 서비스 제공자A={ (접근 제어, 감사), 0.1}

[0051]

한편, 보안 수준 값을 결정하기 위하여 클라우드 서비스 제공자의 보안 취약점 분석결과를 이용할 수 있다. 즉, 하나 이상의 보안 제어 항목을 이용하여 현재 클라우드 서비스 제공자가 보유한 보안 기술로 클라우드 서비스의 보안 위협을 통제할 수 있는지 여부를 평가하여, 클라우드 서비스 제공자가 기본적으로 제공할 수 있는 보안 수준을 분석한다. 이는 각 클라우드 서비스 제공자가 자체적으로 분석할 수 있고, 클라우드 브로커를 통하여 분석할 수도 있으나, 여기에만 한정되는 것은 아니다. 예를 들어, 클라우드 브로커와 시장 참여자나 클라우드 서비스 제공자들 간에 협의를 통하여 결정된 보안 위협에 대하여 각 클라우드 서비스 제공자들에게 해당되는 보안 위협들에 대하여 클라우드 서비스 제공자가 현재 보유한 기술로 통제가능한지 여부 등을 평가하여, 각 클라우드 서비스 제공자가 기본적으로 제공할 수 있는 보안 수준을 분석한다.

[0052] 보안 위험 평가부(106)는 보안 위협에 대한 보안 위험을 평가하는 기능을 제공한다. 보안 위험을 평가하는 방법은 이하에서 자세히 설명한다.

[0053] 클라우드 서비스 제공자 추천부(107)는 클라우드 서비스 사용자가 이용하고자 하는 클라우드 서비스를 선택하고 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 작성하여 협상을 요청하면, 클라우드 서비스 사용자의 요구사항에 부합하는 정도에 따라 이용 가능한 클라우드 서비스 제공자를 판단하여 결과를 전송하는 기능을 제공한다.

[0054] 이하, 본 발명의 실시예에 따른 보안 위험 평가부(106)에서 제공하는 보안 위험을 평가하는 방법에 관하여 구체적으로 설명한다.

수학식 1

$$SR_T = P_T \times [W]_S \times [V]_T$$

[0055]

[0056] 수학식 1은 보안 위협에 대한 보안 위험 평가(Security Risk Assessment)를 나타낸다.

[0057] SR_T 는 위협 T에 대한 보안 위험으로, 보안 위험은 다양한 연구 결과 및 시장 참여자의 논의에 따라 그 종류가 결정될 수 있다. P_T 는 위협 T에 대한 발생 확률 벡터로서, 보안 사고 발생 정도를 기반으로 하여 결정될 수 있다.

[0058] $[W]_S$ 는 클라우드 서비스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목의 가중치 벡터로서, 클라우드 서비스의 유형 즉, 클라우드 서비스의 유형에 따른 특성에 의하여 가중치가 달라질 수 있다. 예를 들어, 클라우드 서비스의 한 유형인 가상 데스크톱 서비스는 보안 사고 위험을 줄이기 위하여, 저장되는 파일의 암호화 보안보다 네트워크 보안이 더 중요할 수 있고, 이 경우에 네트워크 보안의 가중치 값이 파일의 암호화 보안의 가중치 값보다 더 큰 값을 가지게 된다.

[0059] $[V]_T$ 는 위협 T에 대한 평가 대상의 보안 위험 벡터로서, 보안 위험 벡터는 클라우드 브로커에서 정의된 보안 위협 및 관련된 보안 제어 항목으로부터 결정될 수 있다. 예를 들어, 접근 제어 위협은 클라우드 서비스 제공자의 관련 보안 제어 항목 충족 정도에 따라 결정될 수 있다.

[0060] 상기 보안 위험 평가는 사전에 정의된 보안 위협의 종류에 따라 결정되며, 상기 벡터의 각 합은 1이다. 위협 T에 대한 클라우드 서비스 제공자의 보안 위험 벡터는 위협 T에 대하여 클라우드 서비스 제공자의 대응 가능한 보안 제어 항목에 따라 보안 수준(Security-Level)이 결정된다.

[0061] 상기 보안 수준은 사전에 정의된 최고 보안 수준 대비 클라우드 서비스 제공자의 보안 위험 벡터로 결정될 수 있으며, 사용자 보안 요구 수준 대비 서비스 제공자의 보안 수준의 차이가 보안 위협 T에 대한 사용자 측면의 보안 위험 벡터로 결정될 수 있다. 따라서, 클라우드 서비스 제공자에 따른 보안 수준에 따라 사용자 측면의 보안 위험 벡터가 달라질 수 있다.

수학식 2

$$P_T = [T_1, T_2, T_3, T_4, T_5]_T$$

[0062]

$$=[0.111, 0.362, 0.036, 0.086, 0.277, 0.036, 0.094]$$

수학식 2는 보안 위협 발생 확률 벡터를 나타낸다.

상기 보안 위협 발생 확률은 공개된 보안사고 결과를 토대로 도출한 실시예이다. 예를 들어, 보안 위협 T에 대하여 보안 위협 발생 확률 벡터가 T₁, T₂, T₃, T₄, T₅, T₆, T₇이 있다고 하면, 보안 위협 T₁에 대한 발생 확률은 0.111, 보안 위협 T₂에 대한 발생 확률은 0.362, 보안 위협 T₃에 대한 발생 확률은 0.036, 보안 위협 T₄에 대한 발생 확률은 0.086, 보안 위협 T₅에 대한 발생 확률은 0.277, 보안 위협 T₆에 대한 발생 확률은 0.036, 보안 위협 T₇에 대한 발생 확률은 0.094라고 할 수 있다. 그리고, 보안 위협 발생 확률 벡터의 각 합은 1이다.

수학식 3

$$[W]_S = [S, P, N, AC, AU]_S$$

수학식 3은 클라우드 서비스 S에 대하여 보안 위협 T와 관련된 보안 제어 항목의 가중치 벡터를 나타낸다.

실시예에서 사용한 보안 제어 항목은 보안 저장(S: Secure Storage), 보안 처리(P: Secure Processing), 네트워크(N: Network), 접근 제어(AC: Access Control), 감사·확인 및 준수(AU: Audit·Verification and Compliance)이며, 클라우드 서비스 타입은 웹 기반 원격 데스크톱 서비스(WebTop), 온라인 스토리지 서비스(Storage), 웹 기반 응용 프로그램 서비스(WebApp)로 구분하였다. 실시예와 같이 각 클라우드 서비스는 각 클라우드 서비스의 유형에 따른 특성에 의하여 가중치 값이 달라질 수 있다.

수학식 4

$$W_{Webtop} = [0.058, 0.124, 0.417, 0.203, 0.107]_{Webtop}$$

$$W_{Storage} = [0.442, 0.234, 0.124, 0.131, 0.069]_{Storage}$$

$$W_{WebApp} = [0.174, 0.058, 0.103, 0.460, 0.206]_{WebApp}$$

수학식 4는 수학식 3의 실시예를 사용하여 결정된 클라우드 서비스 각각에 대하여 보안 위협과 관련된 보안 제어 항목의 가중치 벡터를 나타낸다.

실시예에서, 웹 기반 원격 데스크톱 서비스(WebTop)의 경우, 보안 저장(S: Secure Storage)의 가중치 값은 0.058, 보안 처리(P: Secure Processing)의 가중치 값은 0.124, 네트워크(N: Network)의 가중치 값은 0.417, 접근 제어(AC: Access Control)의 가중치 값은 0.203, 감사·확인 및 준수(AU: Audit·Verification and Compliance)의 가중치 값은 0.107이라고 정의할 수 있다.

또는, 온라인 스토리지 서비스(Storage)의 경우, 보안 저장(S: Secure Storage)의 가중치 값은 0.442, 보안 처리(P: Secure Processing)의 가중치 값은 0.234, 네트워크(N: Network)의 가중치 값은 0.124, 접근 제어(AC:

Access Control)의 가중치 값은 0.131, 감사·확인 및 준수(AU: Audit·Verification and Compliance)의 가중치 값은 0.069이라고 정의할 수 있다.

[0075] 또는, 웹 기반 응용 프로그램 서비스(WebApp)의 경우, 보안 저장(S: Secure Storage)의 가중치 값은 0.174, 보안 처리(P: Secure Processing)의 가중치 값은 0.058, 네트워크(N: Network)의 가중치 값은 0.103, 접근 제어(AC: Access Control)의 가중치 값은 0.460, 감사·확인 및 준수(AU: Audit·Verification and Compliance)의 가중치 값은 0.206이라고 정의할 수 있다.

[0076] 즉, 웹 기반 원격 데스크톱 서비스(WebTop)의 경우 네트워크(N: Network) 항목이, 온라인 스토리지 서비스(Storage)의 경우 보안 저장(S: Secure Storage) 항목이, 웹 기반 응용 프로그램 서비스(WebApp)의 경우 접근 제어(AC: Access Control) 항목이 중요하므로 가중치 값을 높게 정의할 수 있다. 그리고, 각 벡터의 각 합은 1이다.

[0077] 도 3은 본 발명의 일 실시예에 따른 클라우드 서비스 유형에 따른 보안 위협과 관련된 보안 제어 항목의 가중치 값의 비교 결과를 나타내는 그래프이다.

[0078] 도3을 참조하면, 본 발명의 일 실시예에 따라, 웹 기반 원격 데스크톱 서비스(WebTop)의 경우 네트워크(N: Network)를 위한 보안 제어 항목의 가중치 값이 가장 높고, 온라인 스토리지 서비스(Storage)의 경우 보안 저장(S: Secure Storage)을 위한 보안 제어 항목의 가중치 값이 가장 높으며, 웹 기반 응용 프로그램 서비스(WebApp)의 경우 접근 제어(AC: Access Control)를 위한 보안 제어 항목의 가중치 값이 가장 높다.

수학식 5

$$[V]_T = [S_{<L,T>}, P_{<L,T>}, N_{<L,T>}, AC_{<L,T>}, AU_{<L,T>}]_T$$

[0079]

[0080] 수학식 5는 보안 위협 T에 대한 보안 위협 벡터를 나타낸다.

[0081] 본 실시예에서, 보안 제어 항목을 보안 저장(S: Secure Storage), 보안 처리(P: Secure Processing), 네트워크(N: Network), 접근 제어(AC: Access Control), 감사·확인 및 준수(AU: Audit·Verification and Compliance)이라고 결정하였다. 따라서, $S_{<L,T>}$ 는 위협 T와 관련하여 클라우드 서비스 제공자의 보안 저장(S: Secure Storage)을 위한 보안 제어 항목의 보안 수준(Security-Level) 값을 의미한다. $P_{<L,T>}$ 는 위협 T와 관련하여 클라우드 서비스 제공자의 보안 처리(P: Secure Processing)를 위한 보안 제어 항목의 보안 수준(Security-Level) 값을 의미한다. $N_{<L,T>}$ 는 위협 T와 관련하여 클라우드 서비스 제공자의 네트워크(N: Network)를 위한 보안 제어 항목의 보안 수준(Security-Level) 값을 의미한다. $AC_{<L,T>}$ 는 위협 T와 관련하여 클라우드 서비스 제공자의 접근 제어(AC: Access Control)를 위한 보안 제어 항목의 보안 수준(Security-Level) 값을 의미한다. $AU_{<L,T>}$ 는 위협 T와 관련하여 클라우드 서비스 제공자의 감사·확인 및 준수(AU: Audit·Verification and Compliance)를 위한 보안 제어 항목의 보안 수준(Security Level) 값을 의미한다. 즉, 사전에 분류된 보안 제어 항목에 대하여 보안 위협 별로 보안 수준(Security Level)을 결정하게 된다.

[0082] 상기 보안 위협별 보안 수준에 대하여 관련 보안 제어 항목의 최고 보안 수준 대비 서비스 제공자의 보안 수준을 평가하는 경우, 서비스 제공자 보안 위협 벡터가 결정되며, 사용자 요구 보안 수준 대비 서비스 제공자의 보안 수준을 평가하는 경우, 사용자 측면의 보안 위협 벡터가 결정된다.

수학식 6

$$SR_{total} = \sum_T^n P_T \times [W]_S \times [V]_T$$

수학식 6은 최종 보안 위험 평가를 산출하는 수학식을 나타낸다.

클라우드 서비스에 대한 보안 위험 평가는 상기 보안 위험에 대한 보안 위험 평가의 합산을 통해 계산할 수 있다. 상기 보안 위험 평가의 합산시 보안 위험 평가 목적과 대상(예를 들어, 사용자 요구 보안 수준 존재 여부, 보안 위험 평가 대상, 단순 보안 수준 비교 혹은 서비스 추천 등)에 따라 보안 위험 벡터를 결정하고 평가를 수행할 수 있다.

도 4는 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 보안 위험을 평가하는 방법을 보여주는 흐름도이다. 본 발명의 실시예를 포함하여 이하에서 설명되는 절차는 다양한 형태로 구현하는 것이 가능하다.

도 4를 참조하면, 먼저 클라우드 서비스의 보안 서비스 품질(Quality of Service) 보장을 위한 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 정의한다(S401). 이러한 보안 서비스 수준 협약의 항목 정의는 클라우드 서비스 사용자로부터의 입력에 기초하여 정의될 수 있다. 또는, 클라우드 브로커의 자체적인 연구 결과 또는 관련 업계 보안 전문가들과의 논의를 통해 정의할 수 있다. 예를 들어, 일반적인 클라우드 서비스에서 서비스 수준 협약의 경우, CPU, 스토리지, 메모리 등을 서비스 수준 협약의 항목으로 이용하듯이, 보안 서비스 수준 협약의 경우 계약이나 협약을 통해 제공할 수 있는 암호화 서비스, 다중 요소 로그인 서비스 등 보안 서비스의 종류 등을 보안 서비스 수준 협약의 항목으로 이용할 수 있다. 또한, 클라우드 서비스 제공자가 요청하여 보안 서비스 수준 협약의 항목을 수정하거나 보완할 수도 있다. 예를 들어, 사용자가 온라인 스토리지 서비스를 이용하기 위하여 ‘안전한 로그인’을 SLA 항목으로 정의할 수 있다. 또는, 온라인 스토리지 서비스를 제공하는 클라우드 서비스 제공자는 ‘데이터 암호화’를 SLA 항목으로 보완하도록 요청할 수 있다. 그 결과, ‘안전한 로그인’과 ‘데이터 암호화’가 SLA 항목으로 정의될 수 있다.

다음으로, 보안 위험에 대한 발생 확률 벡터를 결정한다(S402). 여기서, ‘발생 확률 벡터를 결정’한다는 것은 예를 들어 보안 사고가 발생하였을 때의 정보를 수치화 또는 계량화한 통계값을 이용하여 발생 확률 벡터를 결정하는 것을 의미할 수 있다. 즉, 발생 확률 벡터는 보안 사고 발생 정도를 기반으로 하여 결정될 수 있다.

다음으로, 클라우드 서비스와 관련한 보안 제어 항목을 결정한다(S403). 여기서, ‘보안 제어 항목을 결정’한다는 것은 클라우드 서비스에 대한 보안 서비스를 제공하기 위해서 각 보안 서비스를 제공하기 위한 실질적인 보안 기술을 결정하는 것을 의미한다. 이 경우에, 보안 제어 항목은 SLA 항목 정의부에 의하여 정의된 보안 서비스 수준 협약(Security Service Level Agreements)의 항목을 이용하여 결정할 수 있다. 또는 보안 서비스 수준 협약의 항목과 클라우드 서비스의 유형에 따라서 결정할 수도 있으나, 여기에만 한정되는 것은 아니다. 보안 제어 항목에 대해서는 앞에서 도 2을 참고하여 상세히 설명하였다.

다음으로, 클라우드 서비스 유형에 따라 클라우드 서비스 제공자의 보안 제어 항목 간의 가중치 값을 결정한다(S404). 이 경우에, 클라우드 서비스 제공자의 보안 취약점을 분석한 결과를 이용하여 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 특성에 따라 보안 제어 항목 간의 가중치 값을 결정할 수 있다. 여기서, ‘보안 제어 항목의 가중치’라 함은 보안 제어 항목 간의 상대적 중요도를 의미한다. 가중치 값은 클라우드 서비스 제공자가 결정할 수 있으나, 시장 참여자 간 논의를 통하여 결정할 수도 있고, 가중치 값의 결정 방식은 여기에만 한정되는 것은 아니다.

한편, 가중치 값을 두는 이유는 클라우드 서비스의 유형에 따라 요구되는 보안 제어 항목이 달라질 수 있기 때문이다. 즉, 보안 제어 항목은 각 클라우드 서비스의 유형에 따른 특성에 의하여 중요도가 달라질 수 있기 때문에 보안 위험을 평가할 경우 보안 제어 항목에 포함된 보안 기술들이 가지는 의미가 달라질 수 있다. 예를 들어, 클라우드 서비스의 한 유형인 웹 기반 원격 데스크톱 서비스의 경우, 보안 저장(Secure Storage)의 가중치는 0.058, 보안 처리(Secure Processing)의 가중치는 0.124, 네트워크(Network)의 가중치는 0.417, 접근 제어(Access Control)의 가중치는 0.203, 감사·확인 및 준수(Audit·Verification and Compliance)의 가중치는

0.107로 정의할 수 있다. 즉, 웹 기반 원격 데스크톱 서비스(WebTop)의 경우 네트워크(N: Network) 항목이 중요하므로 다른 보안 제어 항목에 비해 가중치 값이 높게 정의되었다. 그리고, 각 벡터의 각 함은 1이다.

[0092]

다음으로, 보안 위협에 대한 클라우드 서비스 제공자의 대응 가능한 보안 제어 항목에 따라 보안 수준 값을 결정한다(S405). 따라서, 클라우드 서비스 제공자에 따라 보안 수준 값은 달라질 수 있다. 여기서, '보안 수준 항목'이라 함은 클라우드 서비스의 보안 서비스 품질을 보장하기 위한 보안 서비스 수준 협약(Security Service Level Agreements)으로 보안 수준을 수치로 결정할 수 있는 세부 항목을 의미한다. 본 발명의 실시예에서 보안 수준은 표 1과 같은 항목에 의해 결정되나, 보안 수준을 결정하기 위한 항목은 다양한 형태로 구성될 수 있으며, 보안 수준 결정 방법론 또한 다양하게 적용 가능하다. 보안 수준 값에 대해서는 앞에서 도 2을 참고하여 상세히 설명하였다.

[0093]

다음으로, 결정된 발생 확률 벡터, 보안 제어 항목, 가중치 값, 보안 수준 값을 이용하여 클라우드 서비스 제공자가 제공하는 클라우드 서비스의 보안 위협에 대한 보안 위험을 평가한다(S406). 보안 위험을 평가하는 방법에도 도 2을 참조하여 설명한 사항들이 동일하게 적용될 수 있다. 따라서 불필요한 반복을 피하기 위하여 보안 위험 평가 방법에 관하여 설명을 생략한다.

[0094]

도 5 및 도 6은 본 발명의 일 실시예에 따른 클라우드 컴퓨팅 환경에서 클라우드 서비스 제공자를 추천하는 방법을 보여주는 흐름도이다.

[0095]

도 5를 참조하면, 먼저 클라우드 서비스 사용자는 이용하고자 하는 클라우드 서비스의 유형과 클라우드 서비스의 보안 서비스 수준 협약(Security Service Level Agreements)을 위한 보안 요구사항을 작성하여 클라우드 브로커에게 협상을 요청메시지를 전송한다(S501).

[0096]

다음으로, 클라우드 브로커는 클라우드 서비스의 보안 서비스 수준 협약의 보안 요구사항을 참고하여 클라우드 서비스 사용자의 요구사항에 부합하는 정도에 따라 이용 가능한 클라우드 서비스 제공자를 판단한다(S502). 클라우드 서비스 사용자가 이용 가능한 클라우드 서비스 제공자를 판단하는 방법은 클라우드 서비스 사용자의 요구사항과 일치하거나 근접하는 클라우드 서비스 제공자를 보안 위험 평가 결과를 기초로 하여 판단할 수 있다.

[0097]

다음으로, 판단한 결과를 클라우드 서비스 사용자에게 전송한다(S503).

[0098]

다음으로, 클라우드 서비스 사용자가 전송받은 클라우드 서비스 제공자 중에서 클라우드 서비스 제공자를 선택하면 단계를 종료하고, 클라우드 서비스 사용자는 클라우드 브로커의 협상 결과를 만족하지 못하는 경우 클라우드 브로커에게 재협상을 요청할 수 있다(S504). 이 경우에 다시 클라우드 브로커는 사용자의 보안 요구사항에 부합하는 정도에 따라 이용 가능한 클라우드 서비스 제공자를 판단한다.

[0099]

본 발명의 일 양상은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현될 수 있다. 상기의 프로그램을 구현하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 디스크 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드로 저장되고 실행될 수 있다.

[0100]

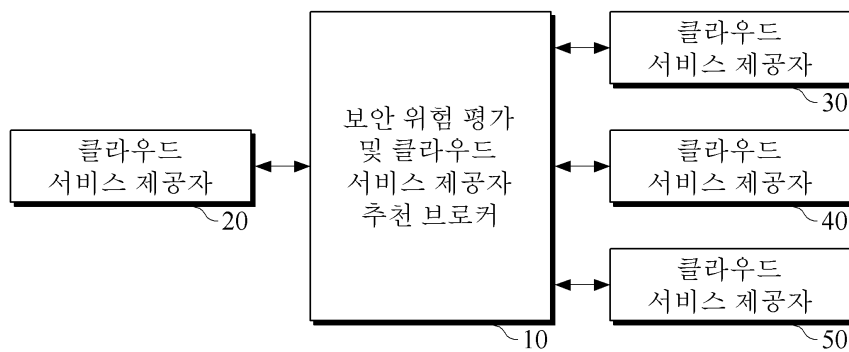
이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위 내에서 다양한 수정, 변경 및 치환이 가능할 것이다. 따라서, 본 발명에 개시된 실시예 및 첨부된 도면들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예 및 첨부된 도면에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

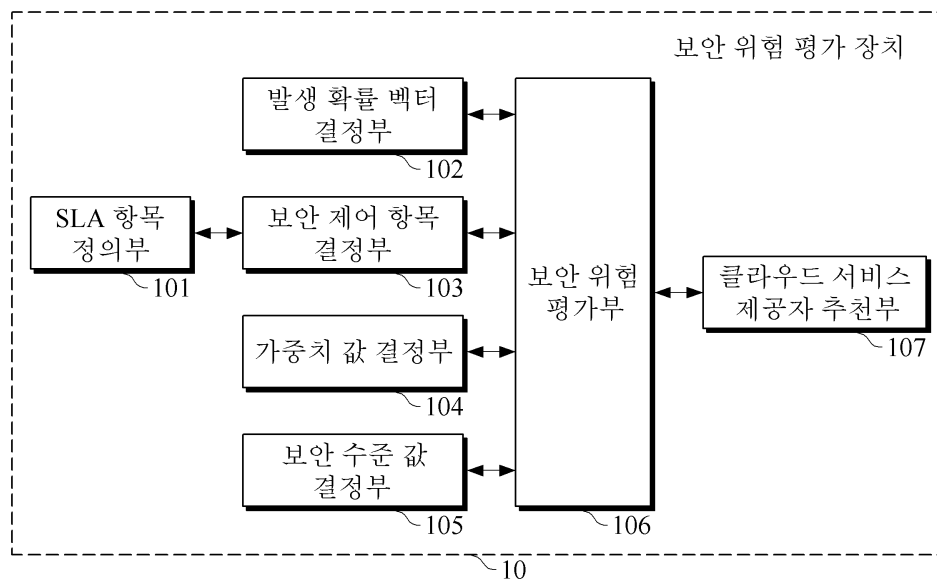
- [0101]
- 10 : 보안 위험 평가 및 클라우드 서비스 제공자 추천 브로커 장치
 - 20 : 클라우드 서비스 사용자
 - 30, 40, 50 : 클라우드 서비스 제공자
 - 101 : SLA 항목 정의부
 - 102 : 발생 확률 벡터 결정부
 - 103 : 보안 제어 항목 결정부
 - 104 : 가중치 값 결정부
 - 105 : 보안 수준 값 결정부
 - 106 : 보안 위험 평가부
 - 107 : 클라우드 서비스 제공자 추천부

도면

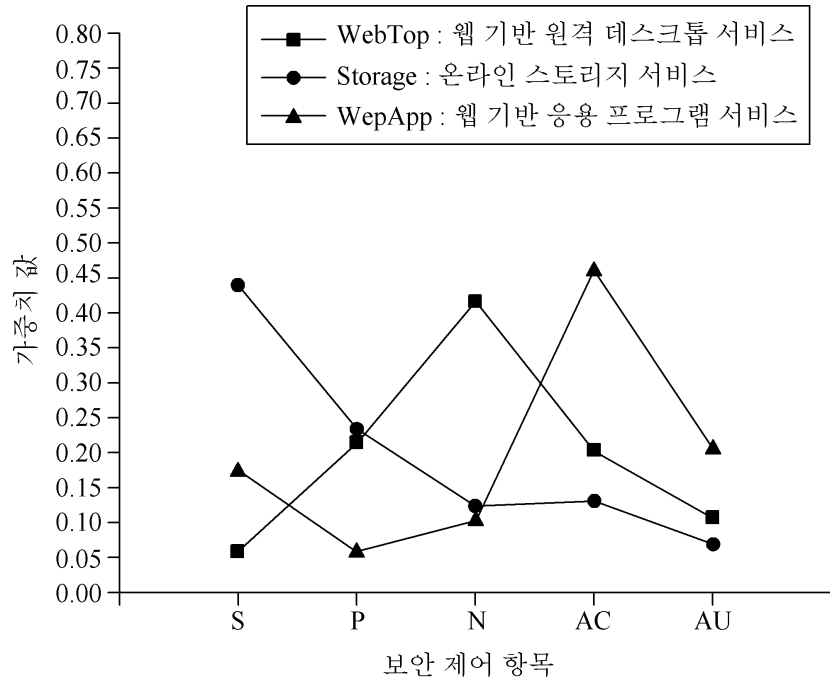
도면1



도면2

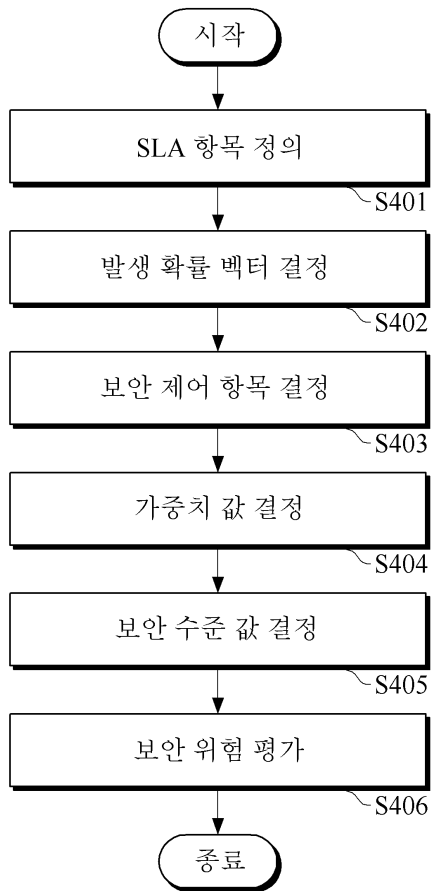


도면3

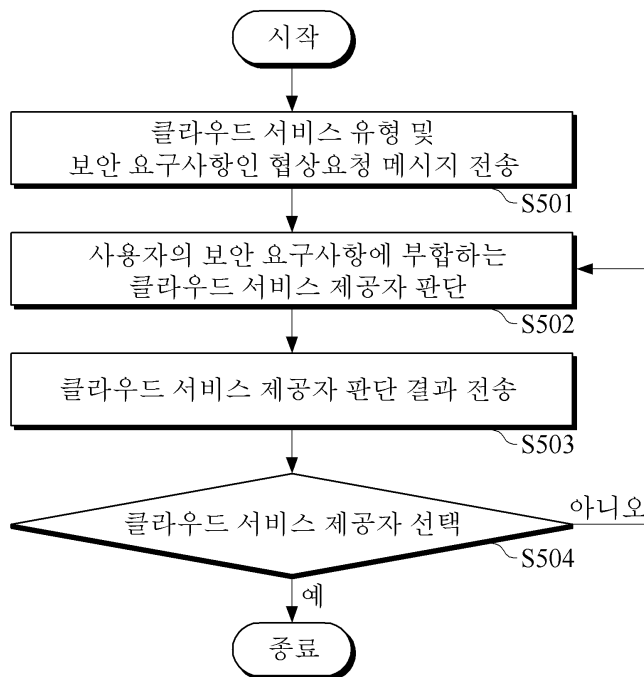


S : 보안 저장(Secure Storage)
P : 보안 처리(Secure Processing)
N : 네트워크(Network)
AC : 접근 제어(Access Control)
AU : 감사·확인 및 준수(Audit·Verification and Compliance)

도면4



도면5



도면6

