



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0032897
(43) 공개일자 2023년03월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G06F 21/57 (2013.01)
H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 63/1433 (2013.01)
G06F 21/577 (2013.01)
(21) 출원번호 10-2022-0098296
(22) 출원일자 2022년08월08일
심사청구일자 2022년08월08일
(30) 우선권주장
1020210114588 2021년08월30일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김승주
서울특별시 강남구 도곡로57길 12, 103동 503호(역삼동, 역삼2차아파트)
박신철
서울특별시 종로구 종로31길 54, 1204호(연지동)
(뒷면에 계속)
(74) 대리인
이대호, 박건홍

전체 청구항 수 : 총 12 항

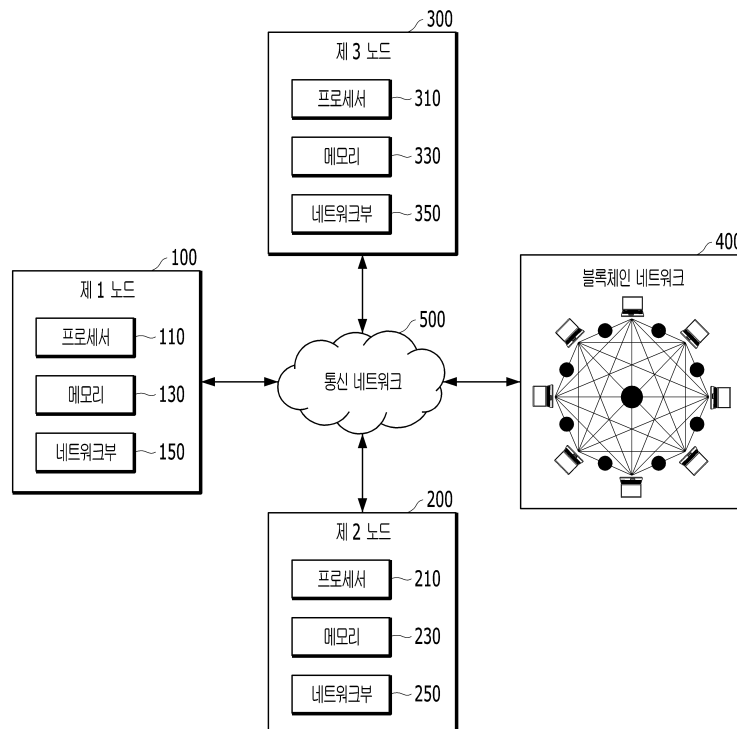
(54) 발명의 명칭 **블록체인 기술을 이용한 위협 모델링 방법**

(57) 요약

본 개시의 일 실시예에 따라, 블록체인 네트워크를 구성하는 제 1 노드에 의해 수행되는 위협 모델링 방법으로서, 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 상기 블록체인 네트워크를 통해 획득하는 단계; 상기 작업 요청에 응답하여, 상기 데이터에 기초하여 수행된 위협 모델링의 결과물을 생성하는 단

(뒷면에 계속)

대표도 - 도1



계; 및 상기 결과물에 대한 평가 정보 및 상기 평가 정보에 대한 검증 정보가 생성될 수 있도록, 상기 위협 모델링의 결과물을 상기 블록체인 네트워크에 전송하는 단계;를 포함하고, 상기 평가 정보는, 상기 블록체인 네트워크를 구성하는 제 2 노드에서, 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 결과물에 대한 평가를 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 상기 검증 정보는, 상기 블록체인 네트워크를 구성하는 제 3 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고 상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정될 수 있다.

(52) CPC특허분류

H04L 63/1441 (2013.01)

H04L 9/50 (2022.05)

H04L 2463/102 (2013.01)

(72) 발명자

홍바울

서울특별시 동작구 장승배기로4길 9, 120동 1203호(상도동, 상도 더샵아파트)

김예준

서울특별시 성북구 고려대로12길 32, 303호(안암동3가)

조광수

서울특별시 은평구 불광로2길 33(불광동, 북한산힐스테이트1차아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711134736

과제번호 2021-0-00613-001

부처명 과학기술정보통신부

과제관리(전문)기관명 정보통신기획평가원

연구사업명 유망 신기술 및 글로벌선도기술 확보

연구과제명 언택트 시대의 기업망 보호를 위한 제로 트러스트 기반 접근제어 및 이상징후 분석

기술 개발

기 여 율 1/1

과제수행기관명 에스지에이솔루션즈 주식회사

연구기간 2021.04.01 ~ 2024.12.31

명세서

청구범위

청구항 1

블록체인 네트워크를 구성하는 제 1 노드에 의해 수행되는 위협 모델링 방법으로서,
 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 상기 블록체인 네트워크를 통해 획득하는 단계;
 상기 작업 요청에 응답하여, 상기 데이터에 기초하여 수행된 위협 모델링의 결과물을 생성하는 단계; 및
 상기 결과물에 대한 평가 정보 및 상기 평가 정보에 대한 검증 정보가 생성될 수 있도록, 상기 위협 모델링의 결과물을 상기 블록체인 네트워크에 전송하는 단계;
 를 포함하고,
 상기 평가 정보는,
 상기 블록체인 네트워크를 구성하는 제 2 노드에서, 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 결과물에 대한 평가를 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고,
 상기 검증 정보는,
 상기 블록체인 네트워크를 구성하는 제 3 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고
 상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정되는,
 방법.

청구항 2

제 1 항에 있어서,
 상기 데이터는,
 데이터 흐름도(data flow diagram, DFD)를 포함하는 시스템 모델의 데이터 또는 아키텍처(architecture)의 데이터 중 적어도 하나를 포함하는,
 방법.

청구항 3

제 1 항에 있어서,
 상기 위협 모델링의 결과물은,
 시스템 모델의 작성에 관한 작업 정보, 공격 라이브러리의 수집에 관한 작업 정보, 위협의 식별에 관한 작업 정보, 공격 시나리오의 작성에 관한 작업 정보, 위협도의 평가에 관한 작업 정보 및 완화대책 마련에 관한 작업 정보 중 적어도 하나를 포함하는,
 방법.

청구항 4

제 1 항에 있어서,
상기 평가 정보는,
상기 위협 모델링의 결과물에 포함된 작업 정보별로 각각 평가되어 산출된 점수(point)를 포함하는,
방법.

청구항 5

제 1 항에 있어서,
상기 사전 결정된 평가 기준은,
상기 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보의 경우, 상기 시스템 모델의 수준,
상기 시스템 모델의 객체 작성 여부 및 상기 시스템 모델의 데이터 흐름 작성 여부를 기준으로 하는,
방법.

청구항 6

제 1 항에 있어서,
상기 사전 결정된 평가 기준은,
상기 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보의 경우, 상기 공격 라이브러리의
공통 취약점 등급 시스템(common vulnerability scoring system) 점수 및 상기 공격 라이브러리의 사용처를
기준으로 하는,
방법.

청구항 7

제 1 항에 있어서,
상기 사전 결정된 평가 기준은,
상기 위협 모델링의 결과물에 포함된 위협의 식별에 관한 작업 정보의 경우, 타겟에 대한 위협 정도를 기준으로
하는,
방법.

청구항 8

제 1 항에 있어서,
상기 사전 결정된 평가 기준은,
상기 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보의 경우, 공격 트리 각 항목의 개
수 및 유효 공격 시나리오 작성 여부를 기준으로 하는,
방법.

청구항 9

제 1 항에 있어서,

상기 사전 결정된 평가 기준은,

상기 위협 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보의 경우, 상기 블록체인 네트워크에 포함된 복수의 노드들의 투표 결과를 기준으로 하는, 방법.

청구항 10

제 1 항에 있어서,

상기 사전 결정된 평가 기준은,

상기 위협 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보의 경우, 상기 블록체인 네트워크에 포함된 복수의 노드들의 투표 결과를 기준으로 하는, 방법.

청구항 11

블록체인 네트워크를 구성하는 제 2 노드에 의해 수행되는 위협 모델링 방법으로서,

데이터에 기초하여 수행된 위협 모델링의 결과물을 상기 블록체인 네트워크를 통해 획득하는 단계;

사전 결정된 평가 기준에 기초하여 상기 결과물에 대한 평가를 통해 평가 정보를 생성하는 단계; 및

상기 평가 정보에 대한 검증 정보가 생성될 수 있도록, 상기 평가 정보를 상기 블록체인 네트워크에 전송하는 단계;

를 포함하고,

상기 위협 모델링의 결과물은,

상기 블록체인 네트워크를 구성하는 제 1 노드에서, 상기 블록체인 네트워크를 통해 획득된 상기 데이터를 포함하는 작업 요청에 응답하여, 상기 데이터에 기초한 수행을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고,

상기 검증 정보는,

상기 블록체인 네트워크를 구성하는 제 3 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고

상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정되는,

방법.

청구항 12

블록체인 네트워크를 구성하는 제 3 노드에 의해 수행되는 위협 모델링 방법으로서,

사전 결정된 평가 기준에 기초하여, 위협 모델링의 결과물에 대한 평가를 통해 생성된 평가 정보를 상기 블록체인 네트워크를 통해 획득하는 단계;

상기 사전 결정된 평가 기준에 기초하여 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 검증 정보를 생성하는 단계; 및

상기 검증 정보를 상기 블록체인 네트워크에 전송하는 단계;

를 포함하고,

상기 위협 모델링의 결과물은,

상기 블록체인 네트워크를 구성하는 제 1 노드에서, 상기 블록체인 네트워크를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 상기 데이터에 기초한 수행을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고,

상기 평가 정보는,

상기 블록체인 네트워크를 구성하는 제 2 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 결과물에 대한 평가를 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고,

상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트 (smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정되는,

방법.

발명의 설명

기술 분야

[0001] 본 개시 내용은 위협 모델링 방법에 관한 것으로, 보다 구체적으로 블록체인 기술을 이용한 위협 모델링 방법에 관한 것이다.

배경 기술

[0002] 정보통신기술(Information & Communication Technology, ICT)의 발달로 인하여 다양한 사이버보안 위협이 증가하고 있다. 따라서, 정보 시스템의 보안 문제로 인한 심각한 재정적 손실이나 인명 피해가 발생할 수 있다. 이러한 보안 문제의 일부는 잘못된 설계로 인해 발생되고 있다. 대부분의 시스템은 보안 기능에 대해서 제대로 설계하지 않고, 시큐어 코딩(secure coding)이나 모의 해킹에 의존하여 보안 기능을 구현하고 있다.

[0003] 보안 기능을 제대로 설계하지 않은 시스템에서 보안 기능의 요구사항을 도출하여 다시 설계할 경우, 시스템의 취약점의 개수는 줄어들 수 있다. 따라서, 보안 기능의 요구사항을 분석하는 단계가 시스템의 개발 초기에 필요할 수 있다.

[0004] 위협 모델링 기법은 보안기능 요구사항을 도출하기 위해서 일반적으로 사용될 수 있다. 위협 모델링은 분석 대상의 자산, 발생 가능한 취약점, 잠재적 위협을 식별하고 열거하며 완화 조치의 우선순위를 지정하는 체계적인 보안성 분석 방법일 수 있다.

[0005] 위협 모델링은 개인이 혼자서 수행하는 것보다 여러 영역의 전문가들이 함께 수행할 때 최선의 결과가 도출될 수 있다. 따라서, 여러 영역의 전문가들이 위협 모델링에 참여하도록 적절한 평가 및 검증을 통해 보상을 지급하는 것이 중요할 수 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허 제10-0862187호(2008.10.01. 등록)

발명의 내용

해결하려는 과제

[0007] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 블록체인 기술을 이용한 위협 모델링 방법을 제공하고자 한다.

[0008] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과

제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0009] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 블록체인 네트워크를 구성하는 제 1 노드에 의해 수행되는 위협 모델링 방법으로서, 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 상기 블록체인 네트워크를 통해 획득하는 단계; 상기 작업 요청에 응답하여, 상기 데이터에 기초하여 수행된 위협 모델링의 결과물을 생성하는 단계; 및 상기 결과물에 대한 평가 정보 및 상기 평가 정보에 대한 검증 정보가 생성될 수 있도록, 상기 위협 모델링의 결과물을 상기 블록체인 네트워크에 전송하는 단계;를 포함하고, 상기 평가 정보는, 상기 블록체인 네트워크를 구성하는 제 2 노드에서, 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 결과물에 대한 평가를 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 상기 검증 정보는, 상기 블록체인 네트워크를 구성하는 제 3 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고 상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정될 수 있다.
- [0010] 대안적으로, 상기 데이터는, 데이터 흐름도(data flow diagram, DFD)를 포함하는 시스템 모델의 데이터 또는 아키텍처(architecture)의 데이터 중 적어도 하나를 포함할 수 있다.
- [0011] 대안적으로, 상기 위협 모델링의 결과물은, 시스템 모델의 작성에 관한 작업 정보, 공격 라이브러리의 수집에 관한 작업 정보, 위협의 식별에 관한 작업 정보, 공격 시나리오의 작성에 관한 작업 정보, 위험도의 평가에 관한 작업 정보 및 완화대책 마련에 관한 작업 정보 중 적어도 하나를 포함할 수 있다.
- [0012] 대안적으로, 상기 평가 정보는, 상기 위협 모델링의 결과물에 포함된 작업 정보별로 각각 평가되어 산출된 점수(point)를 포함할 수 있다.
- [0013] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보의 경우, 상기 시스템 모델의 수준, 상기 시스템 모델의 객체 작성 여부 및 상기 시스템 모델의 데이터 흐름 작성 여부를 기준으로 할 수 있다.
- [0014] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보의 경우, 상기 공격 라이브러리의 공통 취약점 등급 시스템(common vulnerability scoring system) 점수 및 상기 공격 라이브러리의 사용처를 기준으로 할 수 있다.
- [0015] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 위협의 식별에 관한 작업 정보의 경우, 타겟에 대한 위협 정도를 기준으로 할 수 있다.
- [0016] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보의 경우, 공격 트리 각 항목의 개수 및 유효 공격 시나리오 작성 여부를 기준으로 할 수 있다.
- [0017] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보의 경우, 상기 블록체인 네트워크에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다.
- [0018] 대안적으로, 상기 사전 결정된 평가 기준은, 상기 위협 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보의 경우, 상기 블록체인 네트워크에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다.
- [0019] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 다른 실시예에 따라, 블록체인 네트워크를 구성하는 제 2 노드에 의해 수행되는 위협 모델링 방법으로서, 데이터에 기초하여 수행된 위협 모델링의 결과물을 상기 블록체인 네트워크를 통해 획득하는 단계; 사전 결정된 평가 기준에 기초하여 상기 결과물에 대한 평가를 통해 평가 정보를 생성하는 단계; 및 상기 평가 정보에 대한 검증 정보가 생성될 수 있도록, 상기 평가 정보를 상기 블록체인 네트워크에 전송하는 단계;를 포함하고, 상기 위협 모델링의 결과물은, 상기 블록체인 네트워크를 구성하는 제 1 노드에서, 상기 블록체인 네트워크를 통해 획득된 상기 데이터를 포함하는 작업 요청에 응답하여, 상기 데이터에 기초한 수행을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 상기 검증 정보는, 상기 블록체인 네트워크를 구성하는 제 3 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고 상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장

된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정될 수 있다.

[0020] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 또 다른 실시예에 따라, 블록체인 네트워크를 구성하는 제 3 노드에 의해 수행되는 위협 모델링 방법으로서, 사전 결정된 평가 기준에 기초하여, 위협 모델링의 결과물에 대한 평가를 통해 생성된 평가 정보를 상기 블록체인 네트워크를 통해 획득하는 단계; 상기 사전 결정된 평가 기준에 기초하여 상기 평가 정보의 생성의 유효성에 대한 검증을 통해 검증 정보를 생성하는 단계; 및 상기 검증 정보를 상기 블록체인 네트워크에 전송하는 단계;를 포함하고, 상기 위협 모델링의 결과물은, 상기 블록체인 네트워크를 구성하는 제 1 노드에서, 상기 블록체인 네트워크를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 상기 데이터에 기초한 수행을 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 상기 평가 정보는, 상기 블록체인 네트워크를 구성하는 제 2 노드에서, 상기 사전 결정된 평가 기준에 기초하여 상기 블록체인 네트워크를 통해 획득된 상기 결과물에 대한 평가를 통해 생성되고, 그리고 상기 블록체인 네트워크에 전송되고, 그리고 상기 평가 정보의 생성에 대한 유효성이 검증된 경우, 상기 블록체인 네트워크 상에 저장된 스마트 컨트랙트(smart contract)에 의해 상기 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정될 수 있다.

발명의 효과

[0021] 본 개시는 블록체인 기술을 이용하여 위협 모델링을 원활하게 수행할 수 있다.

[0022] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0023] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시될 수 있음은 명백할 것이다.

도 1은 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링 방법을 제공하기 위한 시스템의 블록 구성도이다.

도 2는 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링을 수행하기 위한 아키텍처 계층(architecture layer) 구조를 나타내는 도면이다.

도 3은 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 1 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.

도 4는 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 2 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.

도 5는 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 3 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.

도 6은 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링 방법의 순서도이다.

도 7은 본 개시의 내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 다양한 실시예들이 이제 도면을 참조하여 설명된다. 본 명세서에서, 다양한 설명들이 본 개시의 이해를 제공하기 위해서 제시된다. 그러나, 이러한 실시예들은 이러한 구체적인 설명 없이도 실행될 수 있음이 명백하다.

[0025] 본 명세서에서 사용되는 용어 "컴포넌트", "모듈", "시스템" 등은 컴퓨터-관련 엔티티, 하드웨어, 펌웨어, 소프트웨어, 소프트웨어 및 하드웨어의 조합, 또는 소프트웨어의 실행을 지칭한다. 예를 들어, 컴포넌트는 프로세서 상에서 실행되는 처리과정(procedure), 프로세서, 객체, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수 있지만, 이들로 제한되는 것은 아니다. 예를 들어, 컴퓨팅 장치에서 실행되는 애플리케이션 및 컴퓨팅 장치 모두 컴포넌

트일 수 있다. 하나 이상의 컴포넌트는 프로세서 및/또는 실행 스레드 내에 상주할 수 있다. 일 컴포넌트는 하나의 컴퓨터 내에 로컬화 될 수 있다. 일 컴포넌트는 2개 이상의 컴퓨터들 사이에 분배될 수 있다. 또한, 이러한 컴포넌트들은 그 내부에 저장된 다양한 데이터 구조들을 갖는 다양한 컴퓨터 판독가능한 매체로부터 실행할 수 있다. 컴포넌트들은 예를 들어 하나 이상의 데이터 패킷들을 갖는 신호(예를 들면, 로컬 시스템, 분산 시스템에서 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터 및/또는 신호를 통해 다른 시스템과 인터넷과 같은 네트워크를 통해 전송되는 데이터)에 따라 로컬 및/또는 원격 처리들을 통해 통신할 수 있다.

[0026] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이탬들 중 하나 이상의 아이탬의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0027] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하는 것으로 이해되어야 한다. 다만, "포함한다" 및/또는 "포함하는"이라는 용어는, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0028] 그리고, "A 또는 B 중 적어도 하나"이라는 용어는, "A만을 포함하는 경우", "B 만을 포함하는 경우", "A와 B의 구성으로 조합된 경우"를 의미하는 것으로 해석되어야 한다.

[0029] 당업자들은 추가적으로 여기서 개시된 실시예들과 관련되어 설명된 다양한 예시적 논리적 블록들, 구성들, 모듈들, 회로들, 수단들, 로직들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽 모두의 조합들로 구현될 수 있음을 인식해야 한다. 하드웨어 및 소프트웨어의 상호교환성을 명백하게 예시하기 위해, 다양한 예시적 컴포넌트들, 블록들, 구성들, 수단들, 로직들, 모듈들, 회로들, 및 단계들은 그들의 기능성 측면에서 일반적으로 위에서 설명되었다. 그러한 기능성이 하드웨어로 또는 소프트웨어로서 구현되는지 여부는 전반적인 시스템에 부과된 특정 어플리케이션(application) 및 설계 제한들에 달려 있다. 숙련된 기술자들은 각각의 특정 어플리케이션들을 위해 다양한 방법들로 설명된 기능성을 구현할 수 있다. 다만, 그러한 구현의 결정들이 본 개시내용의 영역을 벗어나게 하는 것으로 해석되어서는 안된다.

[0030] 제시된 실시예들에 대한 설명은 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이다. 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어나지 않고 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 여기에 제시된 실시예 들로 한정되는 것이 아니다. 본 발명은 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의 범위에서 해석되어야 할 것이다.

[0031] 본 개시내용에서의 제 1, 제 2, 또는 제 3 과 같이 제 N 으로 표현되는 용어들은 적어도 하나의 엔티티들을 구분하기 위해 사용된다. 예를 들어, 제 1 과 제 2로 표현된 엔티티들은 서로 동일하거나 또는 상이할 수 있다.

[0033] 도 1은 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링 방법을 제공하기 위한 시스템의 블록 구성도이다.

[0034] 도 1에 도시된 블록체인 기술을 이용한 위협 모델링 방법을 제공하기 위한 시스템의 구성은 간략화 하여 나타낸 예시일 뿐이다. 본 개시의 일 실시예에서 블록체인 기술을 이용한 위협 모델링 방법을 제공하기 위한 시스템은 위협 모델링 방법을 제공하기 위한 다른 구성들이 포함될 수 있고, 개시된 구성들 중 일부만이 컴퓨팅 장치를 구성할 수도 있다.

[0035] 도 1을 참조하면, 블록체인 기술을 이용한 위협 모델링 방법을 제공하기 위한 시스템은 제 1 노드(100), 제 2 노드(200), 제 3 노드(300), 블록체인 네트워크(400) 및/또는 통신 네트워크(500) 중 적어도 하나를 포함할 수 있다. 제 1 노드(100), 제 2 노드(200) 및/또는 제 3 노드(300) 중 적어도 하나는 블록체인 네트워크(400)를 구성하는 노드일 수 있다. 예를 들어, 제 1 노드(100), 제 2 노드(200) 및 제 3 노드(300)는 각각 블록체인 네트워크(400)를 구성하는 노드일 수 있다.

- [0037] 본 개시의 몇몇 실시예에 따른 제 1 노드(100)는 보상을 받기 위해 블록체인 네트워크(400)에 참여한 노드일 수 있다. 제 1 노드(100)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다. 제 1 노드(100)는 블록체인 네트워크(400)를 구성하는 노드일 수 있다. 제 1 노드(100)는 적어도 하나일 수 있고, 복수로 구성될 수도 있다.
- [0038] 제 1 노드(100)는 프로세서(110), 메모리(130), 네트워크부(150)를 포함할 수 있다. 프로세서(110)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치(GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석을 위한 프로세서를 포함할 수 있다. 프로세서(110)는 통상적으로 제 1 노드(100)의 전반적인 동작을 제어할 수 있다. 예를 들어, 프로세서(110)는 제 1 노드(100)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 프로세서(110)는 메모리(130)에 저장된 컴퓨터 프로그램을 관독하여 본 개시의 일 실시예에 따른 데이터 처리를 수행할 수 있다.
- [0039] 본 개시의 몇몇 실시예에 따르면, 메모리(130)는 프로세서(110)가 생성하거나 결정한 임의의 형태의 정보 및 네트워크부(150)가 수신한 임의의 형태의 정보를 저장할 수 있다.
- [0040] 본 개시의 몇몇 실시예에 따르면, 메모리(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 제 1 노드(100)는 인터넷(internet) 상에서 상기 메모리(130)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 네트워크부(150)는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다. 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.
- [0041] 제 1 노드(100)는 위협 모델링을 수행하는 노드인 위협 모델링 수행자 노드(threat modeling performer node)일 수 있다. 제 1 노드(100)의 프로세서(110)는 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 블록체인 네트워크(400)를 통해 획득할 수 있다.
- [0042] 위협 모델링은 분석 대상의 자산, 발생 가능한 취약점 및/또는 잠재적 위협 중 적어도 하나를 식별하고 열거하며 완화 조치의 우선순위를 지정하는 체계적인 보안성 분석 방법일 수 있다.
- [0043] 프로세서(110)는 위협 모델링을 수행하는 과정에서 시스템 모델을 작성할 수 있다. 시스템 모델은 시스템의 설계를 위한 구조, 구성 등을 포함하는 도면, 3D 모델 등을 포함할 수 있다. 예를 들어, 시스템 모델은 데이터 흐름도(data flow diagram, DFD), 공정 흐름도(process flow diagram) 및/또는 통합 모델링 언어 다이어그램(unified modeling language diagram) 중 적어도 하나를 포함할 수 있다. 따라서, 프로세서(110)는 시스템의 구조에 대한 분석을 통해 주요 구성요소에 기반한 데이터 흐름도를 작성할 수 있다.
- [0044] 데이터 흐름도는 시스템의 내부 데이터 흐름을 도식적으로 표현한 것을 의미할 수 있다. 데이터 흐름도는 세부 기능 및/또는 세부 기능 간의 관계 중 적어도 하나를 표현한 도면일 수 있다.
- [0045] 공정 흐름도는 원료에서 제품 완성에 이르기까지의 공정 전체에 대해서 표시한 도면일 수 있다. 예를 들어, 공정 흐름도는 물질의 장치 간의 이동 관계를 표시한 도면, 공정에 대한 물질, 열수지 등을 표시한 도면 및/또는 장치 사이의 배관 관계를 나타낸 도면 중 적어도 하나를 포함할 수 있다.
- [0046] 통합 모델링 언어 다이어그램은 통합 모델링 언어(unified modeling language, UML)를 사용하여 시스템 상호 작용, 업무 흐름, 객체 간의 메시지 전달, 시스템의 구조, 컴포넌트 관계 등을 그린 도면일 수 있다. 예를 들어, 통합 모델링 언어 다이어그램은 요구 분석 과정에서 시스템과 외부와의 상호 작용을 묘사하는 유스케이스(use case) 다이어그램, 업무의 흐름을 모델링하거나 객체의 생명 주기를 표현하는 활성도(activity) 다이어그램, 객체 간의 메시지 전달을 시간적 흐름에서 분석하는 시퀀스(sequence) 다이어그램, 객체와 객체가 주고받는 메시지 중심의 다이어그램인 협력도(collaboration diagram), 시스템의 구조적인 모습을 그리는 Class 다이어그램,

소프트웨어 구조를 그리는 컴포넌트(component) 다이어그램 및/또는 기업 환경의 구성과 컴포넌트들 간의 관계를 그린 배치(deployment) 다이어그램 중 적어도 하나를 포함할 수 있다.

- [0047] 데이터는 위협 모델링의 수행에 요구되는 데이터일 수 있다. 예를 들어, 데이터는 시스템 모델의 데이터 및/또는 아키텍처(architecture)의 데이터 중 적어도 하나를 포함할 수 있다. 시스템 모델의 데이터는 데이터 흐름도(data flow diagram, DFD), 공정 흐름도(process flow diagram) 및/또는 통합 모델링 언어 다이어그램(unified modeling language diagram) 중 적어도 하나의 데이터를 포함할 수 있다.
- [0048] 아키텍처의 데이터는 하드웨어 및/또는 소프트웨어 중 적어도 하나를 포함한 컴퓨터 시스템 전체의 설계 방식 중 적어도 일부의 데이터일 수 있다. 프로세서(110)는 아키텍처의 데이터에 기초하여 시스템 모델의 데이터를 생성할 수 있다.
- [0049] 작업 요청은 블록체인 네트워크(400)에 포함 또는 포함되지 않은 고객(customer) 노드에서 생성될 수 있다. 즉, 고객 노드는 개인 또는 회사의 노드로서 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 생성할 수 있다. 생성된 작업 요청은 고객 노드에서 블록체인 네트워크(400)로 전송될 수 있다. 즉, 고객 노드는 생성된 작업 요청을 블록체인 네트워크(400)로 전송할 수 있다.
- [0050] 고객 노드는 프로세서, 메모리, 네트워크부를 포함할 수 있다. 고객 노드의 프로세서는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치(GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석을 위한 프로세서를 포함할 수 있다. 고객 노드의 프로세서는 통상적으로 고객 노드의 전반적인 동작을 제어할 수 있다. 예를 들어, 고객 노드의 프로세서는 고객 노드에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 고객 노드의 프로세서는 고객 노드의 메모리에 저장된 컴퓨터 프로그램을 판독하여 본 개시의 일 실시예에 따른 데이터 처리를 수행할 수 있다.
- [0051] 본 개시의 몇몇 실시예에 따르면, 고객 노드의 메모리는 고객 노드의 프로세서가 생성하거나 결정한 임의의 형태의 정보 및 고객 노드의 네트워크부가 수신한 임의의 형태의 정보를 저장할 수 있다.
- [0052] 본 개시의 몇몇 실시예에 따르면, 고객 노드의 메모리는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 고객 노드는 인터넷(internet) 상에서 고객 노드의 메모리의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 고객 노드의 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 고객 노드의 네트워크부는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다.
- [0054] 프로세서(110)는 분석 대상(예를 들어, 시스템 모델 등)의 오동작을 일으킬 수 있는 자산(예를 들어, 데이터, 관련 장치(예를 들어, 하드웨어, 소프트웨어 등), 전송 매체, 시스템 등)을 식별할 수 있다.
- [0055] 프로세서(110)는 위협 모델링을 수행하는 과정에서 공격 라이브러리의 수집을 수행할 수 있다. 예를 들어, 프로세서(110)는 복수의 자료에 기초하여 설계 대상인 시스템 모델의 취약점 및/또는 설계 대상인 시스템 모델에 대한 공격 방법 중 적어도 하나와 관련된 공격 라이브러리의 수집을 수행할 수 있다.
- [0056] 복수의 자료는 논문, 컨퍼런스, 기술문서, CVE(Common Vulnerabilities and Exposures) 및/또는 CWE(Common Weakness Enumeration) 중 적어도 하나를 통해 수집되는 자료들을 포함할 수 있다.
- [0057] 공격 라이브러리에 포함된 CVE는 대응되는 공통 취약점 등급 시스템(common vulnerability scoring system, CVSS)의 점수(score)를 포함할 수 있다. 점수는 사전 결정된 범위(예를 들어, 범위 0~10, 최소단위 0.1 등) 내에 존재할 수 있다. 프로세서(110)는 점수에 기초하여 적어도 하나의 CVE 각각에 대응되는 위험군(예를 들어, 저위험군, 중위험군, 고위험군, 치명적 위험군 등)을 결정할 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에 포함된 제 1 CVE의 점수가 0.1이상 3.9이하인 경우, 제 1 CVE를 저위험군으로 판단할 수 있다. 다른 예를 들어, 프로세서(110)는 공격 라이브러리에 포함된 제 2 CVE의 점수가 4.0이상 6.9이하인 경우, 제 2 CVE를 중위험군으로 판단할 수 있다. 또 다른 예를 들어, 프로세서(110)는 공격 라이브러리에 포함된 제 3 CVE의 점수

가 7.0이상 8.9이하인 경우, 제 3 CVE를 고위험군으로 판단할 수 있다. 또 다른 예를 들어, 프로세서(110)는 공격 라이브러리에 포함된 제 4 CVE의 점수가 9.0이상 10.0이하인 경우, 제 4 CVE를 치명적 위험군으로 판단할 수 있다.

[0058] 공격 라이브러리에 포함되는 요소(예를 들어, CVE, CWE 등)는 위협의 식별 과정 및/또는 공격 시나리오의 작성 과정 중 적어도 하나의 과정에 사용될 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에 포함되는 제 1 CVE를 위협의 식별 과정 또는 공격 시나리오의 작성 과정에서 사용할 수 있다.

[0059] 프로세서(110)는 위협 모델링을 수행하는 과정에서 위협의 식별을 수행할 수 있다. 예를 들어, 프로세서(110)는 사전 설정된 보안 속성에 기초하여, 공격 라이브러리에서 설계 대상인 시스템 모델에 대한 위협의 식별 및/또는 분류를 수행할 수 있다. 사전 설정된 보안 속성은 STRIDE(스푸핑(spoofing), 템퍼링(tampering), 부인(repudiation), 정보 공개(information disclosure), 서비스 거부(denial of service), 권한 상승(elevation of privilege))를 포함할 수 있다.

[0060] 스푸핑은 보안 속성 중 인증과 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 가짜 계정을 이용하여 시스템 권한을 획득하는 위협을 식별하고, 해당 위협을 스푸핑에 대응되는 것으로 분류할 수 있다.

[0061] 템퍼링은 보안 속성 중 무결성과 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 불법적으로 데이터를 변경하는 위협을 식별하고, 해당 위협을 템퍼링에 대응되는 것으로 분류할 수 있다.

[0062] 부인은 보안 속성 중 부인방지와 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 특정 서비스를 수행하지 않았다고 부인하거나 책임이 없다고 부인하는 위협 등을 식별하고, 해당 위협들을 부인으로 분류할 수 있다.

[0063] 정보 공개는 보안 속성 중 기밀성과 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 발생할 수 있는 접근 권한이 없는 누군가에게 정보를 제공하는 위협을 식별하고, 해당 위협을 정보 공개로 분류할 수 있다.

[0064] 서비스 거부는 보안 속성 중 가용성과 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 서비스 또는 애플리케이션(application)의 정상 수행을 방해하는 위협을 식별하고, 해당 위협을 서비스 거부로 분류할 수 있다.

[0065] 권한 상승은 보안 속성 중 권한 부여와 관련된 것일 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리에서 사전에 부여되지 않은 특정 서비스를 수행하는 권한을 특정 노드에 부여하는 위협을 식별하고, 해당 위협을 권한 상승으로 분류할 수 있다.

[0066] 프로세서(110)는 위협 모델링을 수행하는 과정에서 공격 시나리오의 작성을 수행할 수 있다. 예를 들어, 프로세서(110)는 공격 라이브러리 및 식별된 위협에 기초하여 공격 트리 및/또는 공격 시나리오를 생성할 수 있다.

[0067] 공격 시나리오는 공격자(공격 노드)가 최종 목표를 달성하기 위해 수행되는 세부적인 프로세스를 표현한 데이터일 수 있다. 예를 들어, 공격 시나리오는 공격자가 특정 권한을 가지고 있는 노드를 해킹하여 특정 권한을 사용하는 것일 수 있다.

[0068] 공격 트리는 최종 공격 목표에 대한 정보를 포함할 수 있다. 예를 들어, 공격 트리는 공격 트리의 최상위 노드에 최종 공격 목표가 배치되고, 최상위 노드와 연관된 적어도 하나의 하위 노드에 최종 공격 목표와 관련된 적어도 하나의 위협이 배치될 수 있다.

[0069] 프로세서(110)는 위협 모델링을 수행하는 과정에서 위협도의 평가를 수행할 수 있다. 프로세서(110)는 식별된 위협에 대한 위협도의 평가를 수행할 수 있다. 예를 들어, 프로세서(110)는 손상 가능성(damage potential) 정보, 재현성(reproducibility) 정보, 악용 가능성(exploitability) 정보, 사용자(affected users) 정보 및 발견 가능성(discoverability)에 기초하여 점수를 책정하고 위협도를 도출할 수 있다. 여기서, 위협도는 식별된 위협의 위험한 정도 또는 식별된 위협으로 인하여 위험성의 발생 정도를 정량적으로 나타낸 것일 수 있다. 손상 가능성 정보는 위협이 발생한 경우에 손상의 정도를 나타내는 정보를 포함할 수 있다. 예를 들어, 프로세서(110)는 위협이 발생한 경우에, 식별 문제로 인해 발생하는 손상의 정도에 기초하여 점수를 책정하고 위협도를 도출할 수 있다.

[0070] 재현성 정보는 위협을 재현하기 위한 난이도를 나타내는 정보를 포함할 수 있다. 예를 들어, 프로세서(110)는

위협을 재현하기 위한 난이도에 기초하여 점수를 책정하고 위험도를 도출할 수 있다.

- [0071] 악용 가능성 정보는 위협을 발생시키기 위한 지식의 필요성을 나타내는 정보를 포함할 수 있다. 예를 들어, 프로세서(110)는 위협을 발생시키기 위한 지식의 필요성에 기초하여 점수를 책정하고 위험도를 도출할 수 있다.
- [0072] 사용자 정보는 위협이 발생한 경우에 영향을 받는 사용자의 수(노드의 수)에 대한 정보를 포함할 수 있다. 예를 들어, 프로세서(110)는 위협이 발생한 경우에 영향을 받는 사용자의 수에 기초하여 점수를 책정하고 위험도를 도출할 수 있다.
- [0073] 발견 가능성 정보는 위협을 발견하기 위한 난이도에 대한 정보를 포함할 수 있다. 예를 들어, 프로세서(110)는 위협을 발견하기 위한 난이도에 기초하여 점수를 책정하고 위험도를 도출할 수 있다. 다만, 위험도를 평가하기 위한 평가 방법은 이에 한정되지 않는다. 따라서, 프로세서(110)는 위험도를 평가하기 위해서 다양한 평가 기법들을 사용할 수 있다.
- [0074] 프로세서(110)는 위협 모델링을 수행하는 과정에서 완화대책 마련을 수행할 수 있다. 프로세서(110)는 식별된 적어도 하나의 위협 각각으로 인해 발생하는 악영향을 완화시키기 위한 완화대책 정보를 생성할 수 있다.
- [0075] 프로세서(110)는 위험도에 기초하여 적어도 하나의 위협 각각에 대응되는 등급을 결정할 수 있다. 프로세서(110)는 제 1 위협의 위험도가 1이상 4이하인 경우, 제 1 위협은 로우(low) 등급에 대응되는 것으로 결정할 수 있다. 프로세서(110)는 제 2 위협의 위험도가 5이상 8이하인 경우, 제 2 위협은 미들(middle) 등급에 대응되는 것으로 결정할 수 있다. 프로세서(110)는 제 3 위협의 위험도가 9이상 12이하인 경우, 제 3 위협은 하이(high) 등급에 대응되는 것으로 결정할 수 있다.
- [0077] 프로세서(110)는 작업 요청에 응답하여, 작업 요청에 포함된 위협 모델링의 수행에 요구되는 데이터에 기초하여 수행된 위협 모델링의 결과물을 생성할 수 있다. 위협 모델링의 결과물은 전술한 시스템 모델의 작성에 관한 작업 정보, 공격 라이브러리의 수집에 관한 작업 정보, 위협의 식별에 관한 작업 정보, 공격 시나리오의 작성에 관한 작업 정보, 위험도의 평가에 관한 작업 정보 및/또는 완화대책 마련에 관한 작업 정보 중 적어도 하나를 포함할 수 있다.
- [0079] 프로세서(110)는 결과물에 대한 평가 정보 및 평가 정보에 대한 검증 정보가 생성될 수 있도록 위협 모델링의 결과물을 블록체인 네트워크(400)에 전송할 수 있다.
- [0080] 평가 정보는 블록체인 네트워크(400)를 구성하는 제 2 노드(200)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크를 통해 획득된 결과물에 대한 평가를 통해 생성될 수 있다. 평가 정보는 제 2 노드(200)에서 블록체인 네트워크(400)에 전송될 수 있다.
- [0081] 평가 정보는 위협 모델링의 결과물에 포함된 작업 정보별로 각각 평가되어 산출된 점수(point)를 포함할 수 있다.
- [0082] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보의 경우, 시스템 모델의 수준, 시스템 모델의 객체 작성 여부 및 시스템 모델의 데이터 흐름 작성 여부를 기준으로 할 수 있다.
- [0083] 시스템 모델의 수준은 시스템 모델의 프로세스의 세분화 정도에 기초하여 결정될 수 있다. 예를 들어, 시스템 모델에 포함된 데이터 흐름도의 수준은 레벨 0, 레벨 1 및/또는 레벨 2 중 적어도 하나를 포함할 수 있다. 레벨 0은 컨텍스트 다이어그램(context diagram)일 수 있다. 레벨 0은 시스템을 외부 엔티티(entity)와의 관계와 함께 단일 상위 수준의 프로세스로 표시한 데이터 흐름도일 수 있다. 레벨 1은 레벨 0의 데이터 흐름도에서 단일 상위 수준의 프로세스에 대한 분류를 표시한 데이터 흐름도일 수 있다. 레벨 2는 레벨 1의 데이터 흐름도에서 표시한 분류에 대한 세부 분류를 표시한 데이터 흐름도일 수 있다.
- [0084] 시스템 모델의 객체 작성은 시스템 모델에 포함되는 객체를 시스템 모델에 입력하는 것을 의미할 수 있다.
- [0085] 시스템 모델의 데이터 흐름 작성은 시스템 모델에 포함되는 객체 간에 발생하는 데이터의 이동과 관련된 표시를 시스템 모델에 입력하는 것을 의미할 수 있다.
- [0086] 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보의 점수(point)에 대한 예시는 아래의 [표 1]에 대응될 수 있다.

표 1

DFD 수준	객체 최종 작성	데이터 흐름 최종 작성
레벨 0	2점	1점
레벨 1	4점	1.5점
레벨 2	6점	2점

[0087]

[0088]

[표 1]을 참조하면, DFD 수준, 객체 최종 작성 및 데이터 흐름 최종 작성에 따라 점수가 결정될 수 있다. 객체 최종 작성 및 데이터 흐름 최종 작성은 개수별로 점수가 누적되어 결정될 수 있다. 예를 들어, 제 1 노드(100) 또는 제 2 노드(200)는 레벨 0 수준의 객체 최종 작성이 2건인 경우, 4점으로 결정할 수 있다. 제 1 노드(100) 또는 제 2 노드(200)는 레벨 0 수준의 데이터 흐름 최종 작성이 10건인 경우, 10점으로 결정할 수 있다. 제 1 노드(100) 또는 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 1 노드(100) 또는 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다. 평가 정보는 작업 정보에 포함된 각 항목에 대해서 참여 횟수, 참여 시기, 시스템 모델의 수준에 기초하여 점수가 측정될 수 있다. 보상은 점수에 비례하여 결정될 수 있다. 본 개시의 몇몇 실시예에 따르면, 제 1 노드(100)는 생성된 시스템 모델을 고객 노드에 전송할 수 있다. 제 1 노드(100)는 고객 노드로부터 시스템 모델의 작성에 관한 보상을 수신할 수 있다. 고객 노드는 생성된 시스템 모델에 대한 평가를 수행하고, 평가에 대응되는 보상을 제 1 노드(100)에 전송할 수 있다. 시스템 모델의 작성에 대한 보상은 고객 노드와 제 1 노드(100) 간의 합의에 따라 이루어질 수 있다.

[0089]

사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보의 경우, 공격 라이브러리의 공통 취약점 등급 시스템(common vulnerability scoring system) 점수 및 공격 라이브러리의 사용처를 기준으로 할 수 있다. 공격 라이브러리의 사용처는 위협의 식별 과정 및 공격 시나리오의 작성 과정을 포함할 수 있다.

[0090]

공격 라이브러리의 공통 취약점 등급 시스템 점수는 공격 라이브러리에 포함된 CVE에 대응되어 결정될 수 있다.

[0091]

공격 라이브러리의 사용처는 위협의 식별 과정 및/또는 공격 시나리오의 작성 과정 중 적어도 하나를 포함할 수 있다.

[0092]

위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보의 점수에 대한 예시는 아래의 [표 2]에 대응될 수 있다.

표 2

항목	세부항목	점수
수집된 공격 라이브러리의 공통 취약점 등급 시스템 점수	0.1~3.9	0.1점
	4.0~6.9	0.2점
	7.0~8.9	0.3점
	9.0~10.0	0.4점
공격 라이브러리	위협 식별에 사용	1점
	공격 시나리오 작성에 사용	5점

[0093]

[0094]

[표 2]를 참조하면, 수집된 공격 라이브러리의 공통 취약점 등급 시스템 점수 및 공격 라이브러리의 사용처에 따라 점수가 결정될 수 있다. 수집된 공격 라이브러리의 공통 취약점 등급 시스템 점수 및 공격 라이브러리의 사용처는 개수별로 점수가 누적되어 결정될 수 있다. 예를 들어, 제 2 노드(200)는 0.2의 CVE, 0.3의 CVE가 존재하는 경우, 0.2점으로 결정할 수 있다. 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다.

[0095]

[표 2]의 구체적인 수치는 복수의 제 2 노드들의 투표 결과에 기초하여 변경될 수 있다.

[0097]

사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 위협의 식별에 관한 작업 정보의 경우, 타겟에 대한 위협 정도를 기준으로 할 수 있다. 예를 들어, 위협이 타겟에 직접적으로 공격을 하는 경우, 제 2 노드(200)는

해당 위협을 타겟에 대한 직접적인 위협으로 결정할 수 있다. 다른 예를 들어, 위협이 타겟에 직접 공격을 하는 것이 아니 우회하여 간접적으로 공격을 하는 경우, 제 2 노드(200)는 해당 위협을 타겟에 대한 간접적인 위협으로 결정할 수 있다.

[0098] 위협 모델링의 결과물에 포함된 위협의 식별에 관한 작업 정보의 점수에 대한 예시는 STRIDE 위협 모델링 기법을 기준으로 아래의 [표 3]에 대응될 수 있다.

표 3

[0099]	항목	세부 항목	점수
	위협 식별	타겟에 대한 간접적인 위협	1점
		타겟에 대한 직접적인 위협	2점

[0100] [표 3]을 참조하면, 수집된 공격 라이브러리의 공통 취약점 등급 시스템 점수 및 공격 라이브러리의 사용처에 따라 점수가 결정될 수 있다. 수집된 공격 라이브러리의 공통 취약점 등급 시스템 점수 및 공격 라이브러리의 사용처는 개수별로 점수가 누적되어 결정될 수 있다. 예를 들어, 제 2 노드(200)는 0.2의 CVE, 0.3의 CVE가 존재하는 경우, 0.2점으로 결정할 수 있다. 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다.

[0101] [표 3]의 구체적인 수치는 복수의 제 2 노드들의 투표 결과에 기초하여 변경될 수 있다.

[0103] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보의 경우, 공격 트리 각 항목의 개수 및 유효 공격 시나리오 작성 여부를 기준으로 할 수 있다.

[0104] 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보의 점수에 대한 예시는 아래의 [표 4]에 대응될 수 있다.

표 4

[0105]	항목	점수
	작성된 공격 트리 각 항목의 작성	0.1점
	유효 공격 시나리오 최종 작성	5점

[0106] [표 4]를 참조하면, 공격 트리 각 항목의 개수 및 유효 공격 시나리오 최종 작성 여부에 따라 점수가 결정될 수 있다. 공격 트리 각 항목의 개수 및 유효 공격 시나리오 최종 작성 여부는 개수별로 점수가 누적되어 결정될 수 있다. 예를 들어, 제 2 노드(200)는 공격 트리의 각 항목이 2개 작성된 경우, 0.2점으로 결정할 수 있다. 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다.[표 4]의 구체적인 수치는 복수의 제 2 노드들의 투표 결과에 기초하여 변경될 수 있다.

[0108] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다. 예를 들어, 제 2 노드(200)는 제 1 노드(100) 및 제 2 노드(200)가 참여한 전체 투표 결과와 제 1 노드(100)의 투표 결과를 비교하여 투표 결과의 오차를 산출할 수 있다. 제 2 노드(200)는 투표 결과의 오차에 기초하여 점수를 결정할 수 있다.

[0109] 위협 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보의 점수에 대한 예시는 아래의 [표 5]에 대응될 수 있다.

표 5

[0110]	항목	점수
	위험도 평가 투표 참여시	1점
	투표 결과 오차 0.5 미만	5점

투표 결과 오차 0.5 이상 1 미만	3점
투표 결과 오차 1 이상 1.5 미만	1점
투표 결과 오차 1.5 이상	0점

[0111] [표 5]를 참조하면, 위험도 평가 투표 참여 여부 및 투표 결과 오차에 따라 점수가 결정될 수 있다. 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위험 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다.

[0112] [표 5]의 구체적인 점수는 복수의 제 2 노드들의 투표 결과에 기초하여 변경될 수 있다.

[0114] 사전 결정된 평가 기준은 위험 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다.

[0115] 식별된 적어도 하나의 위험 각각에 대응되는 위험도는 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 결정될 수 있다. 식별된 적어도 하나의 위험 각각에 대응되는 등급은 위험도에 기초하여 결정될 수 있다. 따라서, 제 2 노드(200)는 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 결정된 위험의 등급에 기초하여 점수를 결정할 수 있다.

[0116] 위험 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보의 점수에 대한 예시는 아래의 [표 6]에 대응될 수 있다.

표 6

[0118]	평가 결과	점수
	로우(low) 등급의 위험에 대한 완화대책 마련	2.5점
	미들(middle) 등급의 위험에 대한 완화대책 마련	5점
	하이(high) 등급의 위험에 대한 완화대책 마련	10점

[0119] [표 6]을 참조하면, 위험의 등급에 따라 점수가 결정될 수 있다. 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 위험 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보를 평가하여 점수를 산출할 수 있다. 제 2 노드(200)는 산출된 점수를 포함하는 평가 정보를 생성할 수 있다.

[0120] [표 6]의 구체적인 점수 수치는 복수의 제 2 노드들의 투표 결과에 기초하여 변경될 수 있다.

[0122] 검증 정보는 블록체인 네트워크(400)를 구성하는 제 3 노드(300)에서 사전 결정된 평가 기준에 기초하여 블록체인 네트워크를 통해 획득된 평가 정보의 생성의 유효성에 대한 검증을 통해 생성될 수 있다. 검증 정보는 제 3 노드(300)에서 블록체인 네트워크(400)에 전송될 수 있다.

[0123] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400)에서, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트(smart contract)에 의해 평가 정보에 대응되는 보상을 제 1 노드에 지급하도록 결정될 수 있다.

[0124] 본 개시내용의 일 실시예에 따른 스마트 컨트랙트는 임의의 형태의 계약 또는 협상을 디지털적으로 증명하고 실행시키기 위한 컴퓨터 프로토콜이다. 스마트 컨트랙트는 디지털 언어로 작성되고 임의의 컴퓨팅 장치에서 실행될 수 있다. 스마트 컨트랙트에 포함된 코드 및/또는 함수가 실행되는 경우, 그 코드 및/또는 함수에 기재된 형태의 동작들이 수행될 수 있다.

[0125] 본 개시내용의 실시예들에 따른 스마트 컨트랙트는, 새로운 스마트 컨트랙트를 생성하는 방식, 특정 스마트 컨트랙트상의 함수를 실행하는 방식, 및/또는 블록체인 네트워크에서 동작가능한 코인/토큰을 전송하는 방식 중 적어도 하나에 의해 실행될 수 있다. 또한, 스마트 컨트랙트는 외부 소유 어카운트에 의해서 발생한 트랜잭션이나 다른 컨트랙트에 의해서 실행될 수 있다.

[0126] 본 개시내용의 실시예들에 따른 보상을 지급하기 위한 스마트 컨트랙트는 예를 들어, 무한 반복같은 악의적인

코드를 막고 보상의 지급과 관련된 데이터의 무결성을 지키기 위해, 트랜잭션을 실행할 때 특정한 실행 비용을 지급하도록 규정할 수도 있다. 여기에서의 실행 비용이란 블록체인 네트워크(400)서 거래가능한 임의의 형태의 코인 또는 코인과 연동될 수 있는 별도의 다른 형태의 매개체(예컨대, 가스(gas) 등)을 의미할 수 있다. 비-제한적인 예시로서, 트랜잭션의 기본 실행 비용은 21,000 가스로 설정될 수 있다. 예를 들어, 이와 같은 실행 비용에는 트랜잭션 발행자의 어카운트 주소에 대한 ECDSA(Elliptic Curve Digital Signature Algorithm)를 처리하기 위한 비용, 트랜잭션 저장을 위한 스토리지 비용, 네트워크 대역폭 비용이 포함될 수 있다. 이와 같이 스마트 컨트랙트 실행 시 특정 비용을 지불하도록 정의되는 경우, 의도적인 디도스 공격과 같은 무한 실행과 같은 악의적인 공격이 방지될 수 있다.

[0127] 스마트 컨트랙트를 생성하거나 또는 실행시키고자 하는 엔티티가 특정한 재화(코인, 토큰 등)를 블록체인 네트워크(400)에 스테이킹(staking)시킨 후, 추가 수수료의 지급 없이 스마트 컨트랙트를 실행시키는 방식의 실행 비용 정책이 사용될 수도 있다. 이러한 경우, 스테이킹이 종료되는 경우, 해당 스마트 컨트랙트의 실행이 허용되지 않게 된다.

[0128] 본 개시내용의 실시예들에 따른 보상을 지급하기 위한 스마트 컨트랙트들 간의 호출은 메시지라는 구조체를 사용하여 구현될 수 있다. 예를 들어, 이러한 메시지는 컨트랙트 어카운트에 의해 생성될 수 있으며, 함수 호출시에 다른 컨트랙트로 전달될 수 있다. 이러한 경우의 메시지는 외부 소유 어카운트에서 발생하는 트랜잭션과는 달리, 블록체인 네트워크(400)의 내부에서 생성되어 처리되기 때문에, 가스와 같은 별도의 실행 비용이 발생되지 않을 수도 있다.

[0129] 본 개시내용의 실시예들에 따른 보상의 지급을 구현하는데 있어서, 스마트 컨트랙트의 함수를 컴파일된 코드 형태로 트랜잭션에 포함하여 블록체인을 통해 동기화할 때, 트랜잭션에 포함된 정보를 함수의 입력으로 하여 코드로 표현된 함수를 실행한 후 그 결과를 별도의 상태로 보관하는 방식으로 스마트 컨트랙트가 구현될 수 있다.

[0130] 본 개시내용의 일 실시예에 따른 스마트 컨트랙트는 등록 컨트랙트(register contract, RC), 프로필 컨트랙트(profile contract, PC) 및/또는 작업 컨트랙트(task contract, TC) 중 적어도 하나를 포함할 수 있다.

[0131] 등록 컨트랙트는 최초에 사용자를 등록을 위한 컨트랙트일 수 있다. 예를 들어, 등록 컨트랙트는 사용자(사용자 노드)가 자신의 계정을 새롭게 블록체인 네트워크(400)에 등록하는 경우에 사용되는 컨트랙트일 수 있다. 등록 컨트랙트는 사용자(사용자 노드)에게 할당된 임의의 ID(identification number), 블록체인 해시 주소 및/또는 프로필 컨트랙트의 주소 중 적어도 하나를 포함할 수 있다.

[0132] 프로필 컨트랙트는 사용자(사용자 노드)의 정보, 수행 중인 위협 모델링의 목록을 보여주기 위한 컨트랙트일 수 있다. 프로필 컨트랙트는 블록체인 주소, 사용자의 프로필, 사용자가 중재자(arbiter)인지 여부를 알려주는 중재자 상태 정보 및/또는 작업 컨트랙트들의 블록체인 주소 중 적어도 하나를 포함할 수 있다.

[0133] 작업 컨트랙트는 작업과 관련된 정보를 포함하는 컨트랙트일 수 있다. 작업 컨트랙트는 사용자의 평판과 사용자가 수행 중인 위협 모델링에 대한 내용을 포함할 수 있다. 예를 들어, 작업 컨트랙트는 블록체인 주소, 현재 작업의 상태, 예치금과 현재 작업에 대한 평가, 블록체인 네트워크(400)의 저장소에 저장된 자료에 대한 접근을 위한 작업 ID 및 작업 포인터, 및/또는 자격이 있는 사용자만 개인키로 서명된 내용에 접근할 수 있도록 새로 발급된 공개키를 반환해주는 컨트랙트 중 적어도 하나를 포함할 수 있다.

[0134] 사용자 노드는 블록체인 네트워크(400)에 포함 또는 포함되지 않는 노드일 수 있다. 사용자 노드는 프로세서, 메모리, 네트워크부를 포함할 수 있다.

[0135] 사용자 노드의 프로세서는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치 (GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석을 위한 프로세서를 포함할 수 있다. 사용자 노드의 프로세서는 통상적으로 사용자 노드의 전반적인 동작을 제어할 수 있다. 예를 들어, 사용자 노드의 프로세서는 사용자 노드에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 사용자 노드의 프로세서는 사용자 노드의 메모리에 저장된 컴퓨터 프로그램을 관독하여 본 개시의 일 실시예에 따른 데이터 처리를 수행할 수 있다.

[0136] 본 개시의 몇몇 실시예에 따르면, 사용자 노드의 메모리는 사용자 노드의 프로세서가 생성하거나 결정된 임의의 형태의 정보 및 사용자 노드의 네트워크부가 수신한 임의의 형태의 정보를 저장할 수 있다.

[0137] 본 개시의 몇몇 실시예에 따르면, 사용자 노드의 메모리는 플래시 메모리 타입(flash memory type), 하드디스크

타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 사용자 노드는 인터넷(internet) 상에서 사용자 노드의 메모리의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 사용자 노드의 네트워크부는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다.

[0139] 제 2 노드(200)는 제 1 노드(100)에서 생성된 위협 모델링의 결과물을 평가하는 평가자 노드(evaluator node)일 수 있다. 제 2 노드(200)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다. 제 2 노드(200)는 블록체인 네트워크(400)를 구성하는 노드일 수 있다. 제 2 노드(200)는 적어도 하나일 수 있고, 복수로 구성될 수도 있다.

[0140] 제 2 노드(200)는 프로세서(210), 메모리(230), 네트워크부(250)를 포함할 수 있다. 제 2 노드(200)의 각 구성들은 제 1 노드(100)의 구성과 대응될 수 있다. 따라서, 제 2 노드(200)의 각 구성들에 대한 구체적인 설명은 대응되는 제 1 노드(100)의 각 구성들에 대한 구체적인 설명으로 대체될 수 있다. 제 2 노드(200)를 설명하는 과정에서 전술한 내용과 중복되는 내용은 생략될 수 있다.

[0141] 프로세서(210)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치(GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석을 위한 프로세서를 포함할 수 있다. 프로세서(210)는 통상적으로 제 2 노드(200)의 전반적인 동작을 제어할 수 있다. 예를 들어, 프로세서(210)는 제 2 노드(200)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 프로세서(210)는 메모리(230)에 저장된 컴퓨터 프로그램을 판독하여 본 개시의 일 실시예에 따른 데이터 처리를 수행할 수 있다.

[0142] 본 개시의 몇몇 실시예에 따르면, 메모리(230)는 프로세서(210)가 생성하거나 결정한 임의의 형태의 정보 및 네트워크부(250)가 수신한 임의의 형태의 정보를 저장할 수 있다.

[0143] 본 개시의 몇몇 실시예에 따르면, 메모리(230)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 제 2 노드(200)는 인터넷(internet) 상에서 상기 메모리(230)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 전술한 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 네트워크부(250)는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다.

[0144] 제 2 노드(200)는 데이터에 기초하여 수행된 위협 모델링의 결과물을 블록체인 네트워크(400)를 통해 획득할 수 있다.

[0145] 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 결과물에 대한 평가를 통해 평가 정보를 생성할 수 있다.

[0146] 제 2 노드(200)는 평가 정보에 대한 검증 정보가 생성될 수 있도록, 평가 정보를 블록체인 네트워크(400)에 전송할 수 있다.

[0147] 위협 모델링의 결과물은 블록체인 네트워크(400)를 구성하는 제 1 노드(100)에서, 블록체인 네트워크(400)를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 데이터에 기초한 수행을 통해 생성될 수 있다. 위협 모델링의 결과물은 제 1 노드(100)에서 블록체인 네트워크(400)에 전송될 수 있다.

[0148] 검증 정보는 블록체인 네트워크(400)를 구성하는 제 3 노드(300)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 평가 정보의 생성의 유효성에 대한 검증을 통해 생성될 수 있다. 검증 정보

는 제 3 노드(300)에서 블록체인 네트워크(400)에 전송될 수 있다.

- [0149] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400)에서, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 제 1 노드에 지급하도록 결정될 수 있다.
- [0150] 제 2 노드(200)는 검토 정보를 블록체인 네트워크(400)를 통해 획득할 수 있다. 제 2 노드(200)는 검토 정보와 평가 정보를 비교하여 블록체인 네트워크(400)에 이의를 제기하기 위한 재심사 요청을 전송할 수 있다.
- [0152] 제 3 노드(300)는 복수의 제 2 노드들 중에서 투표를 통해 선출된 중재자 노드(arbiter node)일 수 있다. 제 3 노드(300)는 제 2 노드(200)에서 생성된 평가 정보에 대한 검증을 수행할 수 있다. 제 3 노드(300)는 위협 모델링 과정에서 발생할 수 있는 악의적인 행동을 방지하는 것을 목적으로 하는 개인 또는 회사일 수 있다.
- [0153] 제 3 노드(300)는 복수의 제 2 노드들 중에서 결정된 후보자 노드들 중에서 결정될 수 있다. 후보자 노드들은 보유한 토큰의 수에 기초하여 결정될 수 있다. 예를 들어, 후보자 노드들은 블록체인 네트워크(400) 상의 토큰 유통물량 중 3% 이상의 토큰을 보유하고 있는 참가자일 수 있다. 제 3 노드(300)는 후보자들 중 상위 10명의 득표자일 수 있다. 제 3 노드(300)는 제 2 노드(200)가 제출한 위협 모델링 평가 내용을 확인하여 정당한 작업 내용에 대해 보상을 적게 주기 위해 의도적으로 낮게 평가하는 부당한 행위가 있었는지 검토할 수 있다. 제 3 노드(300)는 제 1 노드(100)와 담합하여 올바르게 않은 작업 내용에 대해 보상을 높게 주는 등의 부당한 행위가 있었는지 검토할 수 있다.
- [0154] 제 3 노드(300)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다. 제 3 노드(300)는 블록체인 네트워크(400)를 구성하는 노드일 수 있다. 제 3 노드(300)는 적어도 하나일 수 있고, 복수로 구성될 수도 있다.
- [0155] 제 3 노드(300)는 프로세서(310), 메모리(330), 네트워크부(350)를 포함할 수 있다. 제 3 노드(300)의 각 구성들은 제 1 노드(100) 또는 제 2 노드(200)의 구성과 대응될 수 있다. 따라서, 제 3 노드(300)의 각 구성들에 대한 구체적인 설명은 대응되는 제 1 노드(100) 또는 제 2 노드(200)의 각 구성들에 대한 구체적인 설명으로 대체될 수 있다. 제 3 노드(300)를 설명하는 과정에서 기술한 내용과 중복되는 내용은 생략될 수 있다.
- [0156] 프로세서(310)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치 (GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등의 데이터 분석을 위한 프로세서를 포함할 수 있다. 프로세서(310)는 통상적으로 제 3 노드(300)의 전반적인 동작을 제어할 수 있다. 예를 들어, 프로세서(310)는 제 3 노드(300)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터 정보 등을 처리할 수 있다. 다른 예를 들어, 프로세서(310)는 메모리(330)에 저장된 컴퓨터 프로그램을 판독하여 본 개시의 일 실시예에 따른 데이터 처리를 수행할 수 있다.
- [0157] 본 개시의 몇몇 실시예에 따르면, 메모리(330)는 프로세서(310)가 생성하거나 결정한 임의의 형태의 정보 및 네트워크부(350)가 수신한 임의의 형태의 정보를 저장할 수 있다.
- [0158] 본 개시의 몇몇 실시예에 따르면, 메모리(330)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 제 3 노드(300)는 인터넷(internet) 상에서 상기 메모리(330)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다. 기술한 메모리에 대한 기재는 예시일 뿐, 본 개시는 이에 제한되지 않는다. 본 개시의 몇몇 실시예에 따른 네트워크부(350)는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다.
- [0159] 제 3 노드(300)는 사전 결정된 평가 기준에 기초하여, 위협 모델링의 결과물에 대한 평가를 통해 생성된 평가 정보를 블록체인 네트워크(400)를 통해 획득할 수 있다.
- [0160] 제 3 노드(300)는 사전 결정된 평가 기준에 기초하여 평가 정보의 생성의 유효성에 대한 검증을 통해 검증 정보

를 생성할 수 있다.

- [0161] 제 3 노드(300)는 검증 정보를 블록체인 네트워크(400)에 전송할 수 있다.
- [0162] 위협 모델링의 결과물은 블록체인 네트워크(400)를 구성하는 제 1 노드(100)에서, 블록체인 네트워크(400)를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 데이터에 기초한 수행을 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0163] 평가 정보는 블록체인 네트워크(400)를 구성하는 제 2 노드(200)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 결과물에 대한 평가를 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0164] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400)에서, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 상기 제 1 노드에 지급하도록 결정될 수 있다.
- [0165] 제 3 노드(300)는 공격 라이브러리의 수집에 관한 평가 정보의 경우, 공격 라이브러리의 수집에 대해 합의된 점수 시스템(예를 들어, [표 2] 등)에 기초하여 점수 및/또는 보상 지급 내역 중 적어도 하나를 검증할 수 있다.
- [0166] 제 3 노드(300)는 위협의 식별에 관한 평가 정보의 경우, 위협의 식별에 대해 합의된 점수 시스템(예를 들어, [표 3] 등)에 기초하여 점수 및/또는 보상 지급 내역 중 적어도 하나를 검증할 수 있다.
- [0167] 제 3 노드(300)는 공격 시나리오의 작성에 관한 평가 정보의 경우, 공격 시나리오의 작성에 대해 합의된 점수 시스템(예를 들어, [표 4] 등)에 기초하여 점수 및/또는 보상 지급 내역 중 적어도 하나를 검증할 수 있다.
- [0168] 제 3 노드(300)는 위험도의 평가에 관한 평가 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 검증할 수 있다.
- [0169] 제 3 노드(300)는 완화대책 마련에 관한 평가 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 검증할 수 있다.
- [0171] 블록체인 네트워크(400)는 블록체인 기술에 기반하여 동작하는 복수의 노드들(예를 들어, 제 1 노드(100), 제 2 노드(200), 제 3 노드(300) 등)을 포함할 수 있다. 블록체인 기술은 블록들 또는 이벤트들이 서로 연결된 저장 구조 또는 트랜잭션들이 서로 연결된 저장 구조를 사용하여, 관리 대상인 데이터를 복수의 노드들에 분산 저장하는 임의의 형태의 분산 원장(distributed ledger) 기술일 수 있다. 본 개시내용의 일 실시예에 따른 블록체인 네트워크는 DAG(Directed Acyclic Graph) 기술을 기반한 임의의 형태의 분산 원장 기술들에 따라서 동작할 수도 있다.
- [0172] 본 개시내용의 일 실시예에서, 블록체인 네트워크에서의 노드들은 아키텍처 계층(architecture layer) 구조에 따른 블록체인 코어 패키지에 의해 동작할 수 있다. 아키텍처 계층 구조는 애플리케이션 계층, 블록체인 계층 및/또는 저장 계층 중 적어도 하나를 포함할 수 있다.
- [0173] 애플리케이션 계층은 클라이언트(client), 모듈, 프로그램 컴파일러 등을 포함할 수 있다.
- [0174] 클라이언트는 사용자(예를 들어, 제 1 노드(100)의 사용자, 제 2 노드(200)의 사용자, 제 3 노드(300)의 사용자, 고객 노드의 사용자 등)가 위협 모델링을 수행할 수 있게 해주는 인터페이스(interface)(예를 들어, 사용자 인터페이스 등)일 수 있다. 클라이언트는 중앙 서버에 의존하지 않고 실행될 수 있다.
- [0175] 모듈은 사용자 관리 모듈(user management module), 작업 관리 모듈(work management module) 및/또는 투표 모듈(voting module) 중 적어도 하나를 포함할 수 있다.
- [0176] 사용자 관리 모듈은 사용자를 관리하기 위한 모듈일 수 있다. 사용자 관리 모듈은 블록체인 상에 사용자들의 등록을 수행하고, 사용자의 프로필을 조회할 수 있다.
- [0177] 작업 관리 모듈은 작업을 관리하기 위한 모듈일 수 있다. 작업 관리 모듈은 위협 모델링에 관한 사용자들의 작업의 관리, 수행, 제출 및/또는 평가 중 적어도 하나를 할 수 있다.
- [0178] 투표 모듈은 투표를 진행하기 위한 모듈일 수 있다. 투표 모듈은 블록체인 네트워크(400) 내에서 블록체인 네트워크(400)를 구성하는 노드들 간에 투표를 수행할 수 있다. 투표 모듈은 수행된 투표에 대한 결과를 생성할 수도 있다.

- [0179] 블록체인 계층은 중간 계층으로서 블록체인 네트워크(400)에서 합의를 제공하고 상태 머신(state machine)을 실행할 수 있다. 애플리케이션 계층의 프로그램은 컴파일 된 후 블록체인 계층으로 전송될 수 있다. 블록체인 계층에 포함된 적어도 하나의 마이너(miner)는 애플리케이션 계층으로부터 수신한 프로그램을 확인할 수 있다. 마이너들을 통해 확인된 프로그램은 블록체인에 작성될 수 있다. 마이너는 개인의 최대 이익 추구를 위해 블록체인 네트워크에 참여하는 개인 또는 회사의 노드일 수 있다. 마이너는 이익 추구 과정에서 블록체인 네트워크(400)를 안정화시키고 시빌 공격(sybil attack)을 방지할 수 있다.
- [0180] 저장 계층은 작업의 실제 데이터 값을 저장할 수 있다. 저장 계층에 사용되는 저장 공간은 특정되지 않을 수 있다. 실제 데이터 값들은 소유자의 개인키로 서명되어 저장될 수 있다.
- [0181] 본 개시내용에서의 일 실시예에 따른 블록체인 네트워크(400)는 구현 형태에 따라서, 임의의 노드들이 합의 동작을 수행할 수 있는 Public 블록체인 네트워크, 또는 사전결정된 노드만이 합의 동작을 수행할 수 있는 Private 또는 Consortium 블록체인 네트워크를 포함할 수 있다. 다만, 블록체인 네트워크(400)는 이에 한정되지 않는다.
- [0182] 본 개시내용에서의 블록체인 네트워크에서 수행되는 합의 알고리즘은 PoW(Proof of Work) 알고리즘, PoS(Proof of Stake) 알고리즘, DPoS(Delegated Proof of Stake) 알고리즘, PBFT(Practical Byzantine Fault Tolerance) 알고리즘, DBFT(Delegated Byzantine Fault Tolerance) 알고리즘, RBFT(Redundant Byzantine Fault Tolerance) 알고리즘, Sieve 알고리즘, Tendermint 알고리즘, Paxos 알고리즘, Raft 알고리즘, PoA(Proof of Authority) 알고리즘, PoET(Proof of Elapsed Time) 알고리즘, Tangle 네트워크 합의 알고리즘 및/또는 Hedera Hashgraph 합의 알고리즘 중 적어도 하나를 포함할 수 있다.
- [0184] 통신 네트워크(500)는 임의의 형태의 데이터, 신호 및/또는 정보 중 적어도 하나를 송수신할 수 있는 임의의 유무선 통신 네트워크를 포함할 수 있다. 예를 들어, 네트워크(300)는 제 1 노드(100), 제 2 노드(200), 제 3 노드(300) 및 블록체인 네트워크(400) 간에 작업 요청, 위협 모델링의 결과물, 평가 정보, 검증 정보 등을 송수신할 수 있는 유무선 통신 네트워크를 포함할 수 있다.
- [0186] 도 2는 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링을 수행하기 위한 아키텍처 계층(architecture layer) 구조를 나타내는 도면이다.
- [0187] 도 2를 참조하면, 아키텍처 계층 구조는 애플리케이션 계층(10), 블록체인 계층(20) 및/또는 저장 계층(30) 중 적어도 하나를 포함할 수 있다.
- [0188] 애플리케이션 계층(10)은 클라이언트(client), 모듈, 프로그램 컴파일러(program compiler) 등을 포함할 수 있다.
- [0189] 블록체인 계층(20)은 중간 계층으로서 네트워크(예를 들어, 블록체인 네트워크(400))에서 합의 알고리즘(합의 프로토콜(consensus protocol))을 통해 합의를 제공하고, 트랜잭션(transaction)을 통해 상태 머신(state machine)을 실행할 수 있다. 애플리케이션 계층(10)의 프로그램은 컴파일 된 후 블록체인 계층(20)으로 전송될 수 있다. 블록체인 계층(20)에 포함된 적어도 하나의 마이너(miner)는 애플리케이션 계층(10)으로부터 수신한 프로그램을 확인할 수 있다. 마이너들을 통해 확인된 프로그램은 블록체인에 작성될 수 있다. 마이너는 개인의 최대 이익 추구를 위해 블록체인 네트워크에 참여하는 개인 또는 회사의 노드일 수 있다. 마이너는 이익 추구 과정에서 블록체인 네트워크(400)를 안정화시키고 시빌 공격(sybil attack)을 방지할 수 있다.
- [0190] 저장 계층(30)은 작업의 실제 데이터 값을 저장할 수 있다. 저장 계층(30)에 사용되는 저장 공간(storage)은 특정되지 않을 수 있다. 실제 데이터 값들은 소유자의 개인키로 서명되어 저장될 수 있다. 도 2를 통해서 설명되지 않은 아키텍처 계층 구조의 상세한 설명은 도 1을 통해서 기술한 아키텍처 계층 구조의 내용으로 대체될 수 있다.
- [0192] 도 3은 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 1 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.
- [0193] 도 3을 참조하면, 제 1 노드(100)는 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 블록체인

네트워크(400)를 통해 획득할 수 있다(S110).

- [0194] 데이터는 데이터 흐름도를 포함하는 시스템 모델의 데이터 또는 아키텍처의 데이터 중 적어도 하나를 포함할 수 있다.
- [0195] 제 1 노드(100)는 작업 요청에 응답하여, 데이터에 기초하여 수행된 위협 모델링의 결과물을 생성할 수 있다(S120).
- [0196] 위협 모델링의 결과물은 시스템 모델의 작성에 관한 작업 정보, 공격 라이브러리의 수집에 관한 작업 정보, 위협의 식별에 관한 작업 정보, 공격 시나리오의 작성에 관한 작업 정보, 위험도의 평가에 관한 작업 정보 및 완화대책 마련에 관한 작업 정보 중 적어도 하나를 포함할 수 있다.
- [0197] 평가 정보는 위협 모델링의 결과물에 포함된 작업 정보별로 각각 평가되어 산출된 점수(point)를 포함할 수 있다.
- [0198] 제 1 노드(100)는 결과물에 대한 평가 정보 및 평가 정보에 대한 검증 정보가 생성될 수 있도록, 위협 모델링의 결과물을 블록체인 네트워크(400)에 전송할 수 있다(S130).
- [0199] 평가 정보는 블록체인 네트워크(400)를 구성하는 제 2 노드(200)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 결과물에 대한 평가를 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0200] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 시스템 모델의 작성에 관한 작업 정보의 경우, 시스템 모델의 수준, 시스템 모델의 객체 작성 여부 및 시스템 모델의 데이터 흐름 작성 여부를 기준으로 할 수 있다.
- [0201] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 공격 라이브러리의 수집에 관한 작업 정보의 경우, 공격 라이브러리의 공통 취약점 등급 시스템(common vulnerability scoring system) 점수 및 공격 라이브러리의 사용처를 기준으로 할 수 있다.
- [0202] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 위협의 식별에 관한 작업 정보의 경우, 타겟에 대한 위협 정도를 기준으로 할 수 있다.
- [0203] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 공격 시나리오의 작성에 관한 작업 정보의 경우, 공격 트리 각 항목의 개수 및 유효 공격 시나리오 작성 여부를 기준으로 할 수 있다.
- [0204] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 위험도의 평가에 관한 작업 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다.
- [0205] 사전 결정된 평가 기준은 위협 모델링의 결과물에 포함된 완화대책 마련에 관한 작업 정보의 경우, 블록체인 네트워크(400)에 포함된 복수의 노드들의 투표 결과를 기준으로 할 수 있다.
- [0206] 검증 정보는 블록체인 네트워크(400)를 구성하는 제 3 노드(300)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0207] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 제 1 노드에 지급하도록 결정될 수 있다.
- [0209] 도 4는 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 2 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.
- [0210] 제 2 노드(200)는 데이터에 기초하여 수행된 위협 모델링의 결과물을 상기 블록체인 네트워크를 통해 획득할 수 있다(S210).
- [0211] 위협 모델링의 결과물은 블록체인 네트워크(400)를 구성하는 제 1 노드(100)에서, 블록체인 네트워크(400)를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 데이터에 기초한 수행을 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0212] 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 결과물에 대한 평가를 통해 평가 정보를 생성할 수 있다(S220).

- [0213] 제 2 노드(200)는 평가 정보에 대한 검증 정보가 생성될 수 있도록, 평가 정보를 블록체인 네트워크(400)에 전송할 수 있다(S230).
- [0214] 검증 정보는 블록체인 네트워크(400)를 구성하는 제 3 노드(300)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 평가 정보의 생성의 유효성에 대한 검증을 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0215] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 제 1 노드(100)에 지급하도록 결정될 수 있다.
- [0217] 도 5는 본 개시의 몇몇 실시예에 따른 블록체인 네트워크를 구성하는 제 3 노드에 의해 수행되는 위협 모델링 방법을 나타낸 흐름도이다.
- [0218] 제 3 노드(300)는 사전 결정된 평가 기준에 기초하여, 위협 모델링의 결과물에 대한 평가를 통해 생성된 평가 정보를 블록체인 네트워크(400)를 통해 획득할 수 있다(S310).
- [0219] 위협 모델링의 결과물은 블록체인 네트워크(400)를 구성하는 제 1 노드(100)에서, 블록체인 네트워크(400)를 통해 획득된 데이터를 포함하는 작업 요청에 응답하여, 데이터에 기초한 수행을 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0220] 제 3 노드(300)는 사전 결정된 평가 기준에 기초하여 평가 정보의 생성의 유효성에 대한 검증을 통해 검증 정보를 생성할 수 있다(S320).
- [0221] 평가 정보는 블록체인 네트워크(400)를 구성하는 제 2 노드(200)에서, 사전 결정된 평가 기준에 기초하여 블록체인 네트워크(400)를 통해 획득된 결과물에 대한 평가를 통해 생성되고, 그리고 블록체인 네트워크(400)에 전송될 수 있다.
- [0222] 제 3 노드(300)는 검증 정보를 블록체인 네트워크(400)에 전송할 수 있다(S330).
- [0223] 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 제 1 노드(100)에 지급하도록 결정될 수 있다.
- [0225] 도 6은 본 개시의 몇몇 실시예에 따른 블록체인 기술을 이용한 위협 모델링 방법의 순서도이다.
- [0226] 도 6을 참조하면, 블록체인 네트워크(400)는 고객 노드로부터 위협 모델링의 수행에 요구되는 데이터를 포함하는 작업 요청을 수신할 수 있다. 따라서, 작업요청은 블록체인 네트워크(400) 상에 게시될 수도 있다.
- [0227] 제 1 노드(100)는 블록체인 네트워크(400)를 통해 작업 요청을 획득할 수 있다(S411).
- [0228] 제 1 노드(100)는 작업 요청에 응답하여, 위협 모델링의 결과물을 생성할 수 있다(S412).
- [0229] 제 1 노드(100)는 위협 모델링의 결과물을 블록체인 네트워크(400)에 전송할 수 있다(S413). 예를 들어, 제 1 노드(100)는 사전 결정된 마감 기한 내에 위협 모델링의 결과물을 블록체인 네트워크(400)에 전송할 수 있다. 따라서, 위협 모델링의 결과물은 블록체인 네트워크(400) 상에 게시될 수도 있다.
- [0230] 제 2 노드(200)는 위협 모델링의 결과물을 블록체인 네트워크(400)를 통해 획득할 수 있다(S421).
- [0231] 제 2 노드(200)는 사전 결정된 평가 기준에 기초하여 결과물에 대한 평가를 통해 평가 정보를 생성할 수 있다(S422).
- [0232] 제 2 노드(200)는 평가 정보를 블록체인 네트워크(423)에 전송할 수 있다. 따라서, 평가 정보는 블록체인 네트워크(400) 상에 게시될 수도 있다.
- [0233] 제 3 노드(300)는 평가 정보를 블록체인 네트워크(400)를 통해 획득할 수 있다(S431).
- [0234] 제 3 노드(300)는 사전 결정된 평가 기준에 기초하여 평가 정보의 생성의 유효성에 대한 검증을 통해 검증 정보를 생성할 수 있다(S432).
- [0235] 제 3 노드(300)는 검증 정보를 블록체인 네트워크(400)에 전송할 수 있다(S433). 따라서, 검증 정보는 블록체인

네트워크(400) 상에 게시될 수도 있다.

- [0236] 블록체인 네트워크(400)는 검증 정보에 기초하여 평가 정보의 생성에 대한 유효성 검증을 확인할 수 있다(S441).
- [0237] 블록체인 네트워크(400)는 평가 정보의 생성에 대한 유효성이 검증된 경우, 블록체인 네트워크(400) 상에 저장된 스마트 컨트랙트에 의해 평가 정보에 대응되는 보상을 제 1 노드(100)에 지급할 수 있다(S442).
- [0238] 도 3 내지 도 6에 도시되는 단계들은 예시적인 단계들이다. 따라서, 본 개시 내용의 사상 범위를 벗어나지 않는 한도에서 도 2 내지 도 6의 단계들 중 일부가 생략되거나 추가적인 단계들이 존재할 수 있다는 점 또한 당업자에게 명백할 것이다. 또한, 도 2 내지 도 6에 기재된 구성들(예를 들어, 제 1 노드(100), 제 2 노드(200), 제 3 노드(300), 블록체인 네트워크(400) 등)에 관한 구체적인 내용은 앞서 도 1 및 도 2를 통해 설명한 내용으로 대체될 수 있다.
- [0239] 도 1 내지 도 6을 참조하여 상술한 바와 같이, 본 개시의 몇몇 실시예에 따른 블록체인 네트워크(400)를 구성하는 노드들(예를 들어, 제 1 노드(100), 제 2 노드(200), 제 3 노드(300))은 블록체인과 스마트 컨트랙트를 활용한 공평한 보상 시스템을 통해 참여 노드들의 참여도에 따라 보상을 지급하기 때문에 각 분야의 전문가들의 위협 모델링의 참여도를 높일 수 있다. 또한, 본 개시의 몇몇 실시예에 따른 블록체인 네트워크(400)를 구성하는 노드들(예를 들어, 제 1 노드(100), 제 2 노드(200), 제 3 노드(300))은 보상을 통해 복수의 노드들의 참여를 유도하여 최선의 결과를 도출할 수 있다.
- [0241] 도 7은 본 개시의 내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도이다.
- [0242] 본 개시가 일반적으로 컴퓨팅 장치에 의해 구현될 수 있는 것으로 전술되었지만, 당업자라면 본 개시가 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어 및/또는 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로써 구현될 수 있다는 것을 잘 알 것이다.
- [0243] 일반적으로, 프로그램 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드(handheld) 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.
- [0244] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘 다에 위치할 수 있다.
- [0245] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체는 그 어떤 것이든지 컴퓨터 판독가능 매체가 될 수 있고, 이러한 컴퓨터 판독가능 매체는 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다. 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.
- [0246] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터 등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

- [0247] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.
- [0248] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.
- [0249] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 새시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.
- [0250] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 zip 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.
- [0251] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.
- [0252] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.
- [0253] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.
- [0254] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 컴퓨팅 디바이스 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원격 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크,

예를 들어, 인터넷에 연결될 수 있다.

[0255] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 컴퓨팅 디바이스에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워킹화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0256] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순히 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0257] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a, b, g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0258] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 위의 설명에서 참조될 수 있는 데이터, 지시들, 명령들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학장들 또는 입자들, 또는 이들의 임의의 결합에 의해 표현될 수 있다.

[0259] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 소프트웨어로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[0260] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조물품(article)으로 구현될 수 있다. 용어 제조물품은 임의의 컴퓨터-판독가능 저장장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트림, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 또한, 여기서 제시되는 다양한 저장 매체는 정보를 저장하기 위한 하나 이상의 장치 및/또는 다른 기계-판독가능한 매체를 포함한다.

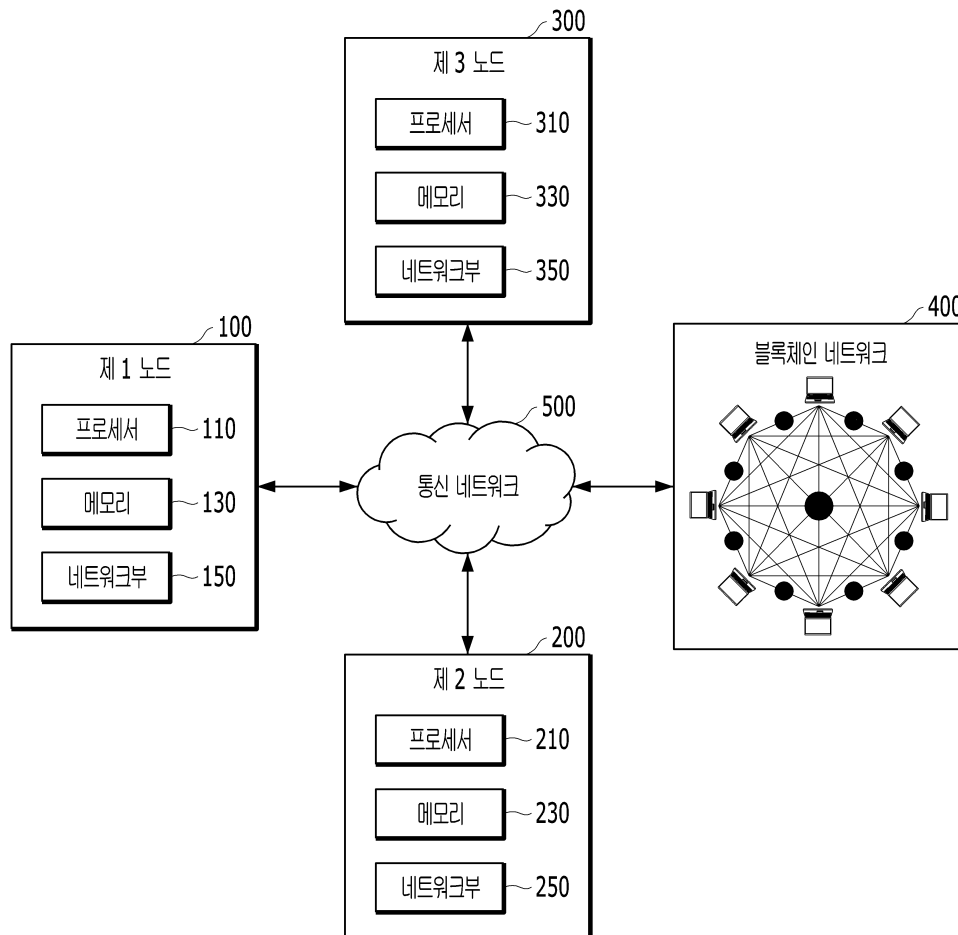
[0261] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 설계 우선순위들에 기반하여, 본 개시의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.

[0262] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거

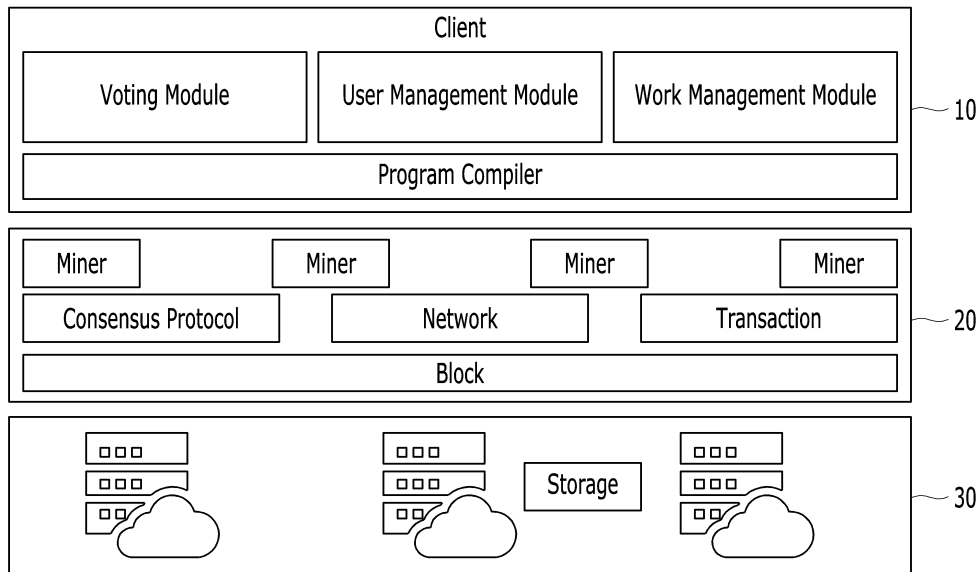
나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

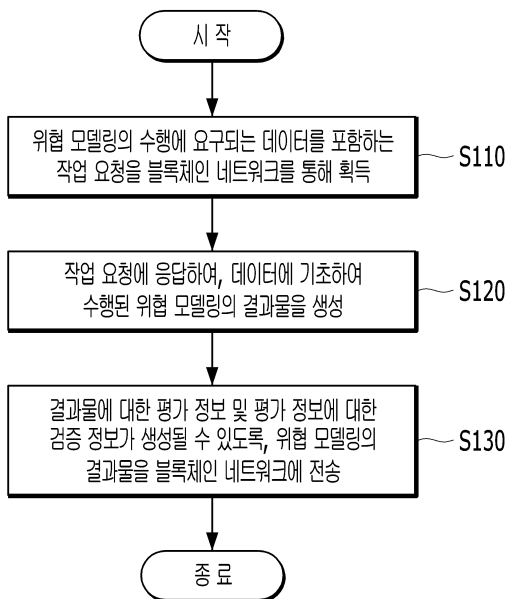
도면1



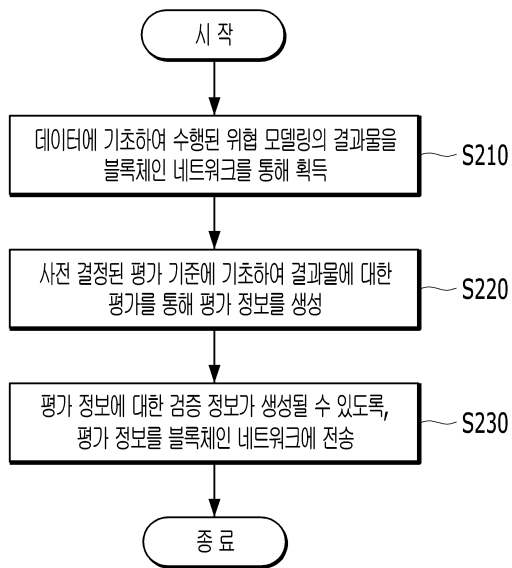
도면2



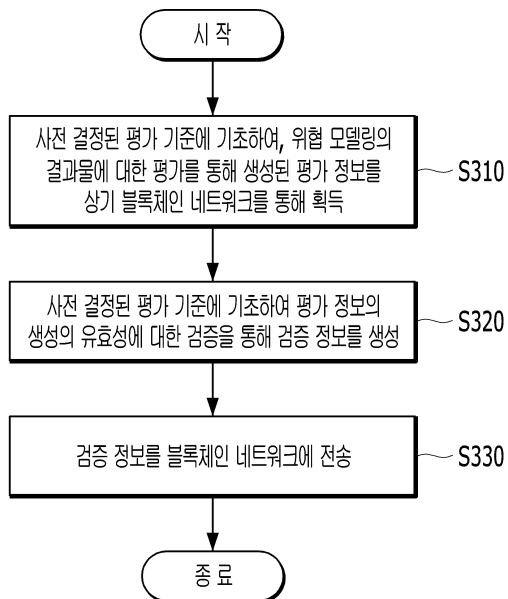
도면3

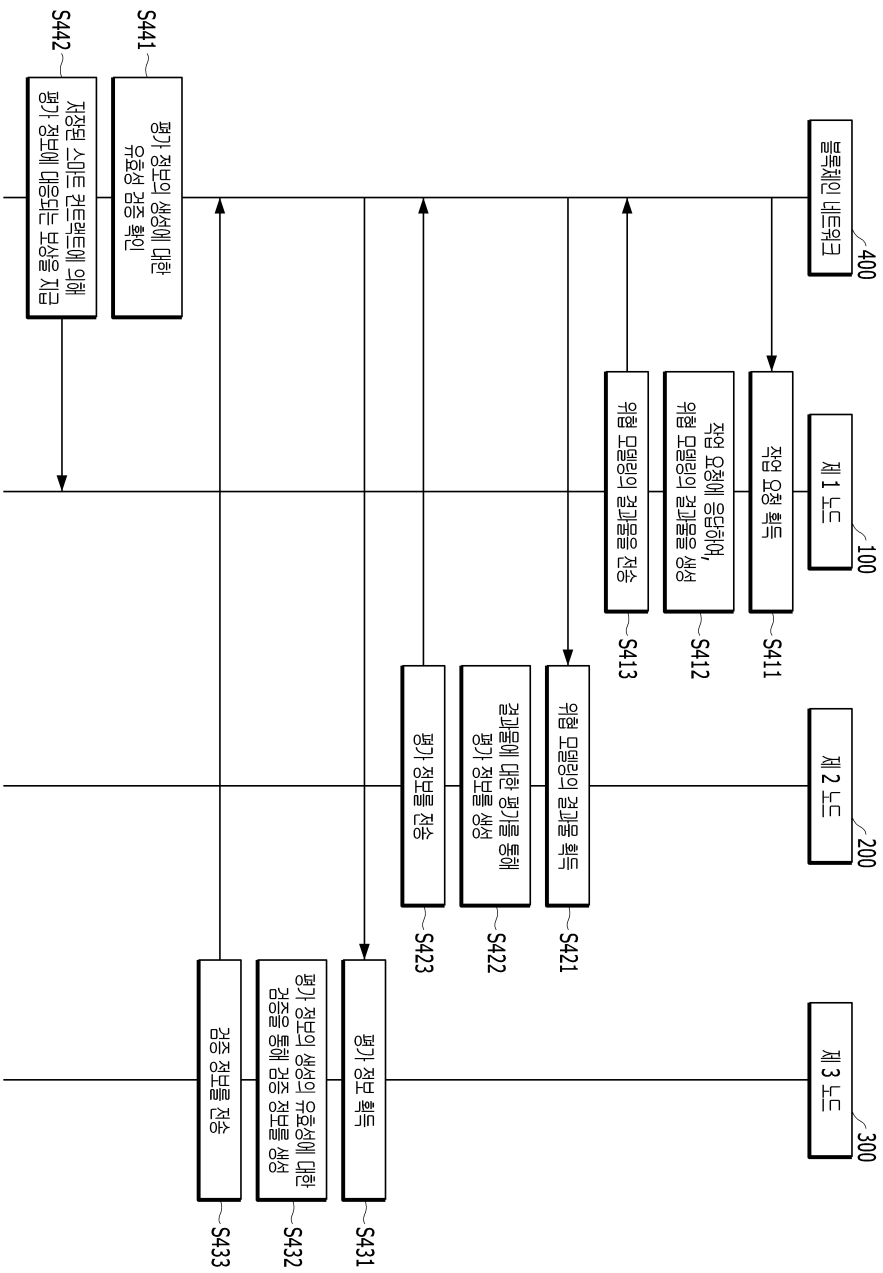


도면4



도면5





도면6

도면7

