



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0100191  
(43) 공개일자 2024년07월01일

(51) 국제특허분류(Int. Cl.)  
H04L 9/40 (2022.01) H04L 67/12 (2022.01)  
H04L 9/00 (2022.01) H04L 9/32 (2006.01)  
(52) CPC특허분류  
H04L 63/1433 (2013.01)  
H04L 63/0428 (2013.01)  
(21) 출원번호 10-2023-0039804  
(22) 출원일자 2023년03월27일  
심사청구일자 2023년03월27일  
(30) 우선권주장  
1020220182311 2022년12월22일 대한민국(KR)

(71) 출원인  
인천대학교 산학협력단  
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)  
(72) 발명자  
전광길  
인천광역시 연수구 해송로 70 송도웰카운티2단지 209동 805호  
(74) 대리인  
특허법인시공

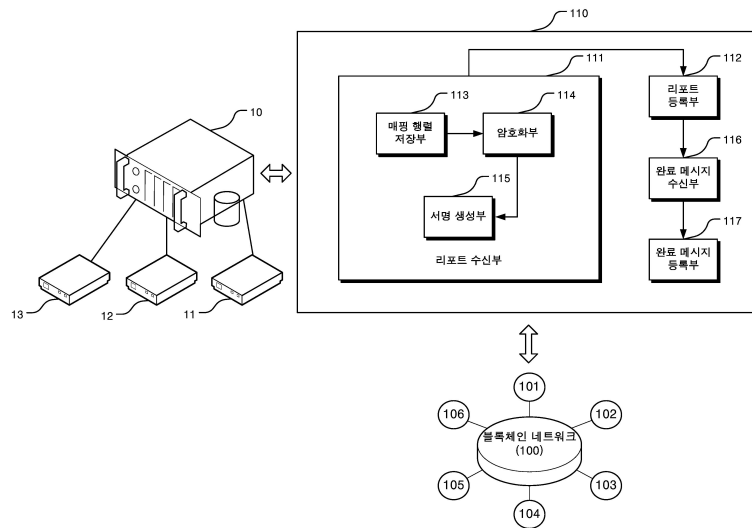
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **블록체인 기반의 IoT 네트워크 보안 관리 시스템 및 그 동작 방법**

(57) 요약

본 발명은 로컬 네트워크를 구성하는 IoT 디바이스들에 대한 보안 취약점 분석 리포트를, 블록체인 네트워크를 통해 IoT 디바이스 제조사들의 관리 단말로 배포할 수 있는 보안 관리 시스템 및 그 동작 방법에 대한 것이다.

대표도 - 도1



(52) CPC특허분류

*H04L 67/12* (2022.05)

*H04L 9/3247* (2013.01)

*H04L 9/50* (2022.05)

*H04L 2209/08* (2013.01)

---

## 명세서

### 청구범위

#### 청구항 1

로컬 네트워크에 접속된 복수의 IoT 디바이스들의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말이 노드로 참여하고 있는 블록체인 네트워크를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포할 수 있는 보안 관리 시스템에 있어서,

상기 네트워크 관리 장치로부터, 상기 복수의 IoT 디바이스들 중 어느 하나인 제1 IoT 디바이스에 대한 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성하는 리포트 수신부; 및

암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제1 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 리포트 등록부

를 포함하는 보안 관리 시스템.

#### 청구항 2

제1항에 있어서,

상기 리포트 등록부는

상기 제1 트랜잭션이 생성되면, 상기 블록체인 네트워크의 노드로서 존재하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중, 어느 하나인 제1 관리 단말을 랜덤하게 선택한 후, 상기 제1 관리 단말로 상기 제1 트랜잭션을 전송하면서, 상기 제1 트랜잭션의 상기 블록체인 네트워크로의 등록 요청을 전송하고,

상기 제1 관리 단말은

상기 보안 관리 시스템으로부터 상기 제1 트랜잭션과 함께 상기 등록 요청이 수신되면, 상기 개인키에 대응되는 사전 발급된 공개키를 기초로, 상기 제1 트랜잭션에 포함된 상기 제1 전자 서명에 대한 복호화 값을 생성한 후, 상기 복호화 값이 상기 제1 트랜잭션에 포함된 암호화된 상기 제1 취약점 분석 리포트와 일치하는지 확인함으로써, 상기 제1 전자 서명에 대한 검증을 수행한 후, 상기 제1 전자 서명에 대한 검증이 완료되면, 메모리 상에 저장되어 있는 블록체인 데이터에 체인으로 연결된 이전 블록을 기초로 상기 제1 트랜잭션이 포함된 제1 블록을 생성하고, 상기 제1 블록을 상기 블록체인 데이터에 체인으로 연결함으로써, 상기 제1 블록에 대한 저장을 완료한 후, 상기 블록체인 네트워크를 통해 상기 제1 블록을, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 상기 제1 관리 단말을 제외한 나머지 관리 단말로 전파하는 것을 특징으로 하는 보안 관리 시스템.

#### 청구항 3

제1항에 있어서,

상기 리포트 수신부는

상기 복수의 IoT 디바이스 제조사들의 관리 단말과 사전 공유하고 있는,  $n \times n$  ( $n$ 은 2이상의 자연수임) 크기의 사전 지정된 매핑 행렬 - 상기 매핑 행렬은, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들이 서로 다른 원-핫(one-hot) 벡터로 구성되어 있음 - 이 저장되어 있는 매핑 행렬 저장부;

상기 네트워크 관리 장치로부터 상기 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트를 구성하는 데이터를  $n$ 개로 분할하여  $n$ 개의 분할 데이터들을 생성한 후, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에 대해 상기  $n$ 개의 분할 데이터들을 하나씩 순차적으로 할당할 다음, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에서 1의 성분을, 각 열벡터에 할당된 분할 데이터로 치환함과 동시에, 상기 매핑 행렬을 구성하는  $n^2$  개의 성분들 중 0의 성분들을, 랜덤하게 생성한 더미(dummy) 데이터로 치환하여 치환 행렬을 생성함으로써,

상기 제1 취약점 분석 리포트에 대한 암호화를 수행하는 암호화부; 및

상기 개인키를 기초로 상기 치환 행렬을 암호화함으로써, 상기 제1 전자 서명을 생성하는 서명 생성부를 포함하고,

상기 리포트 등록부는

상기 치환 행렬과 상기 제1 전자 서명이 생성되면, 상기 치환 행렬과 상기 제1 전자 서명이 포함된 상기 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리하는 것을 특징으로 하는 보안 관리 시스템.

#### 청구항 4

제3항에 있어서,

상기 복수의 IoT 디바이스 제조사들의 관리 단말은

메모리 상에 상기 매핑 행렬을 사전 저장하고 있고, 상기 블록체인 네트워크를 통해 상기 제1 트랜잭션이 수신된 이후, 관리자에 의해 상기 제1 트랜잭션에 포함된 상기 치환 행렬로부터의 상기 제1 취약점 분석 리포트의 복원 명령이 인가되면, 상기 제1 트랜잭션에 포함된 상기 치환 행렬과, 메모리 상에 저장되어 있는 상기 매핑 행렬 간의 요소별 곱셈 연산(element wise product)을 수행하여 연산 행렬을 생성하고, 상기 연산 행렬을 구성하는  $n$ 개의 열벡터들 각각으로부터 0이 아닌 성분을 추출함으로써 상기  $n$ 개의 분할 데이터들을 추출한 후, 상기  $n$ 개의 분할 데이터들을 순차적으로 결합함으로써, 상기 제1 취약점 분석 리포트를 복원하는 것을 특징으로 하는 보안 관리 시스템.

#### 청구항 5

제1항에 있어서,

상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 상기 제1 트랜잭션의 배포가 완료된 이후, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 어느 하나인 제2 관리 단말로부터, 상기 제1 IoT 디바이스에 대한 취약점 보안이 완료되었음을 지시하는 완료 메시지가 수신되면, 상기 개인키를 기초로 상기 완료 메시지에 대한 제2 전자 서명을 생성하는 완료 메시지 수신부; 및

상기 완료 메시지와 상기 제2 전자 서명이 포함된 제2 트랜잭션을 생성한 후, 상기 제2 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제2 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 완료 메시지 등록부

를 더 포함하는 보안 관리 시스템.

#### 청구항 6

로컬 네트워크에 접속된 복수의 IoT 디바이스들의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말이 노드로 참여하고 있는 블록체인 네트워크를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포할 수 있는 보안 관리 시스템의 동작 방법에 있어서,

상기 네트워크 관리 장치로부터, 상기 복수의 IoT 디바이스들 중 어느 하나인 제1 IoT 디바이스에 대한 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성하는 단계; 및

암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제1 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 단계

를 포함하는 보안 관리 시스템의 동작 방법.

#### 청구항 7

제6항에 있어서,

상기 처리하는 단계는

상기 제1 트랜잭션이 생성되면, 상기 블록체인 네트워크의 노드로서 존재하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중, 어느 하나인 제1 관리 단말을 랜덤하게 선택한 후, 상기 제1 관리 단말로 상기 제1 트랜잭션을 전송하면서, 상기 제1 트랜잭션의 상기 블록체인 네트워크로의 등록 요청을 전송하고,

상기 제1 관리 단말은

상기 보안 관리 시스템으로부터 상기 제1 트랜잭션과 함께 상기 등록 요청이 수신되면, 상기 개인키에 대응되는 사전 발급된 공개키를 기초로, 상기 제1 트랜잭션에 포함된 상기 제1 전자 서명에 대한 복호화 값을 생성한 후, 상기 복호화 값이 상기 제1 트랜잭션에 포함된 암호화된 상기 제1 취약점 분석 리포트와 일치하는지 확인함으로써, 상기 제1 전자 서명에 대한 검증을 수행한 후, 상기 제1 전자 서명에 대한 검증이 완료되면, 메모리 상에 저장되어 있는 블록체인 데이터에 체인으로 연결된 이전 블록을 기초로 상기 제1 트랜잭션이 포함된 제1 블록을 생성하고, 상기 제1 블록을 상기 블록체인 데이터에 체인으로 연결함으로써, 상기 제1 블록에 대한 저장을 완료한 후, 상기 블록체인 네트워크를 통해 상기 제1 블록을, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 상기 제1 관리 단말을 제외한 나머지 관리 단말로 전파하는 것을 특징으로 하는 보안 관리 시스템의 동작 방법.

## 청구항 8

제6항에 있어서,

상기 제1 전자 서명을 생성하는 단계는

상기 복수의 IoT 디바이스 제조사들의 관리 단말과 사전 공유하고 있는,  $n \times n$  ( $n$ 은 2이상의 자연수임) 크기의 사전 지정된 매핑 행렬 - 상기 매핑 행렬은, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들이 서로 다른 원-핫(one-hot) 벡터로 구성되어 있음 - 이 저장되어 있는 매핑 행렬 저장부를 유지하는 단계;

상기 네트워크 관리 장치로부터 상기 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트를 구성하는 데이터를  $n$ 개로 분할하여  $n$ 개의 분할 데이터들을 생성한 후, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에 대해 상기  $n$ 개의 분할 데이터들을 하나씩 순차적으로 할당한 다음, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에서 1의 성분을, 각 열벡터에 할당된 분할 데이터로 치환함과 동시에, 상기 매핑 행렬을 구성하는  $n^2$ 개의 성분들 중 0의 성분들을, 랜덤하게 생성한 더미(dummy) 데이터로 치환하여 치환 행렬을 생성함으로써, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행하는 단계; 및

상기 개인키를 기초로 상기 치환 행렬을 암호화함으로써, 상기 제1 전자 서명을 생성하는 단계

를 포함하고,

상기 처리하는 단계는

상기 치환 행렬과 상기 제1 전자 서명이 생성되면, 상기 치환 행렬과 상기 제1 전자 서명이 포함된 상기 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리하는 것을 특징으로 하는 보안 관리 시스템의 동작 방법.

## 청구항 9

제8항에 있어서,

상기 복수의 IoT 디바이스 제조사들의 관리 단말은

메모리 상에 상기 매핑 행렬을 사전 저장하고 있고, 상기 블록체인 네트워크를 통해 상기 제1 트랜잭션이 수신된 이후, 관리자에 의해 상기 제1 트랜잭션에 포함된 상기 치환 행렬로부터의 상기 제1 취약점 분석 리포트의 복원 명령이 인가되면, 상기 제1 트랜잭션에 포함된 상기 치환 행렬과, 메모리 상에 저장되어 있는 상기 매핑 행렬 간의 요소별 곱셈 연산(element wise product)을 수행하여 연산 행렬을 생성하고, 상기 연산 행렬을 구성하는  $n$ 개의 열벡터들 각각으로부터 0이 아닌 성분을 추출함으로써 상기  $n$ 개의 분할 데이터들을 추출한 후, 상기  $n$ 개의 분할 데이터들을 순차적으로 결합함으로써, 상기 제1 취약점 분석 리포트를 복원하는 것을 특징으로 하는 보안 관리 시스템의 동작 방법.

## 청구항 10

제6항에 있어서,

상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 상기 제1 트랜잭션의 배포가 완료된 이후, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 어느 하나인 제2 관리 단말로부터, 상기 제1 IoT 디바이스에 대한 취약점 보완이 완료되었음을 지시하는 완료 메시지가 수신되면, 상기 개인키를 기초로 상기 완료 메시지에 대한 제2 전자 서명을 생성하는 단계; 및

상기 완료 메시지와 상기 제2 전자 서명이 포함된 제2 트랜잭션을 생성한 후, 상기 제2 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제2 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 단계

를 더 포함하는 보안 관리 시스템의 동작 방법.

## 청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

## 청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

## 발명의 설명

### 기술 분야

[0001] 본 발명은 블록체인 기반의 IoT 네트워크 보안 관리 시스템 및 그 동작 방법에 대한 것이다.

### 배경 기술

[0002] 최근 다양한 사물인터넷(Internet of Things: IoT) 디바이스가 사용되면서, 이러한 IoT 디바이스에서의 보안이 중요한 이슈로 떠오르고 있다.

[0003] IoT 디바이스는 기기의 시스템 성능 자체가 높지 않아, 고도의 네트워크 보안 솔루션을 탑재하는 것이 어렵다는 점에서, 해커의 공격에 취약한 문제가 있다.

[0004] 이로 인해, 최근에는 이러한 IoT 디바이스에서의 보안 취약성을 분석할 수 있는 다양한 솔루션들이 출시되고 있다. 이러한 솔루션들 중 대표적인 것으로서, IoT 디바이스에 설치된 펌웨어의 소스코드를 분석하여, 해당 소스코드 상에 보안 취약점이 있는지 분석하는 솔루션이나, 악성코드나 바이러스 정보를 모아 둔 DB를 이용하여, IoT 디바이스에 수신되는 패킷이나, IoT 디바이스에 설치된 소프트웨어 상에 악성코드나 바이러스가 존재하는지 분석하는 솔루션 등이 존재한다.

[0005] 이러한 IoT 디바이스의 활용이 증대됨에 따라, 가정이나 기업, 상점 등에서 둘 이상의 IoT 디바이스들을 로컬 네트워크로 구성하여 동시에 운용하는 경우도 증가하고 있다. 이로 인해, 로컬 네트워크에 접속된 다수의 IoT 디바이스에 대한 보안 취약점 정보를 수집할 수 있는 통합 관리 솔루션이 도입될 필요가 있다.

[0006] 이와 관련해서, 소정의 로컬 네트워크에 접속된 복수의 IoT 디바이스들에 대한 보안 취약점 정보를 수집하여 이에 대한 분석 리포트를 생성한 후, 이 분석 리포트를 IoT 디바이스를 제조하는 제조사들에 배포할 수 있다면, 제조사들이 취약점 분석 리포트를 상호 검토하여 패치 등을 통한 발빠른 대처를 수행할 수 있다는 점에서, 보안 취약점에 따른 피해의 확산을 막을 수 있을 것이다.

[0007] 특히, 최근에는 소정의 데이터를 체인화된 블록으로 구성하여 중앙 서버가 아닌 노드들에 분산 저장함으로써, 해당 데이터에 대한 무결성을 보장할 수 있는 블록체인 기술이 널리 활용되고 있다는 점에서, 이러한 블록체인 기술을 활용하여, 특정 로컬 네트워크에서의 IoT 디바이스에 대한 보안 취약점 분석 리포트를, IoT 디바이스의 제조사들에 빠르고 안전하게 배포하는 시스템 기술의 도입을 고려할 수 있다.

## 발명의 내용

**해결하려는 과제**

[0008] 본 발명은 로컬 네트워크를 구성하는 IoT 디바이스들에 대한 보안 취약점 분석 리포트를, 블록체인 네트워크를 통해 IoT 디바이스 제조사들의 관리 단말로 배포할 수 있는 보안 관리 시스템 및 그 동작 방법을 제시함으로써, IoT 디바이스의 보안 취약점에 대한 빠른 대처가 가능하도록 한다.

**과제의 해결 수단**

[0009] 본 발명의 일실시예에 따른, 로컬 네트워크에 접속된 복수의 IoT 디바이스들의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말이 노드로 참여하고 있는 블록체인 네트워크를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포할 수 있는 보안 관리 시스템은, 상기 네트워크 관리 장치로부터, 상기 복수의 IoT 디바이스들 중 어느 하나인 제1 IoT 디바이스에 대한 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성하는 리포트 수신부 및 암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제1 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 리포트 등록부를 포함한다.

[0010] 또한, 본 발명의 일실시예에 따른, 로컬 네트워크에 접속된 복수의 IoT 디바이스들의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말이 노드로 참여하고 있는 블록체인 네트워크를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포할 수 있는 보안 관리 시스템의 동작 방법은, 상기 네트워크 관리 장치로부터, 상기 복수의 IoT 디바이스들 중 어느 하나인 제1 IoT 디바이스에 대한 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성하는 단계 및 암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제1 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 단계를 포함한다.

**발명의 효과**

[0011] 본 발명은 로컬 네트워크를 구성하는 IoT 디바이스들에 대한 보안 취약점 분석 리포트를, 블록체인 네트워크를 통해 IoT 디바이스 제조사들의 관리 단말로 배포할 수 있는 보안 관리 시스템 및 그 동작 방법을 제시함으로써, IoT 디바이스의 보안 취약점에 대한 빠른 대처가 가능하도록 할 수 있다.

**도면의 간단한 설명**

[0012] 도 1은 본 발명의 일실시예에 따른 보안 관리 시스템의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 보안 관리 시스템의 동작 방법을 도시한 순서도이다.

**발명을 실시하기 위한 구체적인 내용**

[0013] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0014] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로

구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

- [0015] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.
- [0016] 도 1은 본 발명의 일실시예에 따른 보안 관리 시스템의 구조를 도시한 도면이다.
- [0017] 본 발명에 따른 보안 관리 시스템(110)은, 로컬 네트워크에 접속된 복수의 IoT 디바이스들(11, 12, 13)의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치(10)로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)이 노드로 참여하고 있는 블록체인 네트워크(100)를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에 배포할 수 있는 장치로서, 리포트 수신부(111) 및 리포트 등록부(112)를 포함한다.
- [0018] 우선, 본 발명에서는, 가정이나 기업 등에서, 소정의 로컬 네트워크를 구성하고 있는 복수의 IoT 디바이스들(11, 12, 13)과, 상기 로컬 네트워크 관리하는 네트워크 관리 장치(10)가 존재하는 상황임을 가정한다. 이러한 네트워크 관리 장치(10)는 복수의 IoT 디바이스들(11, 12, 13)에 대해, 인터넷 서비스를 제공하기 위한 유무선 공유기나 라우터 등이 될 수 있다.
- [0019] 이때, 네트워크 관리 장치(10)는 로컬 네트워크에 접속된 복수의 IoT 디바이스들(11, 12, 13)의 보안 취약점을 분석하여 취약점 분석 리포트를 생성할 수 있다. 관련해서, 네트워크 관리 장치(10)에는, 복수의 IoT 디바이스들(11, 12, 13)의 펌웨어 소스코드를 분석하여, 소스코드의 보안 취약점을 탐지하거나, 복수의 IoT 디바이스들(11, 12, 13)에 대한 악성코드 또는 바이러스 등을 탐지할 수 있는 솔루션이 설치되어 있을 수 있고, 이로 인해, 네트워크 관리 장치(10)는 복수의 IoT 디바이스들(11, 12, 13)에 대한 보안 취약점을 분석하여, 취약점 분석 리포트를 생성한 후, 이를 본 발명의 보안 관리 시스템(110)으로 전송하도록 구성될 수 있다.
- [0020] 또한, 본 발명에서는, 서로 다른 복수의 IoT 디바이스 제조사들이 관리하고 있는 관리 단말(101, 102, 103, 104, 105, 106)이 블록체인 네트워크(100)의 노드로서 동작하고 있음을 가정한다.
- [0021] 이러한 상황에서, 네트워크 관리 장치(10)에서, 복수의 IoT 디바이스들(11, 12, 13) 중 어느 하나인 제1 IoT 디바이스(11)에 대한 제1 취약점 분석 리포트가 생성됨에 따라, 네트워크 관리 장치(10)로부터 본 발명의 보안 관리 시스템(110)에 상기 제1 취약점 분석 리포트가 수신되면, 리포트 수신부(112)는 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성한다.
- [0022] 그러고 나서, 리포트 등록부(112)는 암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 블록체인 네트워크(100)에 등록 처리함으로써, 상기 제1 트랜잭션이, 블록체인 네트워크(100)를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에 배포되도록 처리한다.
- [0023] 이때, 본 발명의 일실시예에 따르면, 리포트 수신부(111)는 매핑 행렬 저장부(113), 암호화부(114) 및 서명 생성부(115)를 포함할 수 있다.
- [0024] 매핑 행렬 저장부(113)에는 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)과 사전 공유하고 있는,  $n \times n$  ( $n$ 은 2이상의 자연수임) 크기의 사전 지정된 매핑 행렬이 저장되어 있다.
- [0025] 여기서, 상기 매핑 행렬은, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들이 서로 다른 원-핫(one-hot) 벡터로 구

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

성되어 있을 수 있다. 예컨대, n을 3이라고 하는 경우, 상기 매핑 행렬은 '와 같은 형태로 존재할 수 있다.

[0026] 암호화부(114)는 네트워크 관리 장치(10)로부터 상기 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트를 구성하는 데이터를 n개로 분할하여 n개의 분할 데이터들을 생성한 후, 상기 매핑 행렬을 구성하는 n개의 열벡터들 각각에 대해 상기 n개의 분할 데이터들을 하나씩 순차적으로 할당한 다음, 상기 매핑 행렬을 구성하는 n개의 열벡터들 각각에서 1의 성분을, 각 열벡터에 할당된 분할 데이터로 치환함과 동시에, 상기 매핑 행렬을 구성하는  $n^2$ 개의 성분들 중 0의 성분들을, 랜덤하게 생성한 더미(dummy) 데이터로 치환하여 치환 행렬을 생성함으로써, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한다.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

[0027] 관련해서, 상기 매핑 행렬이 '라고 하는 경우, 암호화부(114)는 상기 제1 취약점 분석 리포트를 구성하는 데이터를 3개로 분할하여 3개의 분할 데이터들을 'D1, D2, D3'과 같이 생성한 후, 상기 매핑 행렬을 구

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

성하는 3개의 열벡터들인 '각각에 대해 상기 3개의 분할 데이터들인 'D1, D2, D3'

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

을 하나씩 순차적으로 할당한 다음, '에서 1의 성분을 'D1'으로 치환하고, '에서 1의 성분을 'D

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

2'로 치환하며, '에서 1의 성분을 'D3'으로 치환함과 동시에, 상기 매핑 행렬을 구성하는 9개의 성분들 중 0의 성분들을, 'R1, R2, R3, R4, R5, R6'과 같은 랜덤한 더미 데이터로 치환함으로써,

$$\begin{bmatrix} D1 & R3 & R5 \\ R1 & R4 & D3 \\ R2 & D2 & R6 \end{bmatrix}$$

, '과 같은 치환 행렬을 생성할 수 있다.

[0028] 이렇게, 상기 치환 행렬이 생성되면, 서명 생성부(115)는 상기 개인키를 기초로 상기 치환 행렬을 암호화함으로써, 상기 제1 전자 서명을 생성한다.

[0029] 이때, 리포트 등록부(112)는 상기 치환 행렬과 상기 제1 전자 서명이 생성되면, 상기 치환 행렬과 상기 제1 전자 서명이 포함된 상기 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크(100)에 등록 처리할 수 있다.

[0030] 이때, 본 발명의 일실시예에 따르면, 리포트 등록부(112)는 상기 제1 트랜잭션을 상기 블록체인 네트워크(100)에 등록 처리하기 위해서, 상기 제1 트랜잭션이 생성되면, 상기 블록체인 네트워크(100)의 노드로서 존재하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106) 중, 어느 하나인 제1 관리 단말(101)을 랜덤하게 선택한 후, 상기 제1 관리 단말(101)로 상기 제1 트랜잭션을 전송하면서, 상기 제1 트랜잭션의 상기 블록체인 네트워크(100)의 등록 요청을 전송할 수 있다.

[0031] 이때, 제1 관리 단말(101)은 보안 관리 시스템(110)으로부터 상기 제1 트랜잭션과 함께 상기 등록 요청이 수신

되면, 상기 개인키에 대응되는 사전 발급된 공개키를 기초로, 상기 제1 트랜잭션에 포함된 상기 제1 전자 서명에 대한 복호화 값을 생성한 후, 상기 복호화 값이 상기 제1 트랜잭션에 포함된 암호화된 상기 제1 취약점 분석 리포트와 일치하는지 확인함으로써, 상기 제1 전자 서명에 대한 검증을 수행할 수 있다.

[0032] 만약, 상기 제1 전자 서명에 대한 검증이 완료되면, 제1 관리 단말(101)은 메모리 상에 저장되어 있는 블록체인 데이터에 체인으로 연결된 이전 블록을 기초로 상기 제1 트랜잭션이 포함된 제1 블록을 생성하고, 상기 제1 블록을 상기 블록체인 데이터에 체인으로 연결함으로써, 상기 제1 블록에 대한 저장을 완료한 후, 상기 블록체인 네트워크(100)를 통해 상기 제1 블록을, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106) 중 상기 제1 관리 단말(101)을 제외한 나머지 관리 단말(102, 103, 104, 105, 106)로 전파할 수 있다.

[0033] 이를 통해, 상기 블록체인 네트워크(100)의 노드로서 존재하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에, 상기 제1 트랜잭션이 전파되게 된다.

[0034] 이때, 본 발명의 일실시예에 따르면, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)은, 메모리 상에 상기 매핑 행렬을 사전 저장하고 있고, 상기 블록체인 네트워크(100)를 통해 상기 제1 트랜잭션이 수신된 이후, 관리자에 의해 상기 제1 트랜잭션에 포함된 상기 치환 행렬로부터의 상기 제1 취약점 분석 리포트의 복원 명령이 인가되면, 상기 제1 트랜잭션에 포함된 상기 치환 행렬과, 메모리 상에 저장되어 있는 상기 매핑 행렬 간의 요소별 곱셈 연산(element wise product)을 수행하여 연산 행렬을 생성하고, 상기 연산 행렬을 구성하는 n개의 열벡터를 각각으로부터 0이 아닌 성분을 추출함으로써 상기 n개의 분할 데이터들을 추출한 후, 상기 n개의 분할 데이터들을 순차적으로 결합함으로써, 상기 제1 취약점 분석 리포트를 복원할 수 있다.

[0035] 관련해서, 전술한 예와 같이, 상기 치환 행렬이  $\begin{bmatrix} D1 & R3 & R5 \\ R1 & R4 & D3 \\ R2 & D2 & R6 \end{bmatrix}$  '이고, 상기 매핑 행렬이 '  $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$  '라고 하는 경우, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)은, 상기 블록체인 네트워크(100)를 통해 상기 제1 트랜잭션이 수신된 이후, 각 관리 단말의 관리자에 의해 상기 제1 트랜잭션에 포함된 상기 치환 행렬로부터의 상기 제1 취약점 분석 리포트의 복원 명령이 인가되면, 상기

치환 행렬인  $\begin{bmatrix} D1 & R3 & R5 \\ R1 & R4 & D3 \\ R2 & D2 & R6 \end{bmatrix}$  '와 상기 매핑 행렬인  $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$  ' 간의 요소별 곱셈 연산을 수행하여  $\begin{bmatrix} D1 & 0 & 0 \\ 0 & 0 & D3 \\ 0 & D2 & 0 \end{bmatrix}$  '와 같은 연산 행렬을 생성할 수 있다.

[0036] 그리고 나서, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)은, 상기 연산 행렬인  $\begin{bmatrix} D1 & 0 & 0 \\ 0 & 0 & D3 \\ 0 & D2 & 0 \end{bmatrix}$  '을 구성하는 3개의 열벡터를 각각으로부터 0이 아닌 성분을 추출함으로써 'D1, D2, D3'이라는 분할 데이터들을 추출한 후, 상기 3개의 분할 데이터들을 순차적으로 결합함으로써, 상기 제1 취약점 분석 리포트를 복원할 수 있다.

[0037] 이를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)을 관리하는 각 관리자는, 자신의 관리 단말에서 복원된 상기 제1 취약점 분석 리포트를 확인함으로써, 제1 IoT 디바이스(11)에

보안 취약점이 있음을 파악할 수 있다. 그러면, 상기 복수의 IoT 디바이스 제조사들 중 제1 IoT 디바이스(11)를 제조한 제조사의 관리자는 신속하게 보안 취약점을 해소하기 위한 패치 등을 준비하여, 제1 IoT 디바이스(11)에 대한 펌웨어 업데이트 등의 조치를 수행함으로써, 제1 IoT 디바이스(11)의 보안 취약점으로 인해 상기 로컬 네트워크를 구성하고 있는 나머지 IoT 디바이스들에까지 보안 위협이 미치는 것을 방지할 수 있다.

[0038] 이때, 본 발명에서는, 상기 제1 취약점 분석 리포트를 제1 IoT 디바이스(11)의 제조사의 관리 단말에만 전달하는 것이 아니라, 블록체인 네트워크(100)를 통해, 노드로 참여하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106) 전체에 전달하는 특징을 가지고 있는데, 이렇게, 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106) 전체에 대해, 취약점 분석 리포트를 전달하게 되면, 해당 취약점 분석 리포트에 매칭되는 IoT 디바이스의 제조사가 아닌 제조사에서도, 자신의 IoT 디바이스에 대해 선제적으로 패치 등의 보안 조치를 수행할 수 있기 때문에, 보다 높은 보안성을 유지할 수 있는 장점이 있다.

[0039] 본 발명의 일실시예에 따르면, 보안 관리 시스템(110)은 완료 메시지 수신부(116) 및 완료 메시지 등록부(117)를 더 포함할 수 있다.

[0040] 완료 메시지 수신부(116)는 상기 블록체인 네트워크(100)를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에 상기 제1 트랜잭션의 배포가 완료된 이후, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 어느 하나인 제2 관리 단말(102)로부터, 상기 제1 IoT 디바이스(11)에 대한 취약점 보완이 완료되었음을 지시하는 완료 메시지가 수신되면, 상기 개인키를 기초로 상기 완료 메시지에 대한 제2 전자 서명을 생성한다.

[0041] 관련해서, 상기 제1 IoT 디바이스(11)의 제조사의 관리 단말을 제2 관리 단말(102)이라고 하고, 전술한 설명과 같이, 상기 블록체인 네트워크(100)를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에 상기 제1 트랜잭션의 배포가 완료됨으로 인해, 상기 제1 IoT 디바이스(11)의 제조사의 관리자가, 제2 관리 단말(102)에 배포된 상기 제1 트랜잭션 상의 상기 제1 취약점 분석 리포트를 확인한 후, 상기 제1 IoT 디바이스(11)의 보안 취약점에 대한 보완 작업을 완료하였다고 가정하자.

[0042] 그러면, 관리자는 제2 관리 단말(102)을 통해서, 상기 제1 IoT 디바이스(11)에 대한 취약점 보완이 완료되었음을 지시하는 완료 메시지를 생성하여 본 발명의 보안 관리 시스템(110)으로 전송할 수 있다.

[0043] 이로 인해, 제2 관리 단말(102)로부터 본 발명의 보안 관리 시스템(110)에 상기 완료 메시지가 수신되면, 완료 메시지 수신부(116)는 상기 개인키를 기초로 상기 완료 메시지에 대한 제2 전자 서명을 생성할 수 있다.

[0044] 그 이후, 완료 메시지 등록부(117)는 상기 완료 메시지와 상기 제2 전자 서명이 포함된 제2 트랜잭션을 생성한 후, 상기 제2 트랜잭션을 상기 블록체인 네트워크(100)에 등록 처리함으로써, 상기 제2 트랜잭션이, 상기 블록체인 네트워크(100)를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말(101, 102, 103, 104, 105, 106)에 배포되도록 처리한다.

[0045] 이를 통해, 상기 복수의 IoT 디바이스 제조사들의 각 관리자는 상기 제2 트랜잭션에 포함된 상기 완료 메시지를 확인함으로써, 상기 제1 IoT 디바이스(11)에 대한 보안 취약점이 해소되었음을 인지할 수 있다.

[0046] 도 2는 본 발명의 일실시예에 따른, 로컬 네트워크에 접속된 복수의 IoT 디바이스들의 보안 취약점을 분석하여 취약점 분석 리포트를 생성하는 네트워크 관리 장치로부터, 취약점 분석 리포트를 수신하여, 수신된 취약점 분석 리포트를, 서로 다른 복수의 IoT 디바이스 제조사들의 관리 단말이 노드로 참여하고 있는 블록체인 네트워크를 통해, 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포할 수 있는 보안 관리 시스템의 동작 방법을 도시한 순서도이다.

[0047] 단계(S210)에서는 상기 네트워크 관리 장치로부터, 상기 복수의 IoT 디바이스들 중 어느 하나인 제1 IoT 디바이스에 대한 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행한 후, 사전 설정된 개인키를 기초로, 암호화된 상기 제1 취약점 분석 리포트에 대한 제1 전자 서명을 생성한다.

[0048] 단계(S220)에서는 암호화된 상기 제1 취약점 분석 리포트와 상기 제1 전자 서명이 포함된 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제1 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리한다.

[0049] 이때, 본 발명의 일실시예에 따르면, 단계(S220)에서는 상기 제1 트랜잭션이 생성되면, 상기 블록체인 네트워크의 노드로서 존재하고 있는 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중, 어느 하나인 제1 관리 단말을

랜덤하게 선택한 후, 상기 제1 관리 단말로 상기 제1 트랜잭션을 전송하면서, 상기 제1 트랜잭션의 상기 블록체인 네트워크의 등록 요청을 전송할 수 있다.

[0050] 이때, 상기 제1 관리 단말은 상기 보안 관리 시스템으로부터 상기 제1 트랜잭션과 함께 상기 등록 요청이 수신되면, 상기 개인키에 대응되는 사전 발급된 공개키를 기초로, 상기 제1 트랜잭션에 포함된 상기 제1 전자 서명에 대한 복호화 값을 생성한 후, 상기 복호화 값이 상기 제1 트랜잭션에 포함된 암호화된 상기 제1 취약점 분석 리포트와 일치하는지 확인함으로써, 상기 제1 전자 서명에 대한 검증을 수행한 후, 상기 제1 전자 서명에 대한 검증이 완료되면, 메모리 상에 저장되어 있는 블록체인 데이터에 체인으로 연결된 이전 블록을 기초로 상기 제1 트랜잭션이 포함된 제1 블록을 생성하고, 상기 제1 블록을 상기 블록체인 데이터에 체인으로 연결함으로써, 상기 제1 블록에 대한 저장을 완료한 후, 상기 블록체인 네트워크를 통해 상기 제1 블록을, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 상기 제1 관리 단말을 제외한 나머지 관리 단말로 전파할 수 있다.

[0051] 또한, 본 발명의 일실시예에 따르면, 단계(S210)에서는 상기 복수의 IoT 디바이스 제조사들의 관리 단말과 사전 공유하고 있는,  $n \times n$  ( $n$ 은 2이상의 자연수임) 크기의 사전 지정된 매핑 행렬(상기 매핑 행렬은, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들이 서로 다른 원-핫 벡터로 구성되어 있음)이 저장되어 있는 매핑 행렬 저장부를 유지하는 단계, 상기 네트워크 관리 장치로부터 상기 제1 취약점 분석 리포트가 수신되면, 상기 제1 취약점 분석 리포트를 구성하는 데이터를  $n$ 개로 분할하여  $n$ 개의 분할 데이터들을 생성한 후, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에 대해 상기  $n$ 개의 분할 데이터들을 하나씩 순차적으로 할당한 다음, 상기 매핑 행렬을 구성하는  $n$ 개의 열벡터들 각각에서 1의 성분을, 각 열벡터에 할당된 분할 데이터로 치환함과 동시에, 상기 매핑 행렬을 구성하는  $n^2$ 개의 성분들 중 0의 성분들을, 랜덤하게 생성한 더미 데이터로 치환하여 치환 행렬을 생성함으로써, 상기 제1 취약점 분석 리포트에 대한 암호화를 수행하는 단계 및 상기 개인키를 기초로 상기 치환 행렬을 암호화함으로써, 상기 제1 전자 서명을 생성하는 단계를 포함할 수 있다.

[0052] 이때, 단계(S220)에서는 상기 치환 행렬과 상기 제1 전자 서명이 생성되면, 상기 치환 행렬과 상기 제1 전자 서명이 포함된 상기 제1 트랜잭션을 생성한 후, 상기 제1 트랜잭션을 상기 블록체인 네트워크에 등록 처리할 수 있다.

[0053] 이때, 본 발명의 일실시예에 따르면, 상기 복수의 IoT 디바이스 제조사들의 관리 단말은, 메모리 상에 상기 매핑 행렬을 사전 저장하고 있고, 상기 블록체인 네트워크를 통해 상기 제1 트랜잭션이 수신된 이후, 관리자에 의해 상기 제1 트랜잭션에 포함된 상기 치환 행렬로부터의 상기 제1 취약점 분석 리포트의 복원 명령이 인가되면, 상기 제1 트랜잭션에 포함된 상기 치환 행렬과, 메모리 상에 저장되어 있는 상기 매핑 행렬 간의 요소별 곱셈 연산을 수행하여 연산 행렬을 생성하고, 상기 연산 행렬을 구성하는  $n$ 개의 열벡터들 각각으로부터 0이 아닌 성분을 추출함으로써 상기  $n$ 개의 분할 데이터들을 추출한 후, 상기  $n$ 개의 분할 데이터들을 순차적으로 결합함으로써, 상기 제1 취약점 분석 리포트를 복원할 수 있다.

[0054] 또한, 본 발명의 일실시예에 따르면, 상기 보안 관리 시스템의 동작 방법은 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 상기 제1 트랜잭션의 배포가 완료된 이후, 상기 복수의 IoT 디바이스 제조사들의 관리 단말 중 어느 하나인 제2 관리 단말로부터, 상기 제1 IoT 디바이스에 대한 취약점 보완이 완료되었음을 지시하는 완료 메시지가 수신되면, 상기 개인키를 기초로 상기 완료 메시지에 대한 제2 전자 서명을 생성하는 단계 및 상기 완료 메시지와 상기 제2 전자 서명이 포함된 제2 트랜잭션을 생성한 후, 상기 제2 트랜잭션을 상기 블록체인 네트워크에 등록 처리함으로써, 상기 제2 트랜잭션이, 상기 블록체인 네트워크를 통해 상기 복수의 IoT 디바이스 제조사들의 관리 단말에 배포되도록 처리하는 단계를 더 포함할 수 있다.

[0055] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 보안 관리 시스템의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 보안 관리 시스템의 동작 방법은 도 1을 이용하여 설명한 보안 관리 시스템(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0056] 본 발명의 일실시예에 따른 보안 관리 시스템의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0057] 또한, 본 발명의 일실시예에 따른 보안 관리 시스템의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기

테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0058] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

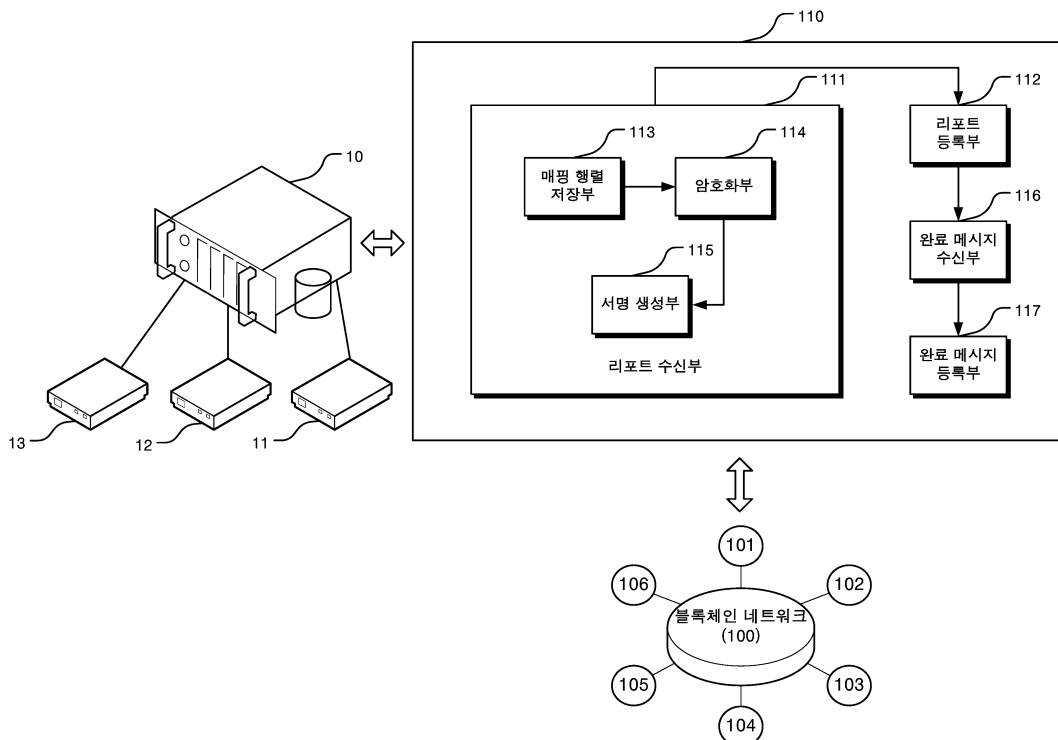
[0059] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

## 부호의 설명

[0060] 110: 보안 관리 시스템  
 111: 리포트 수신부 112: 리포트 등록부  
 113: 매핑 행렬 저장부 114: 암호화부  
 115: 서명 생성부 116: 완료 메시지 수신부  
 117: 완료 메시지 등록부  
 10: 네트워크 관리 장치  
 11, 12, 13: 복수의 IoT 디바이스들  
 100: 블록체인 네트워크  
 101, 102, 103, 104, 105, 106: 복수의 IoT 디바이스 제조사들의 관리 단말

## 도면

### 도면1



도면2

