(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0121459
(43) 공개일자 2018년11월07일

(51) 국제특허분류(Int. Cl.)
G06Q 10/06 (2012.01) *G06F 21/57* (2013.01)
G06Q 10/04 (2012.01)
(52) CPC특허분류
G06Q 10/0631 (2013.01)
G06F 21/577 (2013.01)
(21) 출원번호 10-2018-0131734(분할)
(22) 출원일자 2018년10월31일
심사청구일자 2018년10월31일
(62) 원출원 특허 10-2017-0037575
원출원일자 2017년03월24일
심사청구일자 2017년03월24일
(30) 우선권주장
1020160169213 2016년12월13일 대한민국(KR)

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
허의남
경기도 용인시 수지구 성복2로 251, 209동 404호 (성복동, 버들치마을 성복자이2차)
나상호
경기도 용인시 기흥구 서천동로 60, 405동 103호 (서천동, 서천마을4단지)
박준영
경기도 용인시 기흥구 덕영대로 1732, 전자정보대학 331호 (서천동, 경희대학교 국제캠퍼스)
(74) 대리인
특허법인도담

전체 청구항 수 : 총 16 항

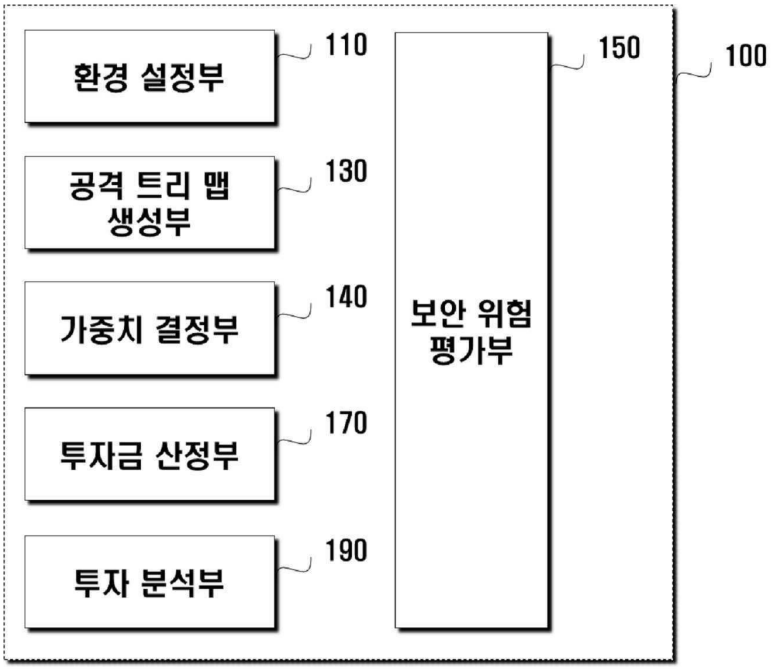
(54) 발명의 명칭 **보안 위험 평가 기반 보안 투자 방법 및 장치**

(57) 요 약

본 발명은 보안 투자 방법 및 장치에 관한 것으로, 보다 자세하게는 클라우드 컴퓨팅 환경에서의 보안 위험 평가를 기반으로 한 보안 투자 방법 및 장치에 관한 것이다. 본 발명은 보안 위험 평가 기반 보안 투자 방법에 있어서, 클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협 및 각 보안

(뒷면에 계속)

대 표 도 - 도1



위협의 단계별 취약점을 설정하는 단계, 하나의 보안 위협을 구성하는 상기 세부 공격 단계별 취약점을 계층적으로 연결하고, 제1 보안 위협 및 제2 보안 위협에 포함된 취약점이 동일한 경우, 동일한 취약점을 하나의 취약점 노드로 단일화하며, 단일화된 취약점 노드로 상기 제1 보안 위협 및 상기 제2 보안 위협을 연결하여 공격 트리 맵을 생성하는 단계, 상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭하는 단계, 상기 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하는 단계, 상기 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적으로 평가하는 단계를 포함하는 것을 일 특징으로 한다. 본 발명에 의하면, 클라우드 환경에서 발생할 수 있는 보안 위협의 공격 단계를 고려하여 보안 위험을 평가함으로써, 중복되는 공격에 대한 이중 평가를 배제하여 보다 정확한 보안 평가를 수행할 수 있다.

(52) CPC특허분류
G06Q 10/04 (2013.01)
G06Q 10/0637 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711035224
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성
연구과제명 실시간 모바일 클라우드 서비스 플랫폼 연구개발
기 여 율 1/1
주관기관 경희대학교 산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협과 상기 보안 위협을 발생시키는 세부 공격 각각에서의 단계별 취약점을 설정하는 단계;

하나의 보안 위협을 구성하는 상기 세부 공격 단계별 취약점을 계층적으로 연결하고, 제1 보안 위협 및 제2 보안 위협에 포함된 취약점이 동일한 경우, 동일한 취약점을 하나의 취약점 노드로 단일화하며, 단일화된 취약점 노드로 상기 제1 보안 위협 및 상기 제2 보안 위협을 연결하여 공격 트리 맵을 생성하는 단계;

상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭하는 단계;

상기 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하는 단계;

상기 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적으로 평가하는 단계를 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 2

제1항에 있어서,

상기 클라우드 서비스 유형에 따라 상기 보안 제어 항목 별 가중치를 결정하는 단계를 더 포함하고,

상기 보안 위험을 정량적으로 평가하는 단계는 상기 보안 제어 항목별로 합산한 취약 점수에 상기 보안 제어 항목의 가중치를 반영하여 상기 보안 위험을 정량적으로 평가하는 단계를 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 3

제1항에 있어서,

임의의 보안 제어 항목 SC_i에 투자 시 상기 보안 제어 항목 SC_i에 대응하는 하나 이상의 투자 취약점의 보안 취약 완화 비율을 결정하는 단계;

상기 투자 취약점 노드의 자식 노드 구조 및 상관도, 상기 투자에 대응하는 투자 금액 및 상기 투자 취약점의 보안 취약 완화 비율을 이용하여 상기 투자 취약점 노드 각각의 완화된 취약 점수를 산출하는 단계;

상기 보안 제어 항목별로 상기 완화된 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 투자 후 보안 위험을 정량적으로 평가하는 단계를 더 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 4

제3항에 있어서,

상기 완화된 취약 점수 산출 단계는

상기 투자 금액이 z_i이면, 상기 투자 취약점 노드 v_{xy}의 완화된 취약 점수 $M(z_i, v_{xy})$는 하기 식에 의하여 산출되며, α 및 β는 기 설정된 상수인 보안 위험 평가 기반 보안 투자 방법.

$$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}$$

청구항 5

제3항에 있어서,

상기 투자 후 보안 위험을 정량적으로 평가한 값이 최소가 되도록 상기 보안 제어 항목별 투자 금액을 산정하는 단계를 더 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 6

제5항에 있어서,

상기 투자 금액 산정 단계는 라그랑지 승수법을 이용하여 이루어지는 보안 위험 평가 기반 보안 투자 방법.

청구항 7

제1항에 있어서,

상기 취약점 노드 각각의 취약 점수를 산출하는 단계는,

임의의 제 1 취약점 노드의 하나 이상의 제 1 자식 노드가 상호 독립적이면, 제 1 자식 노드의 취약 점수와 기 설정된 상기 제 1 자식 노드 - 취약점 노드 간 상관계수의 곱을 합산하여 상기 제 1 취약점 노드의 취약 점수를 산출하는 단계를 포함하며,

임의의 제 2 취약점 노드의 하나 이상의 제 2 자식 노드가 상호 AND 조건 관계이면, 제 2 자식 노드의 취약 점수와 기 설정된 상기 제 2 자식 노드- 취약점 노드 간 상관계수의 곱을 합산한 값을 상기 제 2 자식 노드의 수로 나누어 상기 제 2 취약점 노드의 취약 점수를 산출하는 단계를 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 8

제1항에 있어서,

상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사확인 및 준수(AuditVerification and Compliance) 중 적어도 하나를 포함하는 보안 위험 평가 기반 보안 투자 방법.

청구항 9

클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협과 상기 보안 위협을 발생시키는 세부 공격 각각에서의 단계별 취약점을 설정하는 환경 설정부;

하나의 보안 위협을 구성하는 상기 세부 공격 단계별 취약점을 계층적으로 연결하고, 제1 보안 위협 및 제2 보안 위협에 포함된 취약점이 동일한 경우, 동일한 취약점을 하나의 취약점 노드로 단일화하며, 단일화된 취약점 노드로 상기 제1 보안 위협 및 상기 제2 보안 위협을 연결하여 공격 트리 맵을 생성하고, 상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭하는 공격 트리 맵 생성부;

상기 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하고, 상기 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적

으로 평가하는 보안 위험 평가부를 포함하는 보안 위험 평가 기반 보안 투자 장치.

청구항 10

제9항에 있어서,

상기 클라우드 서비스 유형에 따라 상기 보안 제어 항목 별 가중치를 결정하는 가중치 결정부를 더 포함하고,

상기 보안 위험 평가부는

상기 보안 제어 항목별로 합산한 취약 점수에 상기 보안 제어 항목의 가중치를 반영하여 상기 보안 위험을 정량적으로 평가하는 보안 위험 평가 기반 보안 투자 장치.

청구항 11

제9항에 있어서,

상기 환경 설정부는

임의의 보안 제어 항목 SC_i에 투자 시, 상기 보안 제어 항목 SC_i에 대응하는 하나 이상의 제 1 취약점의 보안 취약 완화 비율을 결정하고,

상기 보안 위험 평가부는

상기 제 1 취약점 노드의 자식 노드 구조 및 상관도, 상기 투자에 대응하는 투자 금액 및 상기 제 1 취약점의 보안 취약 완화 비율을 이용하여 상기 제 1 취약점 노드 각각의 완화된 취약 점수를 산출하며, 상기 보안 제어 항목별로 상기 완화된 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 투자 후 보안 위험을 정량적으로 평가하는 보안 위험 평가 기반 보안 투자 장치.

청구항 12

제11항에 있어서,

상기 보안 위험 평가부는

상기 투자 금액이 z_i이면, 상기 제 1 취약점 노드 v_{xy}의 완화된 취약 점수 $M(z_i, v_{xy})$를 하기 식에 따라 산출하며, α 및 β는 기 설정된 상수인 보안 위험 평가 기반 보안 투자 장치.

$$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}$$

청구항 13

제11항에 있어서,

상기 투자 후 보안 위험을 정량적으로 평가한 값이 최소가 되도록 상기 보안 제어 항목별 투자 금액을 산정하는 투자금 산정부를 더 포함하는 보안 위험 평가 기반 보안 투자 장치.

청구항 14

제13항에 있어서,

상기 투자금 산정부는 라그랑지 승수법을 이용하여 투자 금액을 산정하는 보안 위험 평가 기반 보안 투자 장치.

청구항 15

제9항에 있어서,

상기 보안 위험 평가부는

임의의 제 1 취약점 노드의 하나 이상의 제 1 자식 노드가 상호 독립적이면, 제 1 자식 노드의 취약 점수와 기 설정된 상기 제 1 자식 노드 - 취약점 노드 간 상관계수의 곱을 합산하여 상기 제 1 취약점 노드의 취약 점수를 산출하며,

임의의 제 2 취약점 노드의 하나 이상의 제 2 자식 노드가 상호 AND 조건 관계이면, 제 2 자식 노드의 취약 점수와 기 설정된 상기 제 2 자식 노드- 취약점 노드 간 상관계수의 곱을 합산한 값을 상기 제 2 자식 노드의 수로 나누어 상기 제 2 취약점 노드의 취약 점수를 산출하는 보안 위험 평가 기반 보안 투자 장치.

청구항 16

제9항에 있어서,

상기 보안 제어 항목은 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사확인 및 준수(AuditVerification and Compliance) 중 적어도 하나를 포함하는 보안 위험 평가 기반 보안 투자 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 투자 방법 및 장치에 관한 것으로, 보다 자세하게는 클라우드 컴퓨팅 환경에서의 보안 위험 평가를 기반으로 한 보안 투자 방법 및 장치에 관한 것이다.

배 경 기 술

[0003] 클라우드의 빠른 자원 확장력, 낮은 운용 비용, 끊기지 않는 서비스 등의 특징으로 정보 시스템의 컴퓨팅 환경은 클라우드 중심으로 변화하고 있다. 또한 많은 기업과 단체, 정부기관 등에서도 클라우드 컴퓨팅에 많은 관심을 두고 있다.

[0004] 클라우드 컴퓨팅 제공자는 사용자의 중요한 데이터를 투명하고 체계적으로 관리해야 하며, 사용자는 보안 관리에 대한 설명을 듣기를 원한다. 하지만 현재 클라우드 서비스 제공자는 충분한 보안 가시성 및 투명성 등을 제공하지 못하고 있으며, 미숙한 클라우드 보안 기술로 인하여 사용자의 요구사항을 충족시키지 못하고 있다.

[0005] 이러한 미숙한 클라우드 보안 기술 및 정책을 보완하기 위해서 기업과 단체에서는 클라우드 보안 기술 향상과 시스템 구축을 위해 예산을 배정하고 관리를 수행한다. 하지만 이러한 예산 배정으로 보안 투자를 수행하더라도 보안 투자에 대한 투자 효과를 파악하기에는 어려움이 있다. 기존의 보안 투자 방법들은 보안 위협 및 공격 횟수, 자산 중요도 및 자산 피해 규모 등을 기반으로 보안 투자 효과를 제시하고 있는데, 이러한 방법들에는 몇 가지 문제점이 존재한다.

[0006] 먼저, 기존의 보안 투자 방법들은 정확한 보안 평가를 바탕으로 보안 투자 효과를 제시한다고 보기 어렵다. 보안 공격은 일반적으로 여러 단계로 이뤄지는데, 다양한 공격 방법은 서로 중복되는 단계들이 존재한다. 예를 들어, 클라우드 보안 위협 중 데이터 침해(Breach)와 데이터 분실(Loss)는 서로 다른 보안 위협이지만, 관리자 계정을 탈취하는 공격 단계가 필요하다. 하지만 보안 평가 시에는 중복되는 공격단계를 고려하지 않고 데이터 침해와 데이터 분실을 독립적인 보안 위협으로 고려하여 보안 평가가 이뤄진다. 따라서 정확한 보안 평가가 이뤄

져야 보안 투자 방법 및 보안 투자 효과를 정확하게 평가할 수 있다.

[0007] 또한, 기존의 투자 기법들은 보유한 보안 투자 금액을 고려하지 않고 보안 수준을 최대로 높일 수 있는 방법들을 제안하였다. 그러나 기업이나 단체에서는 보안 투자에 금액이 한정되어 있으므로, 정해진 보안 투자 금액에서 최대의 보안 투자 효과를 찾을 수 있는 방법들이 필요하다.

[0008] 종래에 제안된 바 있는 투자 방법들은 아래와 같으며, 각 투자 방법들의 문제점은 다음과 같다.

[0009] 1. ALE(Annual Loss Expectancy): ALE는 특정 보안 위험이 시스템에 미치는 영향 수준을 고려하지 않으며, 모든 보안 위험의 발생빈도를 알아야만 한다는 점에서 문제가 있다.

[0010] 2. ROI(Return on Investment) 또는 ROSI(Return on Security Investment): 어떠한 투자행위에 대한 선택이 얼마나 효과가 있었는지를 사정한다. 하지만 ROI는 철저하게 현재 또는 특정시간만을 고려하기 때문에 투자 대비 보안효과의 정확성이 상대적으로 떨어지고 신뢰하기 어렵다.

[0011] 3. NPV(Net Present Value)모델: NPV모델은 현재자산가치와 투자후자산가치를 비교하여 투자를 결정하는 모델로, 투자비용-편익분석 이론을 실무에 적용하는데 유용하다. 하지만 모든 자산 평가 및 자산의 할인율(discount rate)을 정의하기가 무척 까다롭다.

[0012] 4. Gordon and Loeb모델: 최적 투자량 결정 방법으로 다양한 연구 중 처음으로 보안 위험(취약성)을 기반으로 투자량 상관관계를 이론적인 해석한 Gordon and Loeb모델은 보안 위협 확률 및 취약성 확률을 구하기가 현실적으로 어려우며, 한 번의 투자로 여러 종류의 정보가 상호연관되어 보호될 가능성을 배제하였다. 또한 최적의 투자량을 찾아내지만 기업 또는 기관에서 보안에 투자되는 자원은 한계가 있음이 고려되지 않았다.

발명의 내용

해결하려는 과제

[0014] 본 발명은 전술한 문제를 해결하기 위한 것으로, 클라우드 환경에서 발생할 수 있는 보안 위협의 공격 단계를 고려하여 보안 위험을 평가함으로써, 중복되는 공격에 대한 이중 평가를 배제하여 보다 정확한 보안 평가를 수행할 수 있는 보안 위험 평가 기반 보안 투자 방법 및 장치를 제공하는 것을 일 목적으로 한다.

[0015] 또한, 본 발명은 한정된 보안 예산에서 최대의 보안 투자 효과를 도출할 수 있는 보안 위험 평가 기반 보안 투자 방법 및 장치를 제공하는 것을 다른 목적으로 한다.

[0016] 또한, 본 발명은 수치적, 가시적으로 투자 효과를 표현함으로써, 경제적인 보안 투자를 가능하게 하는 보안 위험 평가 기반 보안 투자 방법 및 장치를 제공하는 것을 다른 목적으로 한다.

과제의 해결 수단

[0018] 이러한 목적을 달성하기 위한 본 발명은 보안 위험 평가 기반 보안 투자 방법에 있어서, 클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협 및 각 보안 위협의 단계별 취약점을 설정하는 단계, 하나의 보안 위협을 구성하는 상기 세부 공격 단계별 취약점을 계층적으로 연결하고, 제1 보안 위협 및 제2 보안 위협에 포함된 취약점이 동일한 경우, 동일한 취약점을 하나의 취약점 노드로 단일화하며, 단일화된 취약점 노드로 상기 제1 보안 위협 및 상기 제2 보안 위협을 연결하여 공격 트리 맵을 생성하는 단계, 상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭하는 단계, 상기 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하는 단계, 상기 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적으로 평가하는 단계를 포함하는 것을 일 특징으로 한다.

[0019] 또한, 본 발명은 보안 위험 평가 기반 보안 투자 장치에 있어서, 클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협 및 각 보안 위협의 단계별 취약점을 설정하는 환경 설정부, 상기 하나 이상의 보안 위협 전체에 대하여 중복되는 취약점을 하나의 노드로 단일화하여 공격 트리 맵을 생성하고, 상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭하는 공격 트리 맵 생성부, 상기 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수

를 산출하고, 상기 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적으로 평가하는 보안 위험 평가부를 포함하는 것을 일 특징으로 한다.

발명의 효과

[0021] 전술한 바와 같은 본 발명에 의하면, 클라우드 환경에서 발생할 수 있는 보안 위협의 공격 단계를 고려하여 보안 위험을 평가함으로써, 중복되는 공격에 대한 이중 평가를 배제하여 보다 정확한 보안 평가를 수행할 수 있다.

[0022] 또한, 본 발명에 의하면 한정된 보안 예산에서 최대의 보안 투자 효과를 도출할 수 있다.

[0023] 또한, 본 발명에 의하면 수치적, 가시적으로 투자 효과를 표현함으로써, 경제적인 보안 투자가 가능하다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시 예에 의한 보안 위험 평가 기반 보안 투자 장치의 구성을 설명하기 위한 블록도,

도 2는 본 발명의 일 실시 예에 의한 환경 설정 기능을 설명하기 위한 도면,

도 3은 본 발명의 일 실시 예에 의한 공격 트리 맵 생성 방법을 설명하기 위한 도면,

도 4는 본 발명의 일 실시 예에 의한 공격 트리 맵의 노드 구조를 설명하기 위한 도면,

도 5는 본 발명의 일 실시 예에 의한 공격 트리 맵을 설명하기 위한 도면,

도 6은 본 발명의 일 실시 예에 의한 보안 위험 평가 기반 보안 투자 방법을 설명하기 위한 순서도,

도 7은 본 발명의 다른 실시 예에 의한 보안 위험 평가 기반 보안 투자 방법을 설명하기 위한 순서도,

도 8은 투자 전략 수립을 위한 투자 후 보안 위험 평가의 일 실시 예를 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 전술한 목적, 특징 및 장점은 첨부된 도면을 참조하여 상세하게 후술되며, 이에 따라 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 상세한 설명을 생략한다.

[0027] 도면에서 동일한 참조부호는 동일 또는 유사한 구성요소를 가리키는 것으로 사용되며, 명세서 및 특허청구의 범위에 기재된 모든 조합은 임의의 방식으로 조합될 수 있다. 그리고 다른 식으로 규정하지 않는 한, 단수에 대한 언급은 하나 이상을 포함할 수 있고, 단수 표현에 대한 언급은 또한 복수 표현을 포함할 수 있음이 이해되어야 한다.

[0028] 본 명세서에서 사용되는 용어는 단지 특정 예시적 실시 예들을 설명할 목적을 가지고 있으며 한정할 의도로 사용되는 것이 아니다. 본 명세서에서 사용된 바와 같은 단수적 표현들은 또한, 해당 문장에서 명확하게 달리 표시하지 않는 한, 복수의 의미를 포함하도록 의도될 수 있다. 용어 "및/또는," "그리고/또는"은 그 관련되어 나열되는 항목들의 모든 조합들 및 어느 하나를 포함한다. 용어 "포함한다", "포함하는", "포함하고 있는", "구비하는", "갖는", "가지고 있는" 등은 내포적 의미를 갖는바, 이에 따라 이러한 용어들은 그 기재된 특징, 정수, 단계, 동작, 요소, 및/또는 컴포넌트를 특정하며, 하나 이상의 다른 특징, 정수, 단계, 동작, 요소, 컴포넌트, 및/또는 이들의 그룹의 존재 혹은 추가를 배제하지 않는다. 본 명세서에서 설명되는 방법의 단계들, 프로세스들, 동작들은, 구체적으로 그 수행 순서가 확정되는 경우가 아니라면, 이들의 수행을 논의된 혹은 예시된 그러한 특정 순서로 반드시 해야 하는 것으로 해석돼서는 안 된다. 추가적인 혹은 대안적인 단계들이 사용될 수 있음을 또한 이해해야 한다.

[0029] 또한, 각각의 구성요소는 각각 하드웨어 및 소프트웨어 프로세서로 구현될 수 있고, 위 구성요소들이 통합되어 하나의 하드웨어 및 소프트웨어 프로세서로 구현될 수 있으며, 또는 위 구성요소들이 서로 조합되어 복수 개의 하드웨어 및 소프트웨어 프로세서로 구현될 수도 있다.

[0030] 본 발명의 구체적인 실시 예를 설명하기에 앞서, 본 발명이 적용되는 클라우드 환경 및 본 명세서에서 사용되는 용어에 대하여 간략하게 설명한다.

[0031] 클라우드는 자원 가상화 기술을 사용하여 다양한 클라우드 서비스를 제공할 수 있다. 이는 한 대의 서버로 하나의 서비스만 제공했던 기존 컴퓨팅 기술과 차별된 점이다. 이러한 특징으로 인해, 클라우드 보안은 더욱 복잡한 양상을 띤다. 서비스가 하나일 경우 단일 서비스에 대한 보안 위협을 분석하고 이에 대한 대책을 수립하면 되지만, 클라우드 보안의 경우 다양한 서비스를 제공할 수 있기 때문에 그만큼 다양한 보안 위협을 분석하고 각각에 대한 대책을 수립해야하기 때문이다.

[0032] 보안 위협은 세부적인 공격 단계를 거쳐 발생할 수 있는데, 각 보안 위협의 세부 공격 단계는 중복될 수 있다. 따라서 다양한 보안 위협 간에 중복되는 공격 단계에 대한 이중 평가를 배제할 수 있는 보안 평가 방법이 필요한데, 본 명세서에서 이러한 문제를 해결할 수 있는 기술을 제안하고자 한다.

[0033] 또한, 클라우드 서비스 제공 업체들이 보안에 투자할 수 있는 예산은 제한적이므로, 제한된 예산 내에서 최적의 보안 투자가 가능하도록 보안 투자 전략을 수립하고 보안 투자 전략을 평가할 수 있는 방안이 요구된다. 본 발명은 이러한 요구를 충족시키는 보안 위험 평가 기반 보안 투자 방법 및 장치를 제공한다.

[0034] 본 명세서에서 본 발명의 각 실시 예는 하기와 같은 조건 하에서 운용되는 것으로 가정할 수 있다. 첫째로, 하나의 클라우드 보안 위협은 하나 이상의 세부 공격 단계를 갖는 것으로 가정한다. 각각의 세부 공격 단계는 하나 이상의 보안 취약점에 대응되며, 설명의 편의를 위해 하나의 세부 공격 단계가 하나의 보안 취약점에 대응되는 것으로 가정할 수 있다.

[0035] 둘째로, 클라우드 보안 제어 항목(Secure Control, SC)은 해당 보안 제어 항목에 투자가 이루어지는 경우, 타 보안 제어 항목에 영향을 미치지 않는 것으로 가정할 수 있다.

[0036] 셋째로, 하나의 보안 제어 항목은 하나 이상의 보안 취약점을 해결할 수 있는데, 하나의 보안 취약점은 적어도 하나의 보안 제어 항목과 매칭 가능한 것으로 가정할 수 있다.

[0037] 또한, 본 명세서에서 사용되는 각 기호 및 수식은 다음과 같은 의미를 갖는 것으로 해석될 수 있다.

표 1

[0038]

기호	정의
V_{xy}	x번째 보안 위협에 대한 y번째 취약점
SC_i	i번째 보안 제어 항목
CV_{ab-cd}	부모노드(취약점) V_{ab} 와 자식노드 V_{cd} 간의 상관계수
$M(z_i, V_{xy})$	보안 투자 금액 z_i 을 투자 후 취약점 V_{xy} 의 취약점수(투자 후 완화된 취약점수)
vV_{ab}^{0}	취약점 V_{ab} 에 대한 보안 취약 점수
vV_{ab}	ATM를 적용 후 취약점 V_{ab} 의 취약 점수
$vV(SC_i)$	i번째의 보안 제어 항목의 총 취약점수
z_i	i번째 보안 제어항목에 대한 투자 금액
vV_{child}	자식노드(들)의 총 취약 점수
F_{child}	자식노드(들)의 투자 후 총 취약점수
$F(SC_i)$	투자 후 i번째 제어항목의 총 취약점수
$F_{xy}(z_i)$	i번째 제어항목에 투자금액 z_i 을 투자 후 취약점 V_{xy} 의 취약점수
Z	모든 보안 제어항목에 투자한 총 투자금액
TVV	투자 전의 총 취약점수
iTVV	투자 후의 총 취약점수

[0039] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예를 상세히 설명하기로 한다.

[0040] 도 1은 본 발명의 일 실시 예에 의한 보안 위험 평가 기반 보안 투자 장치(이하, '보안 투자 장치'라 한다.)의 구성을 설명하기 위한 블록도이다. 도 1을 참조하면, 본 발명의 일 실시예에 따른 보안 투자 장치(100)는 환

경 설정부(110), 공격 트리 맵 생성부(130), 보안 위험 평가부(150), 투자금 산정부(170)를 포함할 수 있으며, 실시 예에 따라 가중치 결정부(140)를 더 포함할 수 있다. 도 1에 도시되어 있는 보안 투자 장치(100)의 구성은 예시적인 것으로서, 보안 투자 장치(100)는 도 1에 개시되어 있는 모듈의 일부만을 구비하거나 및/또는 그 동작을 위하여 필수적인 다른 모듈들을 추가로 구비할 수도 있다.

[0041] 보안 투자 장치(100)는 클라우드 컴퓨팅 환경에서 운용되며, 클라우드 서비스 제공자(미도시)로부터 환경 설정에 필요한 정보를 수신하여 보안 투자 전략을 수립할 수 있다. 그리고 보안 투자 전략이 수립되면 클라우드 서비스 제공자에게 보안 투자 전략을 하나 이상 제공할 수 있으며, 각각의 보안 투자 전략을 평가하여 제공할 수도 있다.

[0043] 환경 설정부(110)는 클라우드 서비스 환경을 분석하고 보안 위험 평가 및 투자 전략 수립에 필요한 항목들을 설정할 수 있다.

[0044] 예를 들어, 환경 설정부(110)는 클라우드 서비스 별로 발생할 수 있는 보안 위협을 정의할 수 있으며, 해당 보안 위협의 세부 공격 단계를 정의할 수 있다.

[0045] 예를 들어, 클라우드 서비스를 위협하는 주요 보안 위협으로는 클라우드 컴퓨팅의 남용 및 불손한 사용(Abuse and Nefarious Use of Cloud Computing), 불안전한 인터페이스와 애플리케이션 프로그래밍(Insecure Interfaces and APIs), 악의적 내부 관계자(Malicious Insiders), 공유 기술의 취약성(Shared Technology Issues), 데이터 유실 또는 유출(Data Loss or Breach), 서비스/계정 하이재킹(Service/Account Hijacking), 공개되지 않은 위협 프로파일(Unknown Risk Profile), 분산 서비스 거부 공격(Distributed Denial of Services) 등이 있으며, 보안 위협의 종류는 위 예시에 의하여 한정되지 않는다. 각 클라우드 서비스는 그 특성에 따라 보안 위협에 대한 취약 정도가 서로 다를 수 있으며, 따라서 보안 위협 별로 중요도를 다르게 설정할 수 있다. 따라서 환경 설정부(110)는 클라우드 서비스의 특성 및 클라우드 서비스 제공자 설정에 따라 발생 가능한 보안 위협을 정의하고, 특정 클라우드 서비스에 해당하는 보안 위협의 세부 공격 단계를 정의할 수 있다.

[0046] 각 보안 위협은 하나 이상의 공격 단계를 거쳐 발생할 수 있다. 예를 들어, 도 2에 도시된 (B) 데이터 유실(Data Loss)와 같은 보안 위협의 경우, 권한 획득(V_{21})→데이터 접근(V_{22})→데이터 유실(V_{23})의 단계를 포함할 수 있다. 이는 권한 획득 단계에서의 공격, 데이터 접근 시 공격, 최종적인 데이터 유실 단계에서의 공격 중 적어도 하나로 인해 데이터 유실이 발생할 수 있음을 의미한다. 임의의 클라우드 서비스는 데이터 유실의 보안 위협에 있어서, 전술한 세 단계의 세부 공격 단계에 취약점을 가지고 있으므로, 세부 공격 단계는 곧 취약점을 의미하는 것으로 이해될 수 있다. 본 명세서에서 x라는 보안 위협의 y번째 세부 공격 단계 각각은 취약점을 의미하며, 취약점은 표 1에 도시된 바와 같이 V_{xy} 로 표기한다.

[0047] 이하에서는 도 2를 참조하여 환경 설정부(110)의 보안 위협 및 세부 공격 단계 별 취약점 설정을 보다 자세하게 살펴본다.

[0048] 일 예로, 보안 투자 장치(100)가 임의의 클라우드 서비스에 대한 보안 투자 전략을 수립함에 있어서, 환경 설정부(110)는 해당 클라우드 서비스의 유형에 따라 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협 및 각 보안 위협의 단계별 취약점을 도 2와 같이 (A) 데이터 유출(Data Breach), (B) 데이터 손실(Data Loss), (C) 서비스/계정 하이재킹(Service/Account Hijacking), (D) 불안전한 API(Insecure APIs), (E) 악의적 내부 관계자(Malicious Insiders)의 다섯가지로 정의할 수 있다.

[0049] 그리고 환경 설정부(110)는 도 2에 도시된 바와 같이 세부 공격 단계 별 취약점을 설정할 수 있다. 예를 들어, (A) 데이터 유출(Data Breach)은 멀웨어 다운로드(V_{11}) → 감염된 루트킷(V_{12}) → 패스워드 해킹(V_{13}) → 관리자로 동작(V_{14}) → 가치있는 정보에 접속(V_{15})하는 과정을 통해 이루어질 수 있으며, (B) 데이터 손실(Data Loss)은 관리 자격 획득(V_{21}) → 데이터에 접근(V_{22}) → 데이터 손실(V_{23}) 과정을 통해 이루어질 수 있다. (C) 서비스/계정 하이재킹(Service/Account Hijacking)은 트랩에 빠짐(XSS)(V_{31}) → 관리자/사용자 계정 획득(V_{32}) → 암호 획득(V_{33})의 과정을 통해 이루어질 수 있으며, (D) 불안전한 API(Insecure APIs)는 불

안전한 오브젝트 레퍼런스 사용(V_{41}) → 데이터에 접근(V_{42}) 하는 과정을 통해 이루어질 수 있다. 마지막 보안 위협의 예시인 (E) 악의적 내부 관계자(Malicious Insiders)는 물리 서버에의 접근(V_{51}) → 서버 메모리 덤프 스캔(V_{52}) → 사용자 계정 정보 획득 (V_{53}) 과정을 통해 이루어질 수 있다.

[0050] 이와 같이 클라우드 서비스의 특성에 맞는 보안 위협과 세부 공격 단계의 단계별 취약점을 설정하는 과정을 통해 환경 설정부(110)는 보다 정확하게 보안 위험을 평가할 수 있으며, 이는 종래에 보안 위협만을 고려하여 이루어지던 보안 위험 평가의 낮은 정확도를 개선하는 효과가 있다.

[0051] 환경 설정부(110)는 클라우드 서비스의 보안 제어 항목을 설정할 수 있다. '보안 제어 항목 ' 은 보안 제어를 수행하는 물리적인 방법을 의미하며, 분류 방법에 따라 달라질 수 있다. 예를 들어, 환경 설정부(110)는 보안 제어 항목을 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사확인 및 준수(AuditVerification and Compliance) 등으로 분류 설정할 수 있다. 한편, 본 발명의 일 실시 예에서 보안 투자는 보안 제어 항목을 기반으로 이루어지는 것으로 이해될 수 있다.

[0052] 환경 설정부(110)는 상관도를 정의할 수 있다. 상관도는 세부 공격 단계를 트리의 각 노드에 맵핑했을 때, 선행 단계(자식 노드)와 후행 단계(부모 노드) 간 상관관계를 나타내는 상관 계수를 의미한다.

[0053] 예를 들면, 세부 공격은 단계별로 진행되는데, 공격자가 첫 번째 세부 공격 단계에서 공격에 성공하면, 두 번째 단계를 보다 쉽게 공격할 수 있다. 일 예로, 도 2의 (A) 데이터 유출에서 공격자가 V_{11} 단계의 공격에 성공하면 다음 단계인 V_{12} 단계의 공격에 성공할 확률과 V_{12} 단계의 공격에 성공하면 다음 단계인 V_{13} 단계의 공격에 성공할 확률은 서로 다른 값을 가질 수 있다. 이와 같이 각 단계간의 상관 관계를 나타내는 값을 상관도라고 하며, 상관도는 각 공격의 특성에 따라 달라질 수 있다.

[0054] 환경 설정부(110)는 상관도를 설정하여 순차적인 공격에 의한 취약 정도를 보안 평가에 반영할 수 있다. 상관도는 부모 취약점 노드(부모 공격 단계 또는 후행 공격 단계)와 자식 취약점 노드(자식 공격 단계 또는 선행 공격 단계)간에 정의되는 상관 계수로 이해될 수 있으며, 이 값은 클라우드 서비스 제공자의 설정에 따라 달라질 수 있다. 또한, 상관도는 누적된 공격 패턴의 분석 결과에 따라 환경 설정부(110)에 의해 자동으로 설정될 수도 있다.

[0055] 나아가 환경 설정부(110)는 보안 취약 완화 비율을 설정할 수 있다. '보안 취약 완화 비율' 은 임의의 보안 제어 항목에 투자했을 때 해당 보안 제어 항목에 대응하는 취약점의 보안 취약성이 완화되는 비율을 의미한다. 보다 구체적으로, 보안 취약 완화 비율은 보안 취약 완화 함수의 상수 값을 의미하는 것일 수 있다. 예를 들어 이후 보안 위험 평가부(150)가 아래 수학식 1과 같은 보안 취약 함수를 이용하여 완화된 보안 취약 점수를 산출할 수 있는데, 환경 설정부(110)는 수학식 1의 α , β 에 해당하는 상수 값을 각 보안 제어 항목 별로 아래 표 2와 같이 설정할 수 있다.

수학식 1

[0056]
$$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}$$

표 2

[0057]

SC_i	SC_1	SC_2	SC_3	SC_4	SC_5
α	0.078	0.073	0.077	0.047	0.068
β	0.103	0.123	0.162	0.236	0.249

[0058] 환경 설정부(110)에서 설정된 보안 취약 완화 비율은 보안 취약 완화 함수에 사용되므로, 상기 함수의 결과 값을 산출되는 완화된 보안 취약 점수에 영향을 미친다.

[0059] 보안 취약 완화 비율은 보안 제어 항목의 특성에 따라 달라질 수 있으며, 기업과 단체, 서비스 특징, 클라우드 컴퓨팅 환경의 영향을 받을 수 있다. 또한 보안 취약 완화 비율은 기존 투자에 의해 누적된 데이터 및 통계에 따라 다르게 결정될 수 있다.

[0060] 공격 트리 맵 생성부(130)는 하나 이상의 보안 위협 전체에 대하여 중복되는 취약점을 하나의 노드로 단일화하여 공격 트리 맵을 생성하고, 상기 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭할 수 있다.

[0061] 도 3의 예시를 참조하여 공격 트리 맵의 생성 방법을 살펴보자. 도 3은 클라우드 서비스에 설정된 보안 위협이 데이터 유출(Data Breach)와 데이터 손실(Data Loss)인 경우의 일 실시 예이다. 먼저 보안 위협의 단계별 취약점 각각은 하나의 취약점 노드에 대응될 수 있다. (A)에서 각각의 보안 위협은 a1 내지 a4, b1 내지 b4의 단계별 취약점을 포함한다. 여기서, 멀웨어를 다운로드하는 a1과 b1, 감염된 루트킷의 a2와 b2는 동일한 취약점에 해당한다. 공격 트리 맵 생성부(130)는 공격 트리 맵을 생성함에 있어서, 보안 위험 전체를 검토하여 중복되는 취약점을 우측의 (B)와 같이 하나의 노드로 단일화한다.

[0062] 더 나아가 공격 트리 맵 생성부(130)는 도 4에 도시된 바와 같이 취약점 노드 간 관계를 반영하여 공격 트리 맵을 생성할 수 있으며, 각 취약점 노드에 해당 취약점을 보완할 수 있는 보안 제어 항목을 매칭할 수 있다. 도 4의 (A)는 일반적인 구조를 나타낸다. 제 1 보안 위협이 V_{ab}-> V_{ac}의 단계별 취약점을 포함하고, 제 2 보안 위협이 V_{de}-> V_{ac}의 단계별 취약점을 포함할 때, 취약점 V_{ac}가 중복되므로, 해당 취약점 노드는 단일화할 수 있다. V_{ab}, V_{de}는 선행 공격 단계이므로 자식 노드가 되고, V_{ac}는 후행 공격 단계이므로 부모 노드에 해당한다. 또한, 공격 트리 맵 생성부(130)는 각각의 취약점 노드에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭할 수 있는데, V_{ab}에는 SC_i, V_{de}에는 SC_k, V_{ac}에는 SC_j를 매칭할 수 있다.

[0063] (B)는 하나 이상의 자식 노드가 상호 독립적인 경우(OR 조건 관계인 경우)를 공격 트리 맵에 나타낸 것이다. V_{ab}-> V_{ac} 로 진행되는 제 1 보안 위협과 V_{de}-> V_{ac}로 진행되는 제 2 보안 위협은 서로 영향을 미치지 않는다. 이러한 경우에는 공격 트리 맵에 (B)와 같이 OR 조건 관계를 반영하여 표시할 수 있다.

[0064] (C)는 하나 이상의 자식 노드가 상호 AND 조건 관계인 경우를 공격 트리 맵에 나타낸 것이다. V_{ab}와 V_{de} 두 개의 취약점을 모두 만족하는 경우 V_{ac} 단계로 진행되는 보안 위협이 존재할 수 있으며, 이 경우 공격 트리 맵은 (C)와 같이 생성될 수 있다.

[0065] 전술한 바와 같은 자식 노드와 부모 노드가 이루는 노드 구조는 취약 점수 산출에 영향을 미칠 수 있으므로, 공격 트리 맵 생성부(130)는 이러한 구조를 공격 트리 맵에 반영하는 것이 바람직하다.

[0066] 도 5는 도 2의 예시와 같이 공격 위협이 다섯 개로 정의된 클라우드 서비스에서, 공격 트리 맵 생성부(130)가 전술한 자식 노드 구조 및 상관도를 반영하고 보안 제어 항목을 매칭하여 생성한 공격 트리 맵의 일 실시 예이다.

[0067] 도 5의 공격 트리 맵에서, 각각의 취약점 노드(V_{xy})에는 모두 하나 이상의 보안 제어 항목(SC_i)이 매칭되어 있다. 각 노드를 연결한 링크에 표시된 $CV_{xy-x'y'}$는 취약점 노드 V_{xy}와 $V_{x'y'}$간의 상관도를 의미한다.

[0068] 이처럼 공격 트리 맵 생성부(130)는 중복되는 취약점을 제거함으로써, 중복 투자에 소요되는 비용을 제외시킬 수 있으며, 따라서 클라우드 서비스 제공자 및 투자자는 종래 기술에 비해 정확도 높은 보안 투자 금액을 확인할 수 있다.

[0069] 보안 위험 평가부(150)는 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약점수를 산출하는데, 이 때 취약 점수는 다음 수학식 2 내지 수학식 4를 이용하여 도출될 수 있다.

[0070] 예를 들어, 임의의 제 1 취약점 노드의 하나 이상의 제 1 자식 노드가 상호 독립적이면, 제 1 자식 노드의 취약점수와 기 설정된 제 1 자식 노드 - 취약점 노드 간 상관계수의 곱을 합산하여 제 1 취약점 노드의 취약 점수를

산출할 수 있는데, 이는 수학식 2 또는 수학식 3과 같이 수식으로 나타낼 수 있다.

[0071] 또 다른 실시 예로, 임의의 제 2 취약점 노드의 하나 이상의 제 2 자식 노드가 상호 AND 조건 관계이면, 제 2 자식 노드의 취약 점수와 기 설정된 제 2 자식 노드- 취약점 노드 간 상관계수의 곱을 합산한 값을 제 2 자식 노드의 수로 나누어 제 2 취약점 노드의 취약 점수를 산출할 수 있는데, 이는 수학식 4와 같이 수식으로 나타낼 수 있다.

[0072] 수학식 2는 일반적인 구조를 갖는 공격 트리 맵에서의 취약점 V_{ac}의 취약 점수 ${}_{v}V_{ac}$이며, 수학식 3은 취약점 노드(V_{ac})와 자식 노드 간 상호 독립적인 OR 구조를 갖는 경우의 취약점 V_{ac}의 취약 점수 ${}_{v}V_{ac}$이다. 수학식 4는 취약점 노드(V_{ac})와 자식 노드 간 AND 구조를 갖는 경우의 취약점 V_{ac}의 취약 점수 ${}_{v}V_{ac}$이다.

수학식 2

[0073] $$v V_{ac} = v V_{ac}^{0} + (v V_{child} * CV)$$

수학식 3

[0074] $$v V_{ac} = v V_{ac}^{0} + (V_{child1} + V_{child2} + \cdots + V_{childn}) * CV$$

수학식 4

[0075] $$v V_{ac} = v V_{ac}^{0} + \frac{(V_{child1} + V_{child2} + \cdots + V_{childn})}{The number of V_{child}} * CV$$

[0077] 전술한 도 5의 실시 예에서의 각 취약점 노드의 취약 점수는 아래 표 3과 같이 나타낼 수 있다. 이는 각 노드 간 상관도를 0.1로 가정한 경우의 일 예시이다.

표 3

[0078]

취약점 노드	부모 노드	자식 노드	취약점 노드의 보안 취약 점수	매칭된 보안 제어 항목
V_{11}	V_{12}	-	45	SC2
V_{12}	V_{13}	V_{11}	21	SC4
V_{13}	V_{14}	V_{12}, V_{32}, V_{52}	56	SC1
V_{14}	V_{15}	V_{13}	17	SC4
V_{15}	V_{23}	V_{14}, V_{41}	13	SC4
V_{23}	-	V_{15}	15	SC2
V_{31}	V_{32}	-	57	SC3
V_{32}	V_{13}	V_{31}	21	SC4
V_{41}	V_{15}	-	63	SC5
V_{51}	V_{52}	-	24	SC2
V_{52}	V_{13}	V_{51}	21	SC4
Total	-	-	353	-

[0079] 보안 위험 평가부(150)는 보안 제어 항목별로 상기 취약 점수를 합산하여 $vV(SC_i)$를 구할 수 있으며, 이를 모두 합산하여 투자 전의 총 취약점수(TVV)를 산출하여 클라우드 서비스의 보안 위험을 정량적으로 평가한다. 본 발명의 일 실시 예에서, 투자 전의 총 취약점수(TVV)는 클라우드 서비스의 보안 위험을 나타내는 정량적 지표로 이해될 수 있으며, 투자 전의 총 취약 점수(TVV)는 하기 수학식 5와 같이 산출할 수 있다.

수학식 5

[0080] $$vV(SC_i) = \sum_{y=1}^{m}\sum_{x=1}^{n} vV_{xy}, where\ vV_{xy} \in SC_i$$

[0081] $$TVV = \sum_{i=1}^{k} vV(SC_i)$$

[0082] 상술한 표 2의 예시에서, 보안 제어 항목 별 취약점수의 합과 투자 전 총 취약점수(TVV)를 구하면 아래 표 3과 같다.

표 4

[0083]

	SC_1	SC_2	SC_3	SC_4	SC_5	Total
$vV^0(SC_i)$	56	81	57	96	93	353
$vV(SC_i)$	63.56	85.564	57	121.192	63	390.316

[0084] 표 4에서 $vV^0(SC_i)$는 공격 트리 맵을 생성하지 않고 각 취약점의 취약 점수를 보안 제어 항목 별로 단순 합산한 경우의 보안 제어 항목 별 취약 점수의 합이며, $vV(SC_i)$는 상관도 및 구조를 반영하여 공격 트리 맵을 생성한 본 발명의 일 실시 예에 따른 보안 제어 항목 별 취약 점수의 합이다. 종래 기술에 따른 투자 전 총 취약 점수는 353이며, 본 발명의 일 실시 예에 따른 투자 전 총 취약 점수(TVV)는 390.316으로 산출되어 차이가 있음을 확인할 수 있다.

[0085] 가중치 결정부(140)는 클라우드 서비스 유형에 따라 상기 보안 제어 항목 별 가중치를 결정할 수 있다. 클라우드 서비스 유형에 따라 각 보안 제어 항목은 서로 다른 가중치를 가질 수 있는데, 예를 들어 보안 저장에 더 큰 가중치를 부여하는 클라우드 서비스가 있을 수 있고, 보안 처리에 더 큰 가중치를 부여하는 클라우드 서비스가 있기 때문이다. 가중치 결정부(140)는 클라우드 서비스 제공자의 설정 또는 기 누적된 클라우드 서비스 이용 현황 등의 서비스 특성을 학습하여 가중치를 결정할 수 있다.

[0086] 이렇게 가중치 결정부(140)에서 결정된 가중치는 보안 위험 평가부(150)가 투자 전 총 취약 점수(TVV)를 산출할 때 사용될 수 있다. 보안 위험 평가부(150)는 보안 위험을 정량적으로 평가함에 있어서, 보안 제어 항목별로 합산한 취약 점수에 상기 보안 제어 항목의 가중치를 반영할 수 있다.

[0087] 다음으로 보안 위험 평가부(150)는 투자 후의 보안 위험을 정량적으로 평가함으로써, 투자 전략을 수립할 수 있다. 투자 전략 수립을 위한 보안 위험 평가에서, 보안 위험 평가부(150)는 환경 설정부(110)에서 설정된 보안 취약 완화 비율을 이용할 수 있다. 전술한 환경 설정부(110)의 실시 예에서, 임의의 보안 제어 항목 SC_i에 투자 시, 상기 보안 제어 항목 SC_i에 대응하는 하나 이상의 투자 취약점의 보안 취약 완화 비율을 결정한 바 있다.

[0088] 보안 위험 평가부(150)는 투자 취약점 노드의 자식 노드 구조 및 상관도, 상기 투자에 대응하는 투자 금액 및 상기 투자 취약점의 보안 취약 완화 비율을 이용하여 상기 투자 취약점 노드 각각의 완화된 취약 점수를 산출하며, 상기 보안 제어 항목별로 상기 완화된 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 투자

후 보안 위험을 정량적으로 평가한다.

[0089] 예를 들어, 보안 위험 평가부(150)는 투자 금액이 z_i이면, 상기 투자 취약점 노드 v_{xy}의 완화된 취약 점수 $M(z_i, v_{xy})$를 하기 수학식 6에 따라 산출할 수 있다. 이 때, α 및 β는 환경 설정부(110)에서 설정된 상수(보안 취약 완화 비율)일 수 있다.

수학식 6

[0090] $$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}$$

[0091] 보다 구체적으로, 보안 위험 평가부(150)는 취약점 노드와 그의 자식 노드가 이루는 구조를 고려하여 다음과 같이 완화된 취약 점수를 산출할 수 있다.

[0092] 수학식 7 내지 수학식 9는 구조를 고려하여 완화된 취약 점수를 산출하는 식의 일 실시 예이다. 수학식 7은 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 일반적인 구조를 갖는 취약점 노드 V_{xy}의 취약 점수이며, 수학식 8은 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 자식 노드와 OR 구조를 갖는 취약점 노드 V_{xy}의 취약 점수, 수학식 9는 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 자식 노드와 AND 구조를 갖는 취약점 노드 V_{xy}의 취약 점수를 나타낸 것이다.

수학식 7

[0093] $$F_{xy}(z_i) = M(z_i, v\, V_{xy}^0) + CV^* F_{child}$$

수학식 8

[0094] $$F_{xy}(z_i) = M(z_i, v\, V_{xy}^0) + CV^* \sum F_{child}$$

수학식 9

[0095] $$F_{xy}(z_i) = M(z_i, v\, V_{xy}^0) + CV^* \overline{F_{child}}$$

[0097] 각각의 투자 후 완화된 취약 점수는 보안 제어 항목을 중심으로 정리할 수 있으며, 투자 후의 총 취약 점수 iTVV는 다음 수학식 10과 같이 도출될 수 있다. 투자 후 총 취약 점수 iTVV는 투자 후 보안 위험을 정량적으로 평가한 값으로, TVV과 iTVV를 이용하여 투자 후 보안 위험을 투자 전 보안 위험과 비교할 수 있다.

수학식 10

[0098] $$F(SC_i) = \sum_{y=1}^{m} \sum_{x=1}^{n} F_{xy}(z_i), where\ F_{xy}(z_i) \in SC_i$$

[0099] $$iTVV = \sum_{i=1}^{k} F(SC_i)$$

[0101] 투자금 산정부(170)는 보안 위험 평가부(150)에서 정량적으로 평가한 투자 후 보안 위험이 최소가 되도록 보안 제어 항목별 최적 투자 금액을 산정할 수 있다. 일 예로, 투자금 산정부(170)는 최적화 기법인 라그랑지 승수법을 이용하여 아래 수학식 11의 하단 조건을 만족하도록 투자 금액을 산정할 수 있다.

수학식 11

[0102] $$Minimum\ iTVV = \sum_{i=1}^{k} \sum_{y=1}^{m} \sum_{x=1}^{n} F_{xy}(z_i)$$

[0103] $$\sum_{i=1}^{k} z_i = Z, where\ z_i | i = 1, \ldots, k \geq 0$$

[0104] 투자 분석부(190)는 투자 전 총 취약 점수(TVV)와 투자 후 총 취약 점수(iTVV)를 이용하여 투자 전후의 취약 점수를 비교한 결과를 사용자에게 제공할 수 있으며, 종래 기술에 따른 다른 투자 전략과의 정량적 비교를 통해 가장 우수한 투자 전략을 사용자에게 제공(추천)할 수 있다. 예를 들어, 총 투자 금액을 모든 보안 제어 항목에 동일하게 투자한 경우의 총 취약 점수를 산출하여 사용자에게 제공할 수 있으며(균등 투자), 상술한 라그랑지 승수법을 이용하여 iTVV값이 가장 작아지는 경우의 총 취약 점수를 산출하여 사용자에게 제공할 수 있다(최적 투자). 사용자는 보안 투자 장치(100)가 제공한 정량화된 투자 후 보안 위험을 보안 투자를 위한 예산 사용에 참조할 수 있으며, 효과적으로 보안 투자를 실행할 수 있다.

[0105] 도 6은 본 발명의 일 실시 예에 의한 보안 위험 평가 기반 보안 투자 방법(이하, '보안 투자 방법'이라 함)을 설명하기 위한 순서도이다.

[0106] 도 6을 참조하면, 본 발명의 일 실시 예에 의한 보안 투자 방법은 크게 환경 설정 단계(S10), 보안 위험 평가 단계(S20), 투자 전략 수립 단계(S30), 투자 효과 평가 단계(S40)를 포함할 수 있다.

[0107] 단계 10에서 서버는 클라우드 서비스 환경을 분석하고 보안 위험 평가 및 투자 전략 수립에 필요한 항목들을 설정할 수 있다.

[0108] 예를 들어, 서버는 클라우드 서비스 별로 발생할 수 있는 보안 위협을 정의할 수 있으며, 해당 보안 위협의 세부 공격 단계를 정의할 수 있다.

[0109] 예를 들어, 클라우드 서비스를 위협하는 주요 보안 위협으로는 클라우드 컴퓨팅의 남용 및 불손한 사용(Abuse and Nefarious Use of Cloud Computing), 불안전한 인터페이스와 애플리케이션 프로그래밍(Insecure Interfaces and APIs), 악의적인 내부 관계자(Malicious Insiders), 공유 기술의 취약성(Shared Technology Issues), 데이터 유실 또는 유출(Data Loss or leakage), 계정 및 서비스 하이재킹(Account or Service Hijacking), 공개되지 않은 위협 프로파일(Unknown Risk Profile), 분산 서비스 거부 공격(Distributed Denial of Services) 등이 있으며, 보안 위협의 종류는 위 예시에 의하여 한정되지 않는다. 각 클라우드 서비스는 그 특성에 따라 보안 위협에 대한 취약 정도가 서로 다를 수 있으며, 따라서 보안 위협 별로 중요도를 다르게 설정

할 수 있다. 따라서 단계 10에서 서버는 클라우드 서비스의 특성 및 클라우드 서비스 제공자 설정에 따라 발생 가능한 보안 위협을 정의하고, 특정 클라우드 서비스에 해당하는 보안 위협의 세부 공격 단계를 정의할 수 있다.

[0110] 각 보안 위협은 하나 이상의 공격 단계를 거쳐 발생할 수 있다. 예를 들어, 도 2에 도시된 (B) 데이터 유실(Data Loss)와 같은 보안 위협의 경우, 권한 획득(V_{21})→데이터 접근(V_{22})→데이터 유실(V_{23})의 단계를 포함할 수 있다. 이는 권한 획득 단계에서의 공격, 데이터 접근 시 공격, 최종적인 데이터 유실 단계에서의 공격 중 적어도 하나로 인해 데이터 유실이 발생할 수 있음을 의미한다. 임의의 클라우드 서비스는 데이터 유실의 보안 위협에 있어서, 전술한 세 단계의 세부 공격 단계에 취약점을 가지고 있으므로, 세부 공격 단계는 곧 취약점을 의미하는 것으로 이해될 수 있다. 본 명세서에서 x라는 보안 위협의 y번째 세부 공격 단계 각각은 취약점을 의미하며, 취약점은 표 1에 도시된 바와 같이 V_{xy}로 표기한다.

[0111] 이와 같이 클라우드 서비스의 특성에 맞는 보안 위협과 세부 공격 단계를 설정하는 과정을 통해 서버는 보다 정확하게 보안 위험을 평가할 수 있으며, 이는 종래에 보안 위협만을 고려하여 이루어지던 보안 위험 평가의 낮은 정확도를 개선하는 효과가 있다.

[0112] 환경을 설정하는 단계 10에서 서버는 클라우드 서비스의 보안 제어 항목을 설정할 수 있다. '보안 제어 항목'은 보안 제어를 수행하는 물리적인 방법을 의미하며, 분류 방법에 따라 달라질 수 있다. 예를 들어, 서버는 보안 제어 항목을 보안 저장(Secure Storage), 보안 처리(Secure Processing), 네트워크(Network), 접근 제어(Access Control), 감사확인 및 준수(AuditVerification and Compliance) 등으로 분류 설정할 수 있다.

[0113] 서버는 전술한 보안 위협 및 취약점에 대응할 수 있는 보안 제어 항목을 선택하여 각 취약점 마다 하나 이상의 보안 제어 항목을 매칭할 수 있다. 또한, 본 발명의 일 실시 예에서 보안 투자는 보안 제어 항목을 기반으로 이루어지는 것으로 이해될 수 있다.

[0114] 단계 10에서 서버는 상관도를 정의할 수 있다. 상관도는 세부 공격 단계를 트리의 각 노드에 맵핑했을 때, 선행 단계(자식 노드)와 후행 단계(부모 노드) 간 상관관계를 나타내는 상관 계수를 의미한다.

[0115] 예를 들면, 세부 공격은 단계별로 진행되는데, 공격자가 첫 번째 세부 공격 단계에서 공격에 성공하면, 두 번째 단계를 보다 쉽게 공격할 수 있다. 일 예로, 도 2의 (A) 데이터 유출에서 공격자가 V_{11} 단계의 공격에 성공하면 다음 단계인 V_{12} 단계의 공격에 성공할 확률과 V_{12}단계의 공격에 성공하면 다음 단계인 V_{13} 단계의 공격에 성공할 확률은 서로 다른 값을 가질 수 있다. 이와 같이 각 단계간의 상관 관계를 나타내는 값을 상관도라고 하며, 상관도는 각 공격의 특성에 따라 달라질 수 있다.

[0116] 서버는 상관도를 설정하여 순차적인 공격에 의한 취약 정도를 보안 평가에 반영할 수 있다. 상관도는 부모 취약점 노드(부모 공격 단계 또는 후행 공격 단계)와 자식 취약점 노드(자식 공격 단계 또는 선행 공격 단계)간에 정의되는 상관 계수로 이해될 수 있으며, 이 값은 클라우드 서비스 제공자의 설정에 따라 달라질 수 있다. 또한, 상관도는 누적된 공격 패턴의 분석 결과에 따라 서버에 의해 자동으로 설정될 수도 있다.

[0117] 나아가 서버는 단계 10에서 보안 취약 완화 비율을 설정할 수 있다. '보안 취약 완화 비율'은 임의의 보안 제어 항목에 투자했을 때 해당 보안 제어 항목에 대응하는 취약점의 보안 취약성이 완화되는 비율을 의미한다. 보다 구체적으로, 보안 취약 완화 비율은 보안 취약 완화 함수의 상수 값을 의미하는 것일 수 있다. 예를 들어 이후 보안 위험 평가 단계(S20) 또는 투자 전략 수립 단계(S30)에서 아래 수학식 12과 같은 보안 취약 함수를 이용하여 완화된 보안 취약 점수를 산출할 수 있는데, 서버는 단계 10에서 수학식 12의 α, β 에 해당하는 상수 값을 각 보안 제어 항목 별로 설정할 수 있으며, 이는 전술한 표 1을 참조한다.

수학식 12

[0118]
$$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}$$

[0120] 단계 10에서 설정된 보안 취약 완화 비율은 보안 취약 완화 함수에 사용되므로, 상기 함수의 결과 값을 산출되는 완화된 보안 취약 점수에 영향을 미친다.

[0121] 보안 취약 완화 비율은 보안 제어 항목의 특성에 따라 달라질 수 있으며, 기업과 단체, 서비스 특징, 클라우드 컴퓨팅 환경의 영향을 받을 수 있다. 또한 보안 취약 완화 비율은 기존 투자에 의해 누적된 데이터 및 통계에 따라 다르게 결정될 수 있다.

[0122] 다음으로, 서버는 보안 위험을 평가하는데(S20), 보안 위험 평가 단계는 도 7을 참조하여 보다 구체적으로 설명하기로 한다.

[0123] 도 7의 단계 100은 전술한 단계 10과 동일하므로, 구체적인 설명은 생략한다. 보안 위험을 평가하는 단계 20은 도 7의 단계 200 내지 단계 500을 포함할 수 있다. 도 7을 참조하면, 서버는 클라우드 서비스 유형에 따라 상기 클라우드 서비스에서 발생할 수 있는 하나 이상의 보안 위협 및 각 보안 위협의 단계별 취약점을 설정하고(S100), 상기 하나 이상의 보안 위협 전체에 대하여 중복되는 취약점을 하나의 노드로 단일화하여 공격 트리 맵을 생성할 수 있다(S200).

[0124] 다음으로 서버는 공격 트리 맵의 취약점 노드 각각에 해당 취약점을 보완하기 위한 보안 제어 항목을 매칭할 수 있다(S300). 단계 200 내지 300의 실시 예는 도 3의 예시를 참조하여 전술한 바 있으므로, 구체적인 설명은 생략하기로 한다.

[0125] 서버는 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하고(S400), 보안 제어 항목별로 상기 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 보안 위험을 정량적으로 평가한다(S500).

[0126] 단계 400에서 서버는 취약점 노드의 자식 노드 구조 및 상관도를 이용하여 상기 취약점 노드 각각의 취약 점수를 산출하는데, 이 때 취약 점수는 다음 수학식 13 내지 수학식 15를 이용하여 도출될 수 있다.

[0127] 예를 들어, 임의의 제 1 취약점 노드의 하나 이상의 제 1 자식 노드가 상호 독립적이면, 제 1 자식 노드의 취약 점수와 기 설정된 제 1 자식 노드 - 취약점 노드 간 상관계수의 곱을 합산하여 제 1 취약점 노드의 취약 점수를 산출할 수 있는데, 이는 수학식 13 또는 수학식 14와 같이 수식으로 나타낼 수 있다.

[0128] 또 다른 실시 예로, 임의의 제 2 취약점 노드의 하나 이상의 제 2 자식 노드가 상호 AND 조건 관계이면, 제 2 자식 노드의 취약 점수와 기 설정된 제 2 자식 노드- 취약점 노드 간 상관계수의 곱을 합산한 값을 제 2 자식 노드의 수로 나누어 제 2 취약점 노드의 취약 점수를 산출할 수 있는데, 이는 수학식 15와 같이 수식으로 나타낼 수 있다.

[0129] 수학식 13은 일반적인 구조를 갖는 공격 트리 맵에서의 취약점 V_{ac}의 취약 점수 ${}_{n}V_{ac}$이며, 수학식 14는 취약점 노드(V_{ac})와 자식 노드 간 상호 독립적인 OR 구조를 갖는 경우의 취약점 V_{ac}의 취약 점수 ${}_{n}V_{ac}$이다. 수학식 15는 취약점 노드(V_{ac})와 자식 노드 간 AND 구조를 갖는 경우의 취약점 V_{ac}의 취약 점수 ${}_{n}V_{ac}$이다.

수학식 13

[0130] $$v V_{ac} = v V_{ac}^{0} + (v V_{child} * CV)$$

수학식 14

[0131] $$v V_{ac} = v V_{ac}^{0} + (V_{child1} + V_{child2} + \ldots + V_{childn}) * CV$$

수학식 15

[0132]
$$v\,V_{ac} = v\,V_{ac}^{0} + \frac{(V_{child1} + V_{child2} + \cdots + V_{childn})}{The number of\ V_{child}} * CV$$

[0134] 서버는 보안 제어 항목별로 상기 취약 점수를 합산하여 ${}_{n}V(SC_i)$를 구할 수 있으며, 이를 모두 합산하여 투자 전의 총 취약점수(TVV)를 산출하여 클라우드 서비스의 보안 위험을 정량적으로 평가한다. 본 발명의 일 실시예에서, 투자 전의 총 취약점수(TVV)는 클라우드 서비스의 보안 위험을 나타내는 정량적 지표로 이해될 수 있으며, 투자 전의 총 취약 점수(TVV)는 하기 수학식 16과 같이 산출할 수 있다.

수학식 16

[0135]
$$v\,V(SC_i) = \sum_{y=1}^{m}\sum_{x=1}^{n} v\,V_{xy}, where\ v\,V_{xy} \in SC_i$$

[0136]
$$TVV = \sum_{i=1}^{k} v\,V(SC_i)$$

[0138] 보안 위험 평가의 다른 실시 예로 서버는 클라우드 서비스 유형에 따라 상기 보안 제어 항목 별 가중치를 결정할 수 있으며, 단계 500에서 보안 제어 항목별로 합산한 취약 점수에 상기 보안 제어 항목의 가중치를 반영하여 상기 보안 위험을 정량적으로 평가할 수 있다.

[0139] 투자 전의 보안 위험 평가가 완료되면, 서버는 투자 후 보안 위험을 평가할 수 있는데(S30), 단계 30은 도 8을 참조하여 보다 자세히 설명한다.

[0140] 도 8은 투자 전략 수립을 위한 투자 후 보안 위험 평가의 일 실시 예를 설명하기 위한 순서도이다. 도 8을 참조하면, 서버는 전술한 보안 취약 완화 함수를 이용하여 완화된 보안 취약 점수를 산출한다. 완화된 보안 취약 점수는 각 보안 제어 항목 별로 투자가 이루어진 이후의 각 보안 제어 항목 별 보안 취약 점수를 의미한다. 특정 보안 제어 항목에 보안 투자가 이루어지면 해당 보안 제어 항목이 강화되므로, 보안 취약성이 낮아진다. 따라서 보안 취약 점수 또한 낮아질 것으로 예상할 수 있다.

[0141] 단계 30에서, 서버는 단계 10에서 설정된 보안 취약 완화 비율을 이용할 수 있다. 전술한 단계 10의 실시 예에서, 임의의 보안 제어 항목 SC_i에 투자 시, 상기 보안 제어 항목 SC_i에 대응하는 하나 이상의 투자 취약점의 보안 취약 완화 비율을 결정한 바 있다. 다만, 서버는 다른 실시 예에서 도 8에 도시된 바와 같이 투자 후 보안 위험 평가 단계에서 보안 취약 완화 비율을 결정할 수 있다(S600).

[0142] 서버는 투자 취약점 노드의 자식 노드 구조 및 상관도, 상기 투자에 대응하는 투자 금액 및 상기 투자 취약점의 보안 취약 완화 비율을 이용하여 상기 투자 취약점 노드 각각의 완화된 취약 점수를 산출할 수 있다(S700). 그리고 서버는 상기 보안 제어 항목별로 상기 완화된 취약 점수를 합산하고, 이를 이용하여 상기 클라우드 서비스의 투자 후 보안 위험을 정량적으로 평가할 수 있다(S800).

[0143] 예를 들어, 서버는 단계 700에서 투자 금액이 z_i이면, 상기 투자 취약점 노드 v_{xy}의 완화된 취약 점수 $M(z_i, v_{xy})$를 전술한 수학식 12에 따라 산출할 수 있다. 이 때, α 및 β는 단계 10 또는 단계 600에서 결정된 보안 취약 완화 비율일 수 있다.

[0144] 보다 구체적으로, 서버는 단계 700에서 취약점 노드와 그의 자식 노드가 이루는 구조를 고려하여 다음과 같이 완화된 취약 점수를 산출할 수 있다.

[0145] 수학식 17 내지 수학식 19는 구조를 고려하여 완화된 취약 점수를 산출하는 식의 일 실시 예이다. 수학식 17은 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 일반적인 구조를 갖는 취약점 노드 V_{xy}의 취약 점수이며, 수학식 18은 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 자식 노드와 OR 구조를 갖는 취약점 노드 V_{xy}의 취약 점수, 수학식 19는 i번째 보안 제어 항목에 보안 투자 금액 z_i를 투자한 후의 자식 노드와 AND 구조를 갖는 취약점 노드 V_{xy}의 취약 점수를 나타낸 것이다.

수학식 17

[0146] $$F_{xy}(z_i) = M(z_i, v\,V_{xy}^0) + CV^* F_{child}$$

수학식 18

[0147] $$F_{xy}(z_i) = M(z_i, v\,V_{xy}^0) + CV^* \sum F_{child}$$

수학식 19

[0148] $$F_{xy}(z_i) = M(z_i, v\,V_{xy}^0) + CV^* \overline{F_{child}}$$

[0150] 각각의 투자 후 완화된 취약 점수는 보안 제어 항목을 중심으로 정리할 수 있으며, 투자 후의 총 취약 점수 iTVV는 다음 수학식 20과 같이 도출될 수 있다. 투자 후 총 취약 점수 iTVV는 투자 후 보안 위험을 정량적으로 평가한 값으로, 서버는 투자 전략을 수립하는 단계 40에서 TVV과 iTVV를 이용하여 투자 후 보안 위험을 투자 전 보안 위험과 비교할 수 있다.

수학식 20

[0151] $$F(SC_i) = \sum_{y=1}^{m} \sum_{x=1}^{n} F_{xy}(z_i), where\ F_{xy}(z_i) \in SC_i$$

[0152] $$iTVV = \sum_{i=1}^{k} F(SC_i)$$

[0153] 다음으로 단계 40에서 서버는 단계 30에서 정량적으로 평가한 투자 후 보안 위험이 최소가 되도록 보안 제어 항목별 최적 투자 금액을 산정할 수 있다. 일 예로, 투자금 산정부(170)는 최적화 기법인 라그랑지 승수법을 이용하여 아래 수학식 21의 하단 조건을 만족하도록 투자 금액을 산정할 수 있다.

수학식 21

[0154] $$Minimum\ iTVV = \sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n} F_{xy}(z_i)$$

[0155] $$\sum_{i=1}^{k} z_i = Z, where\ z_i | i = 1, \ldots, k \geq 0$$

[0156] 다음으로, 단계 50에서 서버는 투자 전 총 취약 점수(TVV)와 투자 후 총 취약 점수(iTVV)를 이용하여 투자 전후의 취약 점수를 비교한 결과를 사용자에게 제공할 수 있으며, 종래 기술에 따른 다른 투자 전략과의 정량적 비교를 통해 가장 우수한 투자 전략을 사용자에게 제공(추천)할 수 있다. 예를 들어, 총 투자 금액을 모든 보안 제어 항목에 동일하게 투자한 경우의 총 취약 점수를 산출하여 사용자에게 제공할 수 있으며(균등 투자), 상술한 라그랑지 승수법을 이용하여 iTVV값이 가장 작아지는 경우의 총 취약 점수를 산출하여 사용자에게 제공할 수 있다(최적 투자). 사용자는 서버가 제공한 정량화된 투자 후 보안 위험을 보안 투자를 위한 예산 사용에 참조할 수 있으며, 효과적으로 보안 투자를 실행할 수 있다.

[0157] 본 명세서에서 설명되는 방법들은 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 컴퓨터 프로그램들에 의해 구현될 수 있다. 컴퓨터 프로그램들은 비-일시적인 유형의 컴퓨터 판독가능 매체에 저장되는 프로세서-실행가능 명령들을 포함한다. 컴퓨터 프로그램들은 또한 저장된 데이터를 포함할 수 있다. 비-일시적인 유형의 컴퓨터 판독가능 매체(non-transitory tangible computer readable medium)의 비한정적 예들은 비휘발성 메모리 시스템, 자기 저장소 및 광학 저장소이다.

[0158] 앞서 설명된 기법들의 특정 실시형태들은 알고리즘 형태로 본 명세서에서 설명되는 처리 단계들 및 명령들을 포함한다. 앞서 설명된 처리 단계들 및 명령들은 소프트웨어, 펌웨어, 혹은 하드웨어로 구현될 수 있고, 소프트웨어로 구현되는 경우 실시간 네트워크 오퍼레이팅 시스템(real time network operating system)들에서 사용되는 다른 플랫폼들 상에 상주하도록 다운로드 될 수 있고 이로부터 동작될 수 있음에 유의해야만 한다.

[0159] 본 발명은 또한 본 명세서에서의 동작들을 수행하기 위한 장치와 관련된다. 이러한 장치는 원하는 목적을 위해 특별히 구성될 수 있거나, 또는 컴퓨터에 의해 액세스될 수 있는 컴퓨터 판독가능 매체 상에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화되거나 재구성되는 범용 컴퓨터를 포함할 수 있다. 이러한 컴퓨터 프로그램은 유형의 컴퓨터 판독가능 저장 매체에 저장될 수 있는바, 이러한 유형의 컴퓨터 판독가능 저장 매체는, 예를 들어, 플로피 디스크들, 광학 디스크들, CD-ROM들, 자기-광학 디스크들(magnetic-optical disks), 판독-전용 메모리(Read-Only Memory, ROM)들, 랜덤 액세스 메모리(Random Access Memory, RAM)들, EPROM들, EEPROM들, 자기 혹은 광학 카드들, 애플리케이션 특정 집적 회로(ASIC)들을 포함하는 임의 타입의 디스크, 또는 전자 명령들을 저장하기에 적합하고 그 각각이 컴퓨터 시스템 버스에 결합되는 임의 타입의 매체들이 있지만 이러한 것으로만 한정되는 것은 아니다. 더욱이, 본 명세서에서 지칭되는 컴퓨터들은 단일 프로세서를 포함할 수 있거나, 또는 컴퓨팅 능력 증진을 위해 복수의 프로세서 설계를 사용하는 아키텍처들일 수 있다.

[0160] 본 명세서에 제시되는 알고리즘들 및 동작들은 본질적으로 임의의 특정 컴퓨터 혹은 다른 장치들과 관련되지 않는다. 다양한 범용 시스템들이 또한, 본 명세서에서의 가르침에 따른 프로그램들과 함께 사용될 수 있고, 또는 원하는 방법의 단계들을 수행하기 위해 더 특수하게 설계된 장치들을 구성하는 것이 편리한 것으로 판명될 수 있다. 다양한 이러한 시스템들을 위해 그 요구되는 구조는 그 등가적 변형물들과 함께 본 발명의 기술 분야에서 숙련된 자들에게 명백할 것이다. 추가적으로, 본 개시내용은 임의의 특정 프로그래밍 언어와 관련되어 설명되는 것이 아니다. 다양한 프로그래밍 언어가 본 명세서에서 설명되는 바와 같은 본 개시내용의 가르침들을 구현하기 위해 사용될 수 있고, 특정 언어에 대한 임의의 언급은 본 발명의 실시예 및 최상의 모드를 설명하기 위한 것임을 이해해야 한다.

[0161] 본 명세서에서 생략된 일부 실시 예는 그 실시 주체가 동일한 경우 동일하게 적용 가능하다. 또한, 전술한 본 발명은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시 예 및 첨부된 도면에 의해 한정되는

것이 아니다.

부호의 설명

[0163] 100: 보안 위험 평가 기반 보안 투자 장치(서버)

110: 환경 설정부

130: 공격 트리 맵 생성부

140: 가중치 결정부

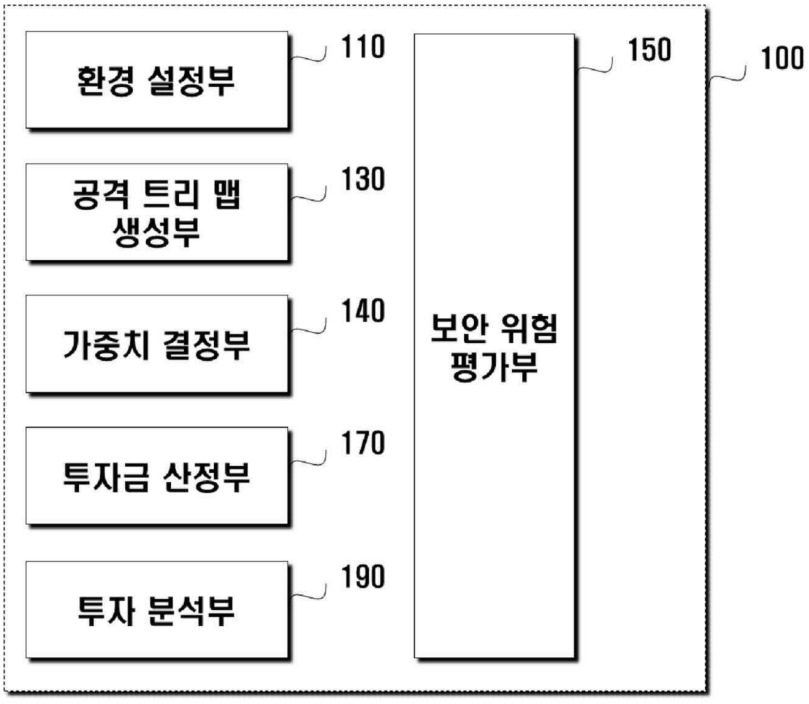
150: 보안 위험 평가부

170: 투자금 산정부

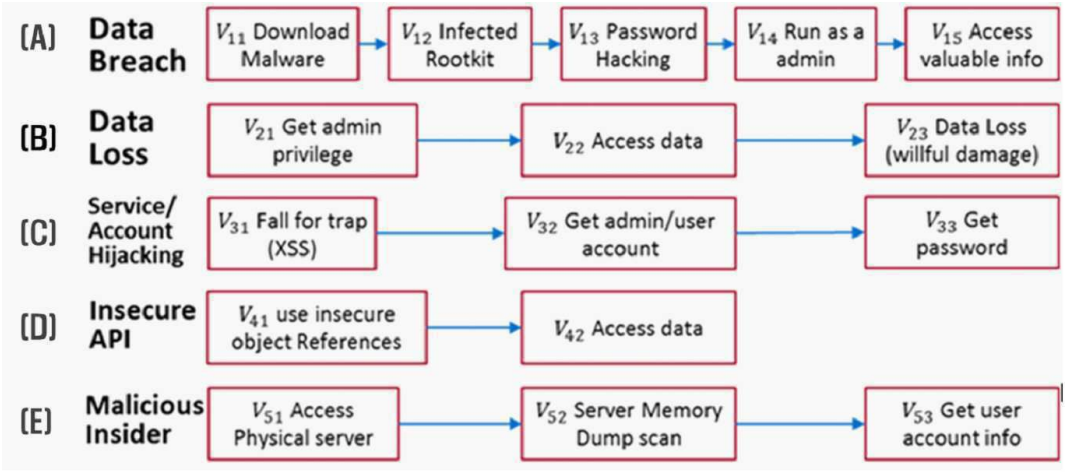
190: 투자 분석부

도면

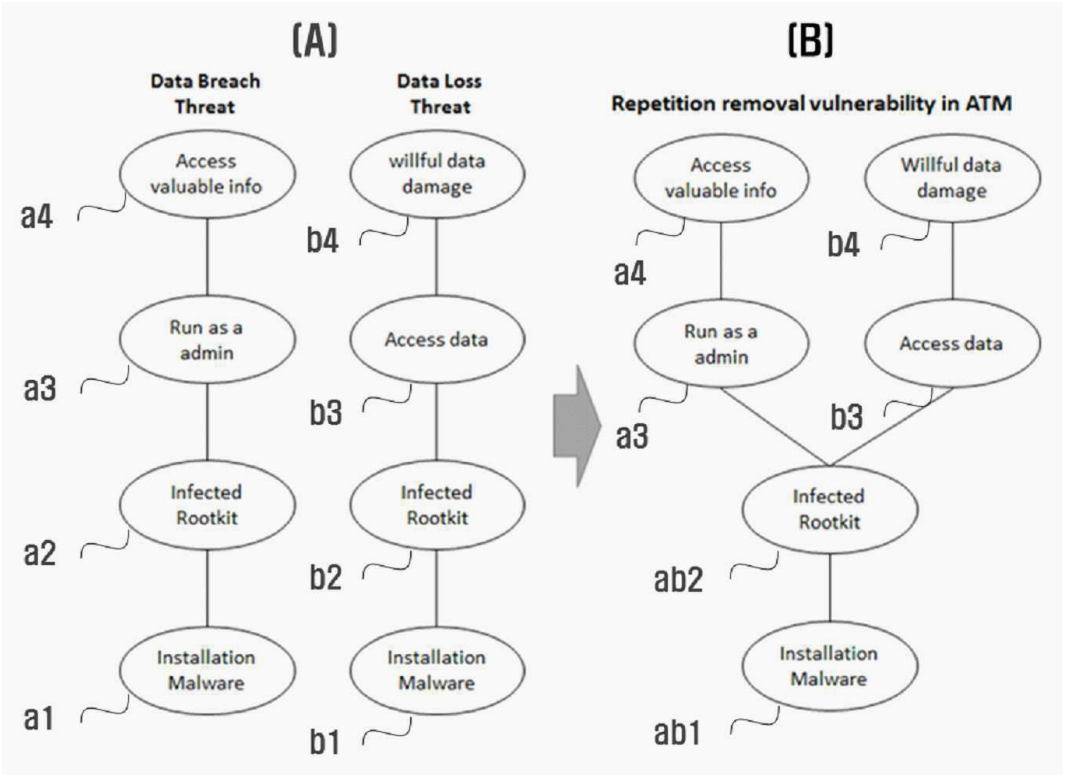
도면1



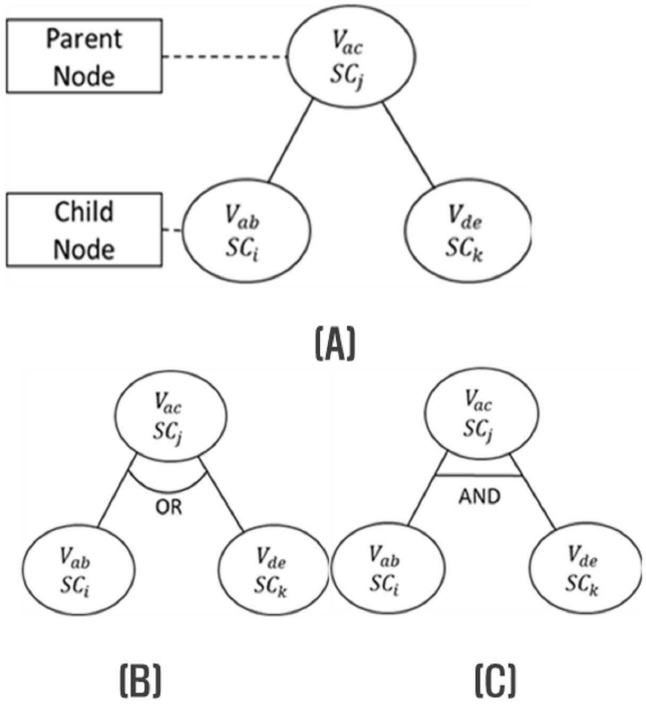
도면2


(A) Data Breach
V_{11} Download Malware
V_{12} Infected Rootkit
V_{13} Password Hacking
V_{14} Run as a admin
V_{15} Access valuable info
(B) Data Loss
V_{21} Get admin privilege
V_{22} Access data
V_{23} Data Loss (willful damage)
(C) Service/ Account Hijacking
V_{31} Fall for trap (XSS)
V_{32} Get admin/user account
V_{33} Get password
(D) Insecure API
V_{41} use insecure object References
V_{42} Access data
(E) Malicious Insider
V_{51} Access Physical server
V_{52} Server Memory Dump scan
V_{53} Get user account info

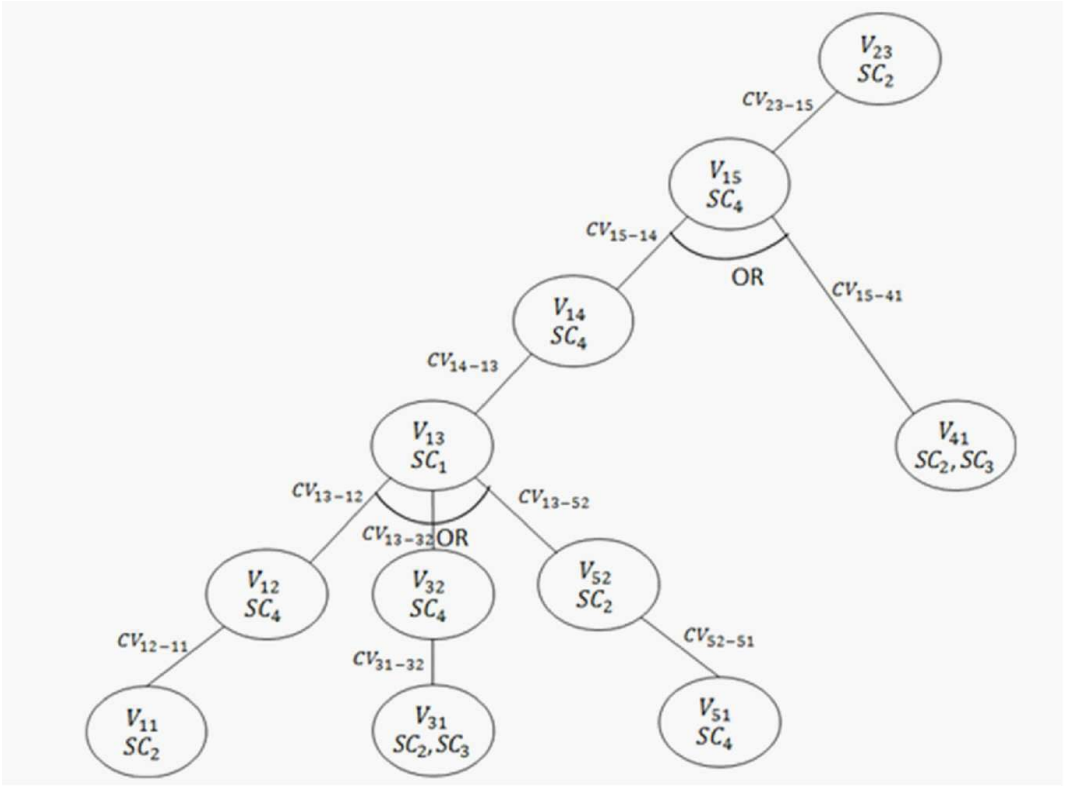
도면3


(A)
Data Breach Threat
Access valuable info
a4
Run as a admin
a3
Infected Rootkit
a2
Installation Malware
a1
Data Loss Threat
willful data damage
b4
Access data
b3
Infected Rootkit
b2
Installation Malware
b1
(B)
Repetition removal vulnerability in ATM
Access valuable info
a4
Willful data damage
b4
Run as a admin
a3
Access data
b3
Infected Rootkit
ab2
Installation Malware
ab1

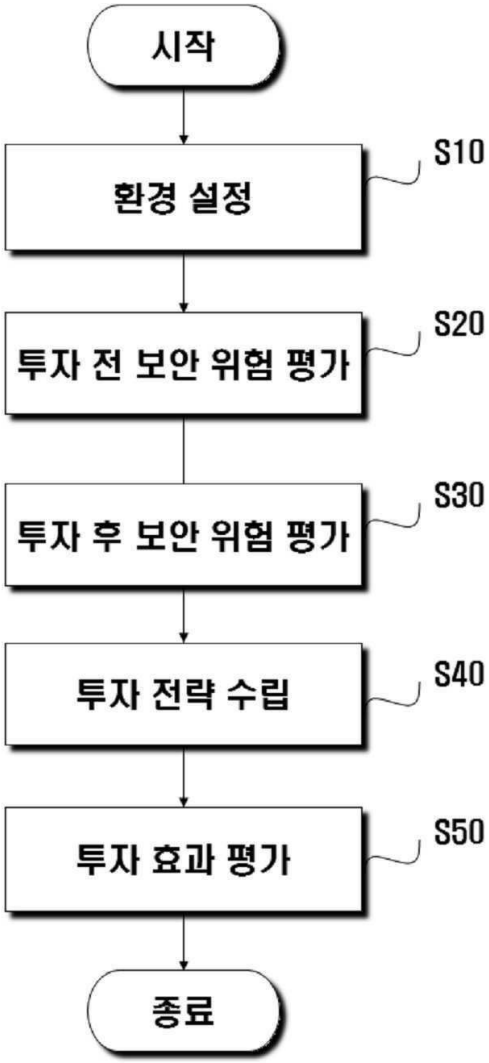
도면4


Parent Node
Child Node
V_{ac} SC_j
V_{ab} SC_i
V_{de} SC_k
(A)
OR
AND
(B)
(C)

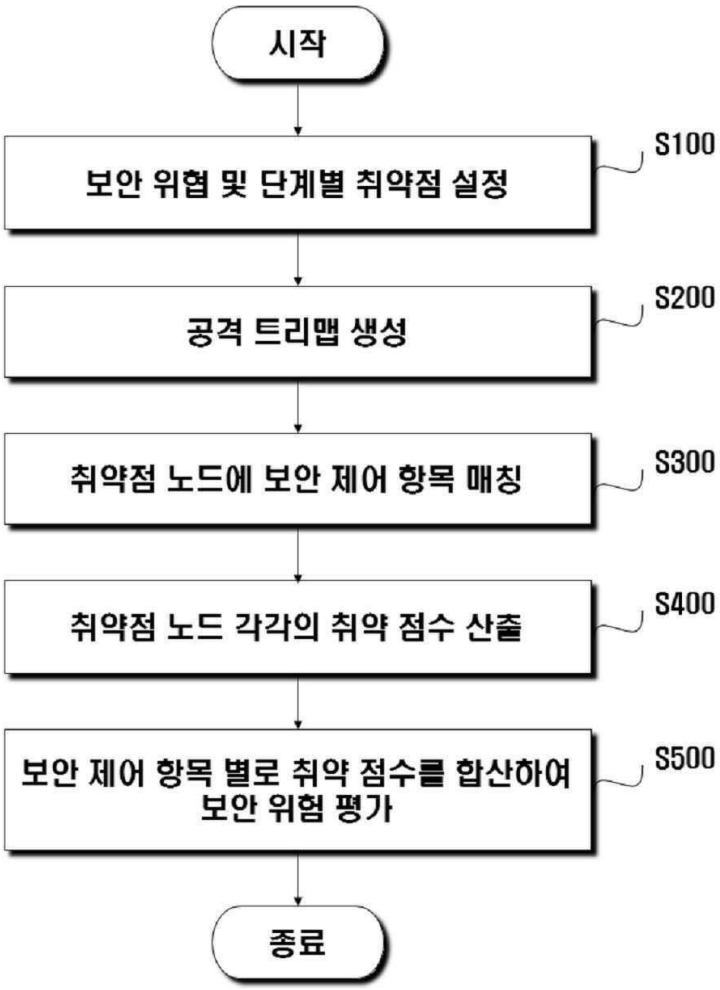
도면5


V_{23} SC_2
CV_{23-15}
V_{15} SC_4
CV_{15-14}
OR
CV_{15-41}
V_{14} SC_4
CV_{14-13}
V_{13} SC_1
V_{41} SC_2, SC_3
CV_{13-12}
CV_{13-32}
OR
CV_{13-52}
V_{12} SC_4
V_{32} SC_4
V_{52} SC_2
CV_{12-11}
CV_{31-32}
CV_{52-51}
V_{11} SC_2
V_{31} SC_2, SC_3
V_{51} SC_4

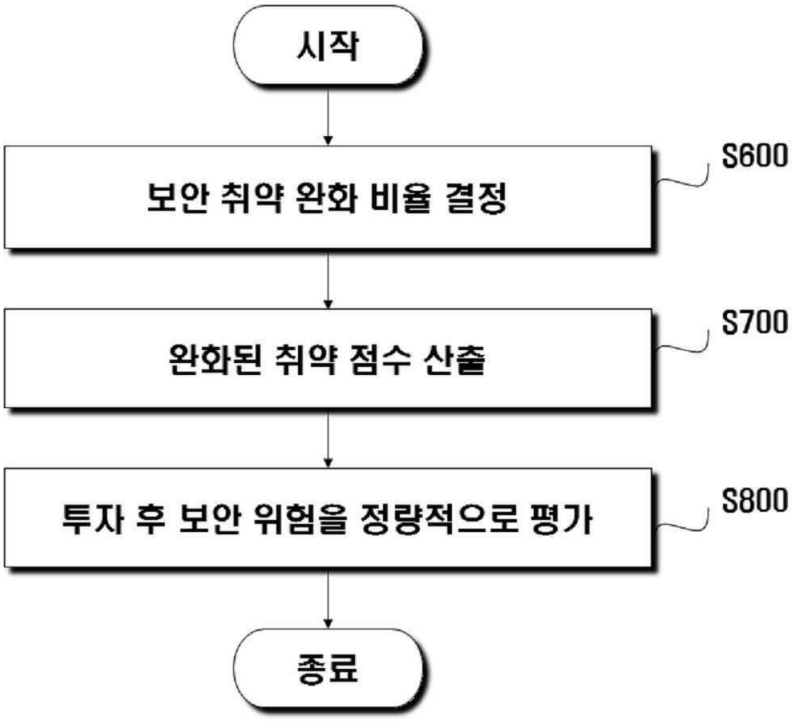
도면6


시작
환경 설정
S10
투자 전 보안 위험 평가
S20
투자 후 보안 위험 평가
S30
투자 전략 수립
S40
투자 효과 평가
S50
종료

도면7


시작
보안 위협 및 단계별 취약점 설정
S100
공격 트리맵 생성
S200
취약점 노드에 보안 제어 항목 매칭
S300
취약점 노드 각각의 취약 점수 산출
S400
보안 제어 항목 별로 취약 점수를 합산하여 보안 위험 평가
S500
종료

도면8


시작
보안 취약 완화 비율 결정
S600
완화된 취약 점수 산출
S700
투자 후 보안 위험을 정량적으로 평가
S800
종료