(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년08월18일
(11) 등록번호 10-2433435
(24) 등록일자 2022년08월11일

(51) 국제특허분류(Int. Cl.)
G06F 11/14 (2006.01) *G06F 21/56* (2013.01)
(52) CPC특허분류
G06F 11/142 (2013.01)
G06F 11/1451 (2013.01)
(21) 출원번호 10-2020-0186971
(22) 출원일자 2020년12월30일
심사청구일자 2020년12월30일
(65) 공개번호 10-2022-0095454
(43) 공개일자 2022년07월07일
(56) 선행기술조사문헌
KR1020090090801 A
(뒷면에 계속)

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
김종
경상북도 포항시 남구 지곡로 155, 9동 1801호
나동빈
경기도 군포시 용호2로 11, 202동 1404호
(뒷면에 계속)
(74) 대리인
특허법인이상

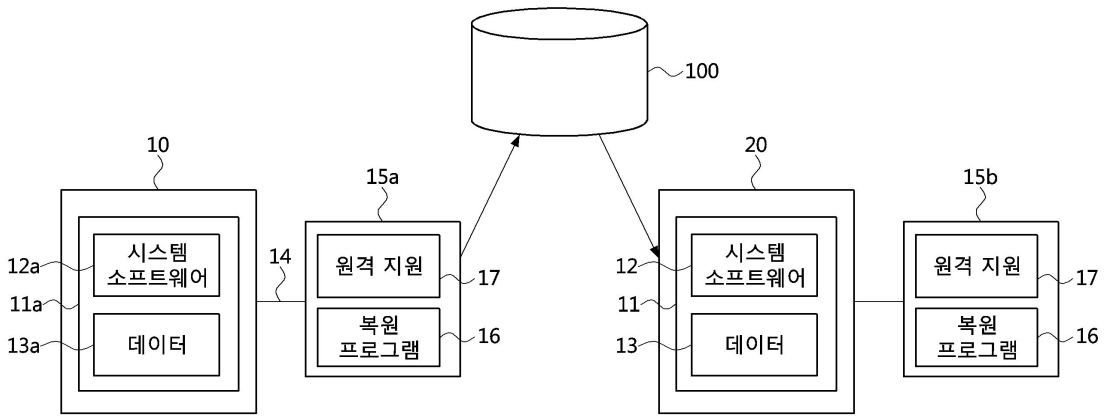
전체 청구항 수 : 총 13 항 심사관 : 김계준

(54) 발명의 명칭 **랜섬웨어 피해 복원을 위한 P2P 디스크 복원 방법 및 장치**

(57) 요 약

사물인터넷이나 산업제어시스템 환경에서 랜섬웨어에 감염되지 않은 동종 기기의 디스크의 내용을 복제하여 피해 기기를 복원하는 피어투피어(P2P) 디스크 복원 방법 및 장치가 개시된다. 네트워크에 연결되는 복원 관리 서버에 의해 실행되는 감염 디스크의 복원을 위한 P2P 디스크 복원 방법으로서, 네트워크 내에서 랜섬웨어나 맬웨어에 감염된 제1 IoT 기기에 연결되어 있는 제1 복원 기기를 활성화하는 단계, 제1 복원 기기로부터 제1 IoT 기기와 동종의 제2 IoT 기기의 탐색 요청을 받는 단계, 탐색 요청에 포함된 제1 IoT 기기에 대한 기기 정보에 기초하여 네트워크 내 제2 IoT 기기를 탐색하는 단계, 및 제1 IoT 기기의 복원 요청을 기탐색된 제2 IoT 기기에 연결된 제2 복원 기기에 전달하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
G06F 11/1458 (2013.01)
G06F 21/568 (2013.01)
H04L 12/12 (2013.01)
H04L 67/104 (2022.05)
H04L 67/12 (2022.05)

(72) 발명자
김태훈
경상북도 포항시 남구 청암로 77
지상우
경상북도 포항시 남구 연일읍 유강길17번길 16-5, 201호
이경민
서울특별시 서대문구 연희로 132-1, 406호
김한준
서울특별시 강남구 언주로116길 6, 104동 1002호

(56) 선행기술조사문헌
KR1020150032703 A
KR101954976 B1
KR1020170121911 A
KR1020160005828 A

이 발명을 지원한 국가연구개발사업

과제고유번호	1711103119
과제번호	2018-0-01392-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발
연구과제명	내재적 기능 기반의 랜섬웨어 공격 피해 복원
기 여 율	1/1
과제수행기관명	포항공과대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

네트워크에 연결되는 복원 관리 서버에 의해 실행되는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 방법으로서,

네트워크 내에서 랜섬웨어나 맬웨어에 감염된 제1 IoT(internet of thing) 기기에 연결되어 있는 제1 복원 기기를 활성화하는 단계;

상기 제1 복원 기기로부터 상기 제1 IoT 기기와 동종의 제2 IoT 기기의 탐색 요청을 받는 단계;

상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 네트워크 내 상기 제2 IoT 기기를 탐색하는 단계; 및

상기 제1 IoT 기기의 복원 요청을 탐색된 제2 IoT 기기에 연결된 제2 복원 기기에 전달하는 단계;를 포함하는 P2P 디스크 복원 방법.

청구항 2

청구항 1에 있어서,

상기 제2 복원 기기의 동작 제어에 의해 상기 제2 IoT 기기는 자신의 주저장장치에 저장된 청크 또는 펌웨어를 복사하여 상기 제1 IoT 기기의 주저장장치에 실시간 덮어쓰기하는, P2P 디스크 복원 방법.

청구항 3

청구항 1에 있어서,

상기 네트워크에서 주저장장치의 복원에 의한 상기 제1 IoT 기기의 정상 상태가 감지되면, 상기 제1 복원 기기 및 상기 제2 복원 기기의 작동을 종료하는 단계를 더 포함하는, P2P 디스크 복원 방법.

청구항 4

네트워크에 연결되는 복원 기기에 의해 실행되는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 방법으로서,

네트워크 내에서 랜섬웨어나 맬웨어에 감염된 제1 IoT(internet of thing) 기기에 연결되고 상기 네트워크에 연결되어 있는 복원 관리 서버로부터 활성화를 위한 제1 제어 신호를 수신하는 단계;

상기 제1 제어 신호에 응하여 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 상기 복원 관리 서버에 전송하는 단계;

상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 시스템 소프트웨어로서 기능하는 단계;

상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 네트워크에 연결된 복원 관리 서버에 의해 탐색된 상기 제2 IoT 기기로부터의 상기 제1 IoT 기기의 주저장장치에 대한 덮어쓰기를 허용하는 단계; 및

상기 덮어쓰기가 완료되면 상기 제1 IoT 기기를 재부팅하는 단계;를 포함하는 P2P 디스크 복원 방법.

청구항 5

청구항 4에 있어서,

상기 제1 제어 신호에 응하여 자체 저장된 기능 유지 프로그램에 의해 상기 제1 IoT 기기의 재부팅이 완료될 때까지 상기 제1 IoT 기기의 본래 기능을 수행하는 단계를 더 포함하는 P2P 디스크 복원 방법.

청구항 6

청구항 4에 있어서,

상기 제2 IoT 기기에 연결되는 제2 복원 기기는 상기 복원 관리 서버로부터의 제2 제어 신호에 응하여 활성화될 때 상기 덮어쓰기의 동작을 위해 상기 제2 IoT 기기의 주저장장치의 내용이 수정되는 경우, 상기 덮어쓰기의 동작 시간동안 상기 제2 IoT 기기의 특정 기능의 동작을 한시적으로 중지시키는, P2P 디스크 복원 방법.

청구항 7

청구항 4에 있어서,

상기 복원 기기는 자체 저장된 데이터 로그 프로그램에 의해 상기 제1 IoT 기기의 정상 동작 상태에서 상기 제1 IoT 기기의 데이터 부분 내용이 수정될 때 해당 수정 오퍼레이션에 대한 내용을 로그로 별도의 자체 저장 공간에 저장하고, 상기 덮어쓰기의 완료 후에 상기 저장 공간에 저장된 로그에 기초하여 상기 제1 IoT 기기의 데이터를 복구하는, P2P 디스크 복원 방법.

청구항 8

네트워크에 연결되는 복원 관리 서버와 복원 기기를 포함하는, 랜섬웨어나 맬웨어에 의해 감염된 제1 IoT(internet of thing) 기기의 주저장장치의 복원을 위한 P2P(pear to pear) 디스크 복원 장치로서, 상기 복원 기기는,

상기 복원 관리 서버로부터 제1 제어 신호를 수신하고, 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 상기 복원 관리 서버에 전송하고, 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 시스템 소프트웨어로서 기능하며, 상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 복원 관리 서버에 의해 탐색된 제2 IoT 기기로부터의 상기 제1 IoT 기기의 주저장장치에 대한 덮어쓰기를 허용하고, 상기 덮어쓰기가 완료되면 상기 제1 IoT 기기를 재부팅하는 복원 프로그램; 및

상기 제1 제어 신호 또는 별도의 트리거 신호나 액티베이션 신호에 기초하여 상기 복원 기기에 전원을 공급하여 상기 복원 기기를 활성화하는 원격 전원;

을 포함하는 P2P 디스크 복원 장치.

청구항 9

청구항 8에 있어서,

상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 복원 혹은 상기 재부팅이 완료될 때까지 상기 제1 IoT 기기의 본래 기능을 수행하는 기능 유지 프로그램을 더 포함하는 P2P 디스크 복원 장치.

청구항 10

청구항 8에 있어서,

상기 제1 IoT 기기의 정상 동작 상태에서 상기 제1 IoT 기기의 데이터 부분 내용이 수정될 때 해당 수정 오퍼레이션에 대한 내용을 로그로 저장하고, 상기 덮어쓰기의 완료 후에 기저장된 상기 로그에 기초하여 상기 제1 IoT 기기의 데이터를 복구하는 데이터 로그 프로그램; 및

상기 데이터 로그 프로그램에 의해 지정되는 로그를 저장하는 저장 공간;을 더 포함하는 P2P 디스크 복원 장치.

청구항 11

네트워크에 연결되는 복원 관리 서버와 복원 기기를 포함하는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 장치로서, 상기 복원 관리 서버는,

상기 네트워크 내 제1 IoT 기기의 랜섬웨어 또는 맬웨어 피해 감지에 따라 상기 제1 IoT 기기에 연결된 제1 복원 기기에 전송할 제1 제어 신호를 생성하는 제어신호 생성부;

상기 제1 복원 기기로부터 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 받고, 상기 탐색 요청에 포함된 상기 제1 IoT 기기의 기기 정보를 추출하는 메시지 처리부; 및

상기 제1 IoT 기기의 기기 정보에 기초하여 상기 네트워크 내에서 상기 제2 IoT 기기를 탐색하는 탐색부;를 포

함하는 P2P 디스크 복원 장치.

청구항 12

청구항 11에 있어서,

상기 네트워크 내 상기 제1 IoT 기기의 랜섬웨어 또는 맬웨어 피해를 감지하는 감지부를 더 포함하며, 상기 감지부에서 생성된 출력 신호는 상기 제어신호 생성부에 전달되는 P2P 디스크 복원 장치.

청구항 13

청구항 12에 있어서,

상기 제1 IoT 기기의 주저장장치의 복원에 따라 네트워크 상에서 상기 제1 IoT 기기의 정상 상태가 상기 감지부에 감지되면, 상기 감지부의 신호에 따라 상기 제어신호 생성부는 상기 제1 복원 기기 및 상기 제2 IoT 기기에 연결된 제2 복원 기기의 작동을 종료하기 위한 제어신호나 작동종료신호를 생성하는, P2P 디스크 복원 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 피어-투-피어(pear to pear, P2P) 디스크 복원을 이용한 랜섬웨어 피해 복원 방법에 관한 것으로, 보다 상세하게는 사물인터넷(internet of thing, IoT)이나 산업제어시스템(industry control system, ICS) 환경에서 랜섬웨어에 감염되지 않은 동종 기기의 디스크의 내용을 복제하여 피해 기기를 복원하는 P2P 디스크 복원 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 컴퓨터 시스템을 강제로 잠그거나 파일을 암호화하여 금전을 지불해야 잠금 해제 형태 또는 파일을 복호화해 주는 형태의 악성코드인 '랜섬웨어(ransomware)'는 개인 사용자뿐만 아니라 기업, 산업 시설 또는 기간 시설에도 피해를 주고 있다. 이에 따라 랜섬웨어를 탐지하는 연구와 랜섬웨어 피해를 복원하는 방법에 대한 다양한 연구가 대두되고 있다.

[0003] 하지만 대부분의 기존 연구는 백업을 통해 피해를 복원하거나 SSD(solid state dirve) 등의 특정한 디스크의 사용을 필요로 하기 때문에, 사물인터넷 환경이나 스마트 팩토리(smart factory) 등의 산업제어시스템 환경에서 이를 적용하기가 어렵다는 단점이 있다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 공개특허공보 제10-2017-0121911호(2017.11.03)

(특허문헌 0002) 공개특허공보 제10-2019-0140314호(2019.12.19)

발명의 내용

해결하려는 과제

[0005] 본 발명은 종래 기술의 문제점을 해결하기 위해 도출된 것으로, 본 발명의 목적은 사물인터넷이나 스마트 팩토리 등의 산업제어시스템 환경에서 하나 이상의 IoT(internet of thing) 기기가 랜섬웨어에 감염되었을 때 랜섬웨어에 감염되지 않은 다른 동종 기기를 이용하여 감염된 기기의 디스크를 복원할 수 있는, 랜섬웨어 피해 복원을 위한 P2P(pear to pear) 디스크 복원 방법 및 장치를 제공하는데 있다.

[0006] 본 발명의 다른 목적은, 사물인터넷이나 스마트 팩토리에서 기기의 동작을 유지하는데 필요한 시스템 소프트웨어 또는 필수 어플리케이션까지 복원할 수 있는, 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 방법 및 장치를 제공하는데 있다.

과제의 해결 수단

[0007] 상기 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른 랜섬웨어 피해 복원을 위한 P2P(pear to pear) 디스크 복원 방법은, 네트워크에 연결되는 복원 관리 서버에 의해 실행되는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 방법으로서, 네트워크 내에서 랜섬웨어나 맬웨어에 감염된 제1 IoT(internet of thing) 기기에 연결되어 있는 제1 복원 기기를 활성화하는 단계; 상기 제1 복원 기기로부터 상기 제1 IoT 기기와 동종의 제2 IoT 기기의 탐색 요청을 받는 단계; 상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 네트워크 내 상기 제2 IoT 기기를 탐색하는 단계; 및 상기 제1 IoT 기기의 복원 요청을 탐색된 제2 IoT 기기에 연결된 제2 복원 기기에 전달하는 단계를 포함한다.

[0008] 일실시예에서, 상기 제2 복원 기기의 동작 제어에 의해 상기 제2 IoT 기기는 자신의 주저장장치에 저장된 청크 또는 펌웨어를 복사하여 상기 제1 IoT 기기의 주저장장치에 실시간 덮어쓰기한다.

[0009] 일실시예에서, P2P 디스크 복원 방법은, 상기 네트워크에서 주저장장치의 복원에 의한 상기 제1 IoT 기기의 정상 상태가 감지되면, 상기 제1 복원 기기 및 상기 제2 복원 기기의 작동을 종료하는 단계를 더 포함한다.

[0010] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 측면에 따른 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 방법은, 네트워크에 연결되는 복원 기기에 의해 실행되는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 방법으로서, 네트워크 내에서 랜섬웨어나 맬웨어에 감염된 제1 IoT(internet of thing) 기기에 연결되고 상기 네트워크에 연결되어 있는 복원 관리 서버로부터 활성화를 위한 제1 제어 신호를 수신하는 단계; 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 상기 복원 관리 서버에 전송하는 단계; 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 시스템 소프트웨어로서 기능하는 단계; 상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 네트워크에 연결된 복원 관리 서버에 의해 탐색된 상기 제2 IoT 기기로부터의 상기 제1 IoT 기기의 주저장장치에 대한 덮어쓰기를 허용하는 단계; 및 상기 덮어쓰기가 완료되면 상기 제1 IoT 기기를 재부팅하는 단계를 포함한다.

[0011] 일실시예에서, P2P 디스크 복원 방법은, 상기 제1 제어 신호에 응하여 자체 저장된 기능 유지 프로그램에 의해 상기 제1 IoT 기기의 재부팅이 완료될 때까지 상기 제1 IoT 기기의 본래 기능을 수행하는 단계를 더 포함한다.

[0012] 일실시예에서, 상기 제2 IoT 기기에 연결되는 제2 복원 기기는 상기 복원 관리 서버로부터의 제2 제어 신호에 응하여 활성화될 때 그리고 상기 덮어쓰기의 동작을 위해 상기 제2 IoT 기기의 주저장장치의 내용이 수정되는 경우, 상기 덮어쓰기의 동작 시간동안 상기 제2 IoT 기기의 특정 기능의 동작을 한시적으로 중지시킬 수 있다.

[0013] 일실시예에서, 상기 복원 기기는 자체 저장된 데이터 로그 프로그램에 의해 상기 제1 IoT 기기의 정상 동작 상태에서 상기 제1 IoT 기기의 데이터 부분 내용이 수정될 때 해당 수정 오퍼레이션에 대한 내용을 로그로 별도의 자체 저장 공간에 저장하고, 상기 덮어쓰기의 완료 후에 상기 저장 공간에 저장된 로그에 기초하여 상기 제1 IoT 기기의 데이터를 복구할 수 있다.

[0014] 상기 기술적 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 장치는, 네트워크에 연결되는 복원 관리 서버와 복원 기기를 포함하는, 랜섬웨어나 맬웨어에 의해 감염된 제1 IoT(internet of thing) 기기의 주저장장치의 복원을 위한 P2P(pear to pear) 디스크 복원 장치이다. 여기서, 상기 복원 기기는, 상기 복원 관리 서버로부터 제1 제어 신호를 수신하고, 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 상기 복원 관리 서버에 전송하고, 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 시스템 소프트웨어로서 기능하며, 상기 탐색 요청에 포함된 상기 제1 IoT 기기에 대한 기기 정보에 기초하여 상기 복원 관리 서버에 의해 탐색된 제2 IoT 기기로부터의 상기 제1 IoT 기기의 주저장장치에 대한 덮어쓰기를 허용하고, 상기 덮어쓰기가 완료되면 상기 제1 IoT 기기를 재부팅하는 복원 프로그램; 및 상기 제1 제어 신호 또는 별도의 트리거 신호나 액티베이션 신호에 기초하여 상기 복원 기기에 전원을 공급하여 상기 복원 기기를 활성화하는 원격 전원을 포함한다.

[0015] 일실시예에서, P2P 디스크 복원 장치는, 상기 제1 제어 신호에 응하여 상기 제1 IoT 기기의 복원 혹은 상기 재부팅이 완료될 때까지 상기 제1 IoT 기기의 본래 기능을 수행하는 기능 유지 프로그램을 더 포함한다.

[0016] 일실시예에서, P2P 디스크 복원 장치는, 상기 제1 IoT 기기의 정상 동작 상태에서 상기 제1 IoT 기기의 데이터 부분 내용이 수정될 때 해당 수정 오퍼레이션에 대한 내용을 로그로 저장하고, 상기 덮어쓰기의 완료 후에 기저장된 상기 로그에 기초하여 상기 제1 IoT 기기의 데이터를 복구하는 데이터 로그 프로그램; 및 상기 데이터 로그 프로그램에 의해 지정되는 로그를 저장하는 저장 공간을 더 포함할 수 있다.

[0017] 상기 기술적 과제를 해결하기 위한 본 발명의 또 다른 측면에 따른 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 장치는, 네트워크에 연결되는 복원 관리 서버와 복원 기기를 포함하는, 랜섬웨어나 맬웨어에 의해 감염된 디스크의 복원을 위한 P2P(pear to pear) 디스크 복원 장치이다. 여기서, 상기 복원 관리 서버는, 상기 네트워크 내 제1 IoT 기기의 랜섬웨어 또는 맬웨어 피해 감지에 따라 상기 제1 IoT 기기에 연결된 제1 복원 기기에 전송할 제1 제어 신호를 생성하는 제어신호 생성부; 상기 제1 복원 기기로부터 상기 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 받고, 상기 탐색 요청에 포함된 상기 제1 IoT 기기의 기기 정보를 추출하는 메시지 처리부; 및 상기 제1 IoT 기기의 기기 정보에 기초하여 상기 네트워크 내에서 상기 제2 IoT 기기를 탐색하는 탐색부를 포함한다.

[0018] 일실시예에서, P2P 디스크 복원 장치는 상기 네트워크 내 상기 제1 IoT 기기의 랜섬웨어 또는 맬웨어 피해를 감지하는 감지부를 더 포함한다. 상기 감지부에서 생성된 출력 신호는 상기 제어신호 생성부에 전달된다.

[0019] 일실시예에서, 상기 제1 IoT 기기의 주저장장치의 복원에 따라 네트워크 상에서 상기 제1 IoT 기기의 정상 상태가 상기 감지부에 감지되면, 상기 제어신호 생성부는 상기 감지부의 신호에 따라 상기 제1 복원 기기 및 상기 제2 복원 기기의 작동을 종료하기 위한 제어신호나 작동종료신호를 생성할 수 있다.

발명의 효과

[0020] 전술한 랜섬웨어 피해 복원을 위한 P2P(pear to pear) 디스크 복원 방법 및 장치를 사용하는 경우에는, 랜섬웨어(Ransomware) 또는 맬웨어(Malware)로 인해 사물인터넷(internet of thing, IoT) 기기나 산업제어시스템의 디스크 내용이 손상되었을 때, 실제 작동하고 있는 다른 동종 기기의 디스크 내용을 복사하여 감염된 기기의 디스크를 효과적으로 복원할 수 있다.

[0021] 또한, 본 발명에 의하면, 복원의 소스(source)가 되는 기기의 작동이 랜섬웨어 피해 기기의 디스크 내용을 수정하는 경우, 해당 복원의 소스가 되는 기기의 작동을 한시적으로 중지시키고 그에 의해 덮어쓰기가 수행되는 동안에 복원의 소스의 내용이 변경되는 것을 방지(즉, 소스가 되는 기기의 복원 동작이 스스로의 디스크 내용을 수정하는 것을 방지)함으로써 복원의 소스가 되는 기기의 복원 기기를 이용하여 랜섬웨어 피해 기기의 디스크를 신뢰성있고 신속하게 복원할 수 있다.

[0022] 또한, 본 발명에 의하면, 복원 소스가 되는 기기의 작동을 중지시킬 경우, 복원 기기에 존재하는 필수 프로그램을 실행하여 복원대상 기기의 디스크 복원 과정에도 복원대상 기기가 수행해야 하는 기능을 지속적으로 수행할 수 있도록 하는 효과가 있다.

[0023] 또한, 본 발명에 의하면, 랜섬웨어나 맬웨어에 감염된 복원대상 기기에 연결된 복원 기기의 데이터 로그를 통해 복원대상 기기의 특정 데이터 부분을 효과적으로 복원할 수 있다.

[0024] 아울러, 본 발명에 의하면, 복원대상 기기가 랜섬웨어나 맬웨어에 감염된 경우, 복원대상 기기에 결합하는 복원 기기를 이용하여 복원대상 기기의 감염된 디스크 내 소프트웨어 시스템을 복원하여 사물인터넷, 스마트 팩토리 내에서 해당 IoT 기기나 산업제어시스템 기기로서 요구되는 필수 기능을 유지할 수 있도록 하는 효과가 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일실시예에 따른 랜섬웨어 피해 복원을 위한 P2P(pear to pear) 디스크 복원 방법을 구현하는 시스템(이하 간략히 '디스크 복원 장치)의 거시적 IoT 환경 구성을 설명하기 위한 블록도이다.

도 2는 도 1의 디스크 복원 장치에 채용할 수 있는 IoT 기기의 환경 구성을 설명하기 위한 블록도이다.

도 3은 도 2의 IoT 기기와 복원 기기를 예시한 도면이다.

도 4는 도 3의 IoT 기기와 복원 기기의 구성에 대한 개략적인 블록도이다.

도 5 및 도 6은 본 발명의 다른 실시예에 따른 디스크 복원 장치에 대한 작동 원리를 설명하기 위한 구성도들이다.

도 7a 및 도 7b는 도 5의 디스크 복원 장치에 대한 작동 원리를 설명하기 위한 흐름도이다.

도 8은 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제1 구성을 나타낸 블록도이다.

도 9는 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제2 구성을 나타낸 블록도이다.

도 10은 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제3 구성을 나타낸 블록도이다.

도 11은 도 5의 디스크 복원 장치의 복원 관리 서버에 채용할 수 있는 구성을 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 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.

[0027] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0028] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0029] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0031] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0032] 본 실시예의 상세 설명에 앞서, 사물인터넷(internet of thing, IoT)이나 산업제어시스템(industry control system, ICS) 환경을 정의하면, 사물인터넷이나 산업제어시스템 환경은 여러 대의 동일한 기기가 사용되고 있는 환경으로서, 시스템 소프트웨어 혹은 필수 어플리케이션의 복원만으로 기기를 정상 동작하게 만들 수 있는 환경을 가리킨다.

[0033] 또한, 용어 'IoT 기기'는 수동 작업 없이 유선 혹은 무선 네트워크 상에서 신호 혹은 데이터를 수신하고 전송하는 물리적 기기를 지칭하며, 본 실시예서는 사물인터넷이나 산업제어시스템에서 사용되는 센서, 조절 장치, 네트워크 통신 기기, 로봇 팔의 동작 제어기 등을 포함할 수 있다. 그리고 용어 '디스크'는 주저장장치와 혼용하여 사용될 수 있다.

[0034] 도 1은 본 발명의 일실시예에 따른 랜섬웨어 피해 복원을 위한 P2P(pear to pear) 디스크 복원 방법을 구현하는 시스템(이하 간략히 '디스크 복원 장치)의 거시적 IoT 환경 구성을 설명하기 위한 블록도이다. 도 2는 도 1의 디스크 복원 장치에 채용할 수 있는 IoT 기기의 환경 구성을 설명하기 위한 블록도이다.

[0035] 도 1을 참조하면, 본 실시예에 따른 디스크 복원 장치은 복수의 IoT 기기들(10 내지 13 및 20 내지 23)과 복원 관리 서버(100)를 포함한다. 디스크 복원 장치은 동종 기기를 포함한 다수의 IoT 기기들이 존재하는 환경에서 IoT 기기들(10 내지 13 및 20 내지 23)에 연결되는 복원 관리 서버(100)를 통해 램섬웨어 피해나 맬웨어 피해를 당한 IoT 기기내 디스크의 복원 관리를 수행한다.

[0036] 본 실시예에 따른 IoT 기기(10)는 도 2에 도시한 바와 같이 주저장장치(11)를 포함한다. 주저장장치(11)는 시스템 소프트웨어(12)와 데이터(13)를 저장한다. 본 실시예에서 하나의 IoT 기기(10)는 하나의 복원 기기(15)에 연

결되거나 하나의 복원 기기(15)를 포함하도록 구성된다. 복원 기기(15)는 복원 프로그램(16)을 탑재한다. 복원 프로그램(16)은 랜섬웨어나 맬웨어에 감염된 IoT 기기(10)의 디스크를 복원하기 위한 긴급 시스템 소프트웨어의 기능을 포함한다.

[0037] IoT 기기(10)와 복원 기기(15)는 유선 통신이나 무선 통신을 포함한 네트워크를 통해 복원 관리 서버(100)와 신호를 주고받을 수 있다. 본 실시예에서 복원 기기(15)와 복원 관리 서버(100)는 랜섬웨어나 맬웨어에 감염된 IoT 기기(10)의 디스크를 복원하거나 복원 중에 그 기능을 유지하도록 작동한다.

[0038] 좀더 상세히 설명하면, 복원 관리 서버(100)는 IoT 기기들 사이의 P2P(pear to pear) 복원을 중개하는 역할을 한다. 복원 관리 서버(100)는 P2P 복원 과정에서 IoT 기기의 사용을 종료하거나, 복원 기기(15)의 동작을 제어하고, 복원 프로그램(16)을 통해 IoT 기기(10)를 부팅하는 동작을 관리할 수 있다. 즉, 복원 관리 서버(100)는 IoT 기기(10)의 종료 및 재부팅과 복원 기기(15)의 동작을 관리할 수 있다.

[0039] 본 실시예에 의하면, 복원 관리 서버(100)가 P2P 복원 과정에 필요한 IoT 기기들를 제어하나 실제 P2P 복원은 해당 IoT 기기들 사이에서 이루어지므로, 본 실시예의 디스크 복원 장치는 서버가 감염되지 않은 디스크 이미지를 직접 가지고 배포하는 기본 방식에 비해 복원 관리 서버의 부하를 줄일 수 있는 장점이 있다.

[0040] 도 3은 도 2의 IoT 기기와 복원 기기를 예시한 도면이다. 도 4는 도 3의 IoT 기기와 복원 기기의 구성에 대한 개략적인 블록도이다.

[0041] 도 3을 참조하면, 본 실시예에 따른 디스크 복원 장치는 IoT 기기(10)와 복원 기기(15) 및 이들의 연결 수단(14)을 포함한다. IoT 기기(10)는 미노우보드 터봇(MinnowBoard Turbot)으로 구현될 수 있고, 또한 그 변형예에서 미노우보드 터봇과 동일하거나 유사한 기능을 수행하는 수단이나 구성부를 포함하는 장치로 구현될 수 있다.

[0042] 그리고 복원 기기(15)는 라즈베리 파이 제로(Raspberry pi zero)를 사용하여 구현될 수 있고, 또한 라즈베리 파이 제로와 동일하거나 유사한 기능을 수행하는 수단이나 구성부를 포함하는 장치로 구현될 수 있다.

[0043] IoT 기기(10)와 복원 기기(15)는 범용직렬버스(universal serial bus, USB)로 연결될 수 있으나, 이러한 연결 수단(14)은 USB로 한정되는 것은 아니며, 다양한 유선 네트워크의 다른 연결 방식들 중 어느 하나 이상이나 기존의 무선 네트워크의 연결 방식 중 어느 하나 이상을 구현한 수단이나 구성부를 선택하여 사용할 수 있다.

[0044] IoT 기기(10)는 SD 카드(secure digital card)를 주저장장치로 사용할 수 있으며, 그 시스템 소프트웨어로는 우분투 서버(Ubuntu server)를 사용할 수 있다. 여기서, IoT 기기(10)는 스마트 팩토리 등을 위한 산업제어시스템 기기를 포함한다.

[0045] 전술한 IoT 기기(10)와 복원 기기(15)의 쌍은 IoT 환경이나 산업제어시스템 환경에서 다수개가 존재하는 것으로 가정하고, IoT 기기(10)와 복원 기기(15) 각각은 USB 등의 또 다른 연결 수단을 통해 복원 관리 서버에 연결될 수 있다.

[0046] 전술한 디스크 복원 환경에서, 랜섬웨어나 맬웨어 등의 바이러스에 IoT 기기(10)가 감염되면, IoT 기기(10)의 주저장장치에 저장된 내용들은 암화화된다. 특히, 시스템 소프트웨어가 암호화되는 경우, IoT 기기(10)는 부팅이 불가능하게 되고 IoT 기기의 사용이 불가능하게 된다. 따라서 IoT 기기(10)의 복원이 요구된다.

[0047] IoT 기기(10)를 복원한다는 것은 IoT 기기(10)가 그 기능을 수행할 수 있도록 하는 것을 의미한다. 즉, 도 4에 도시한 바와 같이, IoT 기기(10)의 기능을 수행하기 위해서는 시스템 소프트웨어(12) 및 데이터(13) 내 필수 어플리케이션의 복원이 필수적이다.

[0048] IoT 기기(10)가 랜섬웨어나 맬웨어에 의해 감염되면, 복원 관리 서버(100)는 복원 기기(15)를 활성화시키고, IoT 기기(10)의 주저장장치(11)를 통한 부팅이 불가능하기 때문에 복원 기기(15)를 통해 IoT 기기(10)의 복원과 부팅을 진행한다. 복원 기기(15)의 복원 프로그램(16)은 주저장장치(11)의 복원을 위한 긴급 복구 프로그램으로서 기능한다.

[0049] 이 때, 복원 기기(15)는 원격 전원(17)을 구비하며, 이를 토대로 복원 관리 서버(100)는 IoT 기기(10)의 복원이 필요할 때만 해당 복원 기기(15)를 작동시킬 수 있다. 즉, 복원 기기(15)는 IoT 기기(10)의 랜섬웨어 피해를 복원하고자 하는 경우에만 원격 전원(17)을 통해 선택적으로 활성화될 수 있다.

[0050] 위에서 설명한 바와 같이, 본 실시예에 따른 디스크 복원 장치에 채용할 수 있는 시스템 환경은 다음과 같다. 복원 관리 서버가 연결되는 네트워크 내에 동일한 시스템 소프트웨어 등을 가진 동종 IoT 기기들이 존재하며, 이러한 IoT 기기들은 시스템의 핵심적인 기능을 수행하고, 그 기능은 별도로 존재하는 복원 관리 서버와 상호작

용한다.

[0051] 그리고 IoT 기기가 랜섬웨어에 감염되면 해당 IoT 기기는 부팅이 불가능하며 사용할 수 없게 된다. IoT 기기가 본래의 기능을 수행하도록 복원하기 위해서는 해당 IoT 기기의 시스템 소프트웨어의 복원이 필수적이다. 이러한 환경에서 랜섬웨어에 감염된 IoT 기기의 복원을 위하여 본 실시예에 따른 디스크 복원 장치의 복원 기기는 대응되는 한 개의 대상 IoT 기기와 연결되어 있으며, 대상 IoT 기기를 복원하기 위한 복원 프로그램을 구비한다.

[0052] 복원 프로그램은 대상 IoT 기기의 주저장장치의 복원을 위한 긴급 복구 기능을 수행한다. 복원 기기는 원격 전원을 통해 복원이 필요할 때만 작동할 수 있다. 복원 기기에는 대상 IoT 기기의 기능 유지를 위한 프로그램과 데이터 복원을 위한 로그 프로그램, 독립 저장 장치가 구비될 수 있다.

[0053] 복원 관리 서버는 IoT 기기 및 복원 기기와 각각 통신하며, 복원 기능을 지원한다. 랜섬웨어에 감염된 IoT 기기는 작동이 불가능하므로, 감염됨 IoT 기기를 작동하기 위해 복원 관리 서버는 랜섬웨어에 감염된 IoT 기기에 연결되고 복원 소프트웨어를 탑재한 복원 기기를 활성화시킨다. 복원 기기는 랜섬웨어의 감염 전에 IoT 기기에 물리적으로 연결되어 있는 상태일 수 있다. 복원 기기는 감염된 IoT 기기의 피해 디스크에 접근할 수 있도록 설치되어 있으므로, 감염되지 않은 다른 IoT 기기의 디스크 내용을 복제하여 감염된 IoT 기기의 디스크에 저장하도록 동작할 수 있다. 이와 같이, 본 실시예에 의하면, 감염 디스크의 피해를 복원하고 올바른 동작을 재개할 수 있다.

[0054] 만약 복제의 원천이 되는 IoT 기기가 작동할 때 해당 IoT 기기의 디스크 내용을 수정하는 시스템이라면, 복제 원천이 되는 IoT 기기를 종료하고 감염 디스크의 피해를 복원할 수 있다.

[0055] 이 때 복원 기기를 이용하여 사물인터넷, 스마트 팩토리에서 끊어지면 안되는 IoT 기기의 본래 기능을 수행할 수 있다. 이를 위해, 디스크 복원 장치는 데이터의 로그(log) 및 복원을 이용하여 랜섬웨어 피해를 복원할 때 시스템 소프트웨어나 필수 어플리케이션뿐만 아니라 이러한 프로그램으로 인해 생성된 데이터들도 복원하도록 구현될 수 있다.

[0056] 도 5 및 도 6은 본 발명의 다른 실시예에 따른 디스크 복원 장치에 대한 작동 원리를 설명하기 위한 구성도들이다. 그리고 도 7a 및 도 7b는 도 5의 디스크 복원 장치에 대한 작동 원리를 설명하기 위한 흐름도이다.

[0057] 도 5 내지 도 7a 및 도 7b를 참조하면, 본 실시예에 따른 디스크 복원 방법에 있어서, 복원 관리 서버(100)는 IoT 센서나 관리자 입력 등에 의해 제1 IoT 기기(10)의 랜섬웨어 피해를 감지할 수 있다(S71). 제1 IoT 기기(10)에 대한 랜섬웨어 피해가 발생하면, 복원 관리 서버(100)는 제1 트리거 신호나 제1 제어 신호를 전송하여 제1 IoT 기기(10)에 연결되어 있는 제1 복원 기기(15a)를 작동시킨다(S72). 제1 복원 기기(15a)는 제1 제어 신호에 응하여 복원 프로그램을 작동시킬 수 있다(S72a).

[0058] 다음, 제1 복원 기기(15a)는 제1 제어 신호에 응하여 복원 프로그램(16)을 통해 IoT 환경이나 산업제어시스템 환경 내에 랜섬웨어의 피해 없이 온전하게 작동 중인 동종의 IoT 기기에 대한 탐색을 복원 관리 서버(100)에 요청한다(S73). 그리고 제1 복원 기기(15a)는 제1 제어 신호에 응하여 미리 저장된 제어 모듈을 통해 제1 IoT 기기(10)의 시스템 소프트웨어의 기능을 수행한다(S76c 참조).

[0059] 다음, 복원 관리 서버(100)는 동종 IoT 기기 탐색에 대한 제1 요청 메시지에 포함된 특정 종류의 IoT 기기가 현재 연결된 네트워크인 IoT 환경이나 산업제어시스템 환경 내에 존재하는지를 탐색한다(S74). 탐색은 네트워크로 연결되어 있는 IoT 기기들에 소정의 핑(ping) 신호 등의 미리 설정된 동작 체크 신호를 전송하고 그에 대한 피드백을 받음으로써 수행될 수 있다.

[0060] 다음, 제2 IoT 기기(20)가 정상 작동 중인 동종 IoT 기기로 탐색되면, 복원 관리 서버(100)는 제2 트리거 신호나 제2 제어 신호를 통해 탐색된 제2 IoT 기기(20)의 제2 복원 기기(15b)를 작동시킨다(S75).

[0061] 이 때, 제2 복원 기기(15b)의 작동이 제2 IoT 기기(20)의 주저장장치(11)에 저장된 시스템 소프트웨어(12)를 변경하도록 설정되어 있는 경우, 제2 트리거 신호나 제2 제어 신호는 제2 IoT 기기(20)를 우선 종료하도록 하는 메시지나 명령을 포함할 수 있다. 물론 변형예에서, 복원 관리 서버(100)는 탐색된 제2 IoT 기기(20)의 작동을 중지시키는 별도의 신호나 명령을 전달하여 먼저 제2 IoT 기기(20)의 시스템 소프트웨어(12)를 종료시킬 수 있다. 그런 다음, 제2 IoT 기기(20)는 제2 복원 기기(15b)의 활성화 상태에서 다시 부팅되어 정상 동작할 수 있다.

[0062] 다음, 제2 복원 기기(15b)는 제2 제어 신호에 응하여 제2 IoT 기기(20)에 미리 설정된 제3 제어 신호나 그에 대응하는 명령을 전달(S76a)함으로써 제2 IoT 기기(20)가 주저장장치(11)에 저장된 내용을 미리 설정된 네트워크

경로(30)를 통해 제1 IoT 기기(10)으로 전송(S76b)하도록 기능한다. 이때, 제1 복원 기기(15a)의 복원 프로그램은 제1 IoT 기기(10)의 제어 모듈로서 제2 IoT 기기(20)의 주저장장치(11)의 내용을 수신하고, 수신한 내용을 제1 IoT 기기(10)의 주저장장치(11)에 덮어쓰기 하도록 기능한다(S76c).

[0063] 다음, 제1 IoT 기기(10)의 주저장장치(11)에 제2 IoT 기기(20)의 주저장장치(11)의 내용이 모두 덮어씌워지면(S77a), 제1 복원 기기(15a)는 제1 IoT 기기(10)를 재부팅한다(S77b). 이 때, 제1 IoT 기기(10)의 재부팅은 제1 IoT 기기(10)의 복원된 주저장장치(11)을 이용하여 부팅한다.

[0064] 본 실시예에 의하면, 제2 IoT 기기(20)과 제1 IoT 기기(12) 간의 P2P 디스크 복원을 통해 랜섬웨어에 감염된 제1 IoT 기기(10)의 디스크를 복원하여 자체 부팅할 수 있다.

[0065] 아울러, 제1 복원 기기(15a)는 제1 IoT 기기(10)의 복원된 디스크 내용 중 미리 설정된 일부 데이터 부분을 삭제하도록 설정될 수 있다. 또한, 제1 복원 기기(15a)는 랜섬웨어에 감염되기 전에 제1 IoT 기기(10)로부터 받아 저장하고 있던 일부 데이터를 사용하여 제1 IoT 기기(10)의 복원된 디스크의 내용 일부를 초기화하도록 구현될 수 있다. 그 경우, 제1 복원 기기(15a)는 제1 IoT 기기(10)의 데이터 내용을 별도로 로깅해 두기 위한 데이터 로그 프로그램과 일부 데이터 내용을 저장하는 별도의 독립된 저장 공간을 구비할 수 있다.

[0066] 다음, 제1 IoT 기기(10)의 재부팅 및 데이터 초기화가 완료되면(S78a), 복원 관리 서버(100)는 작동종료신호 등을 전달(S78b)하여 제1 복원 기기(15a)와 제2 복원 기기(15b)의 작동을 종료할 수 있다(S79a, S79b). 제1 IoT 기기(10)의 재부팅 및 데이터 초기화의 완료는 제1 IoT 기기(10)에서 전달되는 신호나 데이터에 기초하여 복원 관리 서버(100)가 제1 IoT 기기의 정상 동작을 감지하는 것으로 구현될 수 있다.

[0067] 도 8은 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제1 구성을 나타낸 블록도이다. 그리고 도 9는 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제2 구성을 나타낸 블록도이다.

[0068] 도 8을 참조하면, 본 실시예에 따른 디스크 복원 장치의 복원 기기(15)는 복원 프로그램(16), 원격 전원(17) 및 기능 유지 프로그램(18)을 탑재한다.

[0069] 복원 프로그램(16)은 복원 기기의 기본 구성요소로서 대응 IoT 기기가 랜섬웨어에 감염되었을 때 대응 IoT 기기의 디스크를 복원하기 위한 것이다.

[0070] 원격 전원(17)은 복원 프로그램(16)이 대응 IoT 기기의 랜섬웨어 감염 상황에서 복원 기기(15)의 선택적 부팅에 사용하기 위한 것이다. 즉, 원격 전원(17)은 복원 프로그램(16)이 파일 시스템으로 포맷되어야 할 때 대응 IoT 기기의 랜섬웨어 감염시 복원 기기(15)도 랜섬웨어의 피해에 노출되지 않도록 필요한 경우에만 복원 기기(15)나 복원 프로그램(16)을 선택적으로 기동시켜 사용할 수 있도록 기능한다.

[0071] 기능 유지 프로그램(18)은 복원 기기(15)의 복원 프로그램(16) 내부에 탑재된다. 기능 유지 프로그램(18)은 스마트 팩토리 등의 IoT 기기와 같이 IoT 기기의 지속적인 작동을 필요로 하는 경우에 대응 IoT 기기가 부팅되는 시간 동안 대응 IoT 기기의 필수적인 기능을 수행할 수 있다. 필수적인 기능은 예를 들어 센서 측정, 네트워크 통신, 로봇 팔의 동작 등을 포함할 수 있다.

[0072] 한편, 기능 유지 프로그램(18)은 도 9에 도시한 바와 같이 복원 기기(15)의 복원 프로그램(16) 내부에 탑재되지 않고 별도의 소프트웨어(16a)에 복원 프로그램(16)과 함께 탑재될 수 있다.

[0073] 이러한 기능 유지 프로그램(18)은 랜섬웨어에 감염된 IoT 기기나 감염됨 IoT 기기에 디스크 내용을 복사하여 전달하는 정상 동작 IoT 기기에 모두 사용될 수 있다.

[0074] 예를 들어, 실제 동작하고 있고 IoT 기기의 디스크를 복사의 소스(source)로 사용할 때, IoT 기기의 작동이 시스템 소프트웨어 영역을 덮어쓰는 경우와 단순 복사하는 경우가 존재할 수 있다.

[0075] 시스템 소프트웨어 영역을 덮어쓰는 경우, 본 실시예에서는 해당 IoT 기기를 종료하여 덮어쓰기가 발생하지 못하게 하고, 복원 기기를 통해 디스크 복사를 수행하도록 구현된다.

[0076] 그리고, 디스크 복사 과정에서 IoT 기기의 종료가 필요한 이유는 디스크 복사 도중에 즉, 복사의 시작 시점과 복사의 종료 시점에 소스 디크스의 내용이 동일하게 유지되도록, 다시 말해서 소스 디스크의 내용 특히 시스템 소프트웨어의 변동사항이 없도록 하기 위함이다. 디스크 내용 복사는 IoT 기기의 성능과 통신의 성능에 따라 소요 시간이 다르며, 그러한 이유로 복사 도중에 시스템 소프트웨어 부분이 변경된다면, 변경된 부분의 무결성(integrity)가 손상되고, 그에 의해 복사된 시스템 소프트웨어가 해당 IoT 기기에서 정상 기능을 제공하지 않을 수 있다. 따라서, 이러한 문제를 방지하기 위해 시스템 소프트웨어를 포함한 디스크 복사 시에 IoT 기기의 종료

를 선택할 수 있다.

[0077] 도 10은 도 5의 디스크 복원 장치의 복원 기기에 채용할 수 있는 또 다른 제3 구성을 나타낸 블록도이다.

[0078] 도 10을 참조하면, 본 실시예에 따른 디스크 복원 장치의 복원 기기(15)는 복원 프로그램(16), 원격 전원(17), 기능 유지 프로그램(18), 데이터 로그 프로그램(19a) 및 저장 공간(19b)을 구비한다. 복원 프로그램(16), 기능 유지 프로그램(18) 및 데이터 로그 프로그램(19a)은 별도의 소프트웨어(16b)에 함께 탑재될 수 있다.

[0079] 데이터 로그 프로그램(19a)은 IoT 기기의 데이터 부분 내용이 수정될 때, 해당 수정 오퍼레이션에 대한 내용을 로그(log)로 남길 수 있다. 이러한 로그는 복원 기기(15) 내부의 별도의 저장 공간(19b)에 저장된다. 즉, 본 실시예에서 로그는 하드웨어 레벨로 저장된다. 그리고 저장된 로그는 복원 기기(15)의 독립된 저장 공간(19b)에 저장되므로 IoT 기기에서는 볼 수 없게 된다.

[0080] 이와 같이, 본 실시예에서는 데이터 로그 프로그램(19a)을 지원함으로써 복원 대상이 되는 IoT 기기의 데이터까지 복원할 수 있다.

[0081] 또한, IoT 기기의 시스템 소프트웨어 복원 후에, 복원 기기(15)는 독립된 저장 공간(19b)에서 데이터 수정 로그를 불러와 재실행하는 방식으로 IoT 기기의 데이터를 복원할 수 있다.

[0082] 또한, 복원 기기(15)에서 복원 프로그램(16), 기능 유지 프로그램(18), 데이터 로그 프로그램(19a) 등의 다양한 기능을 제공하는 경우, 본 실시예의 복원 관리 서버나 복원 기기를 포함하는 디스크 복원 장치에서는 복원 기기에 탑재된 기능성 프로그램의 실행 유무를 선택적으로 결정하거나 필요시 선택적으로 기동시키도록 구성함으로써 랜섬웨어에 의해 복원 프로그램 등의 기능성 프로그램이 감염되는 것을 방지할 수 있다. 예를 들어, IoT 기기의 데이터 부분을 로그(log)로 남길 때, 데이터 로그 프로그램만을 실행하면, IoT 기기에서 복원 프로그램이 보이지 않아 IoT 기기의 랜섬웨어의 감염시에 복원 기기의 프로그램이 함께 감염되는 것을 방지할 수 있다.

[0083] 도 11은 도 5의 디스크 복원 장치의 복원 관리 서버에 채용할 수 있는 구성을 나타낸 블록도이다.

[0084] 도 11을 참조하면, 본 실시예에 따른 복원 관리 서버(100)는 감지부(110), 제어신호 생성부(120), 메시지 처리부(130) 및 탐색부(140)를 포함한다.

[0085] 복원 관리 서버(100)는 감지부(110)에 의해 네트워크 내 제1 IoT 기기가 랜섬웨어 또는 맬웨어에 의해 감염된 것을 감지하고, 감지부(110)에 연결된 제어신호 생성부(120)를 통해 제1 IoT 기기에 연결된 제1 복원 기기에 전송할 제1 제어 신호를 생성한다.

[0086] 또한, 복원 관리 서버(100)는 메시지 처리부(130)를 통해 제1 복원 기기로부터 제1 IoT 기기와 동종의 제2 IoT 기기에 대한 탐색 요청을 받고, 탐색 요청에 포함된 제1 IoT 기기의 기기 정보를 추출한다.

[0087] 그리고, 복원 관리 서버(100)는 제1 IoT 기기의 기기 정보에 기초하여 탐색부(140)를 통해 네트워크 내에 존재하는 제2 IoT 기기를 탐색한다.

[0088] 제2 IoT 기기가 탐색되면, 복원 관리 서버(100)는 제어신호 생성부(120)를 통해 제2 제어 신호를 생성하고, 제2 제어 신호를 제2 IoT 기기에 연결되어 있는 제2 복원 기기에 전달한다. 이 때, 제2 복원 기기는 제2 제어 신호에 응하여 제2 IoT 기기의 동작을 제어함으로써 제2 IoT 기기가 주저장장치의 내용을 복사하여 제1 IoT 기기의 주저장장치를 덮어쓰기할 수 있도록 한다.

[0089] 제1 IoT 기기의 주저장장치의 덮어쓰기 및 재부팅에 의해 제1 IoT 기기의 복원이 완료되면, 복원 관리 서버는 네트워크 상에서 제1 IoT 기기의 정상 상태를 감지하고, 그에 따라 제어신호 생성부(120)를 통해 상기 제1 복원 기기 및 상기 제2 복원 기기의 작동을 종료하기 위한 제어신호나 작동종료신호를 생성할 수 있다.

[0090] 전술한 실시예에 의하면, 랜섬웨어, 맬웨어 등으로 인해 사물인터넷이나 산업제어시스템 환경 내의 IoT 기기의 디스크 내용이 손상되었을 때, 실제 작동하고 있는 다른 동종 IoT 기기의 디스크 내용을 복사하여 손상된 디스크 내용을 효과적으로 복원하여 해당 IoT 기기가 신속하게 복구되어 정상작동할 수 있도록 한다.

[0091] 한편, 전술한 실시예들을 통해 설명한 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 방법은 다양한 컴퓨터 수단을 통해 수행될 수 있는 모듈이나 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 모듈은 하드웨어, 소프트웨어, 펌웨어(firmware) 또는 이들의 조합을 포함하는 유닛을 의미할 수 있다. 유닛은 예를 들어 로직(logic), 논리 블록(logical block), 부품(component) 또는 회로(circuit) 등으로 지칭될 수 있으며, 본 실시예에 따른 방법을 위한 일련의 동작을 수행하는 ASIC(application-specific integrated circuit)

칩, FPGA(field-programmable gate arrays) 및 프로그램 가능 논리 장치(programmable-logic device) 중 적어도 어느 하나를 포함할 수 있다.

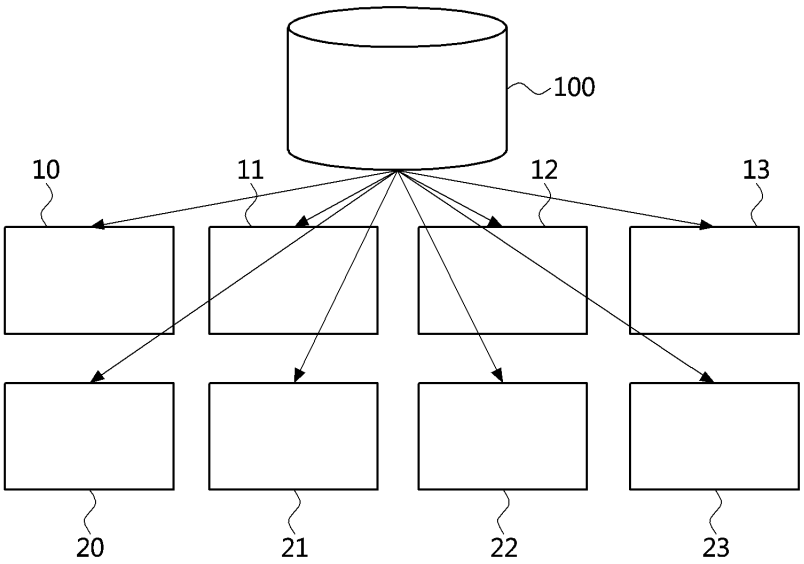
[0092] 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 본 발명을 위해 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용가능한 것일 수 있다.

[0093] 또한 컴퓨터 판독 가능 매체의 예에는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함한다. 상술한 하드웨어 장치는 본 실시예에 따른 랜섬웨어 피해 복원을 위한 P2P 디스크 복원 방법의 일련의 동작을 수행하기 위해 적어도 하나의 소프트웨어 모듈로 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

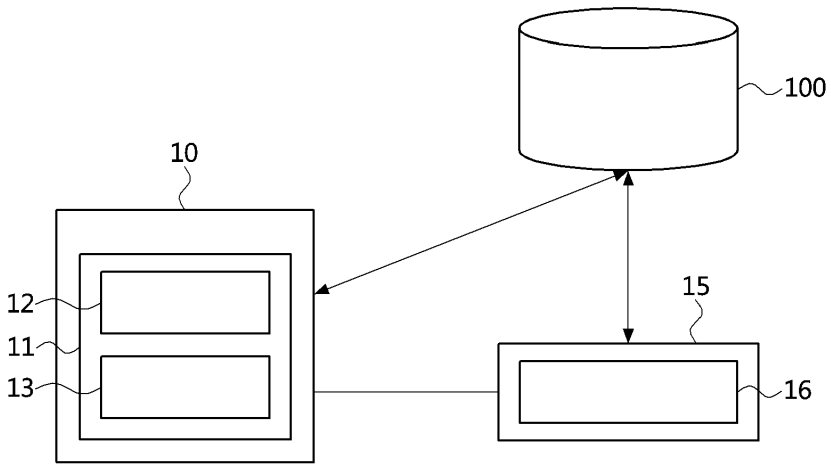
[0094] 이상 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

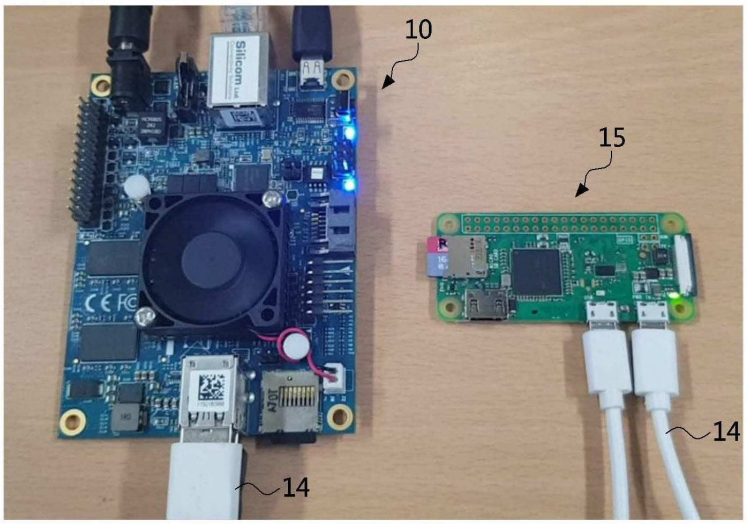
도면1



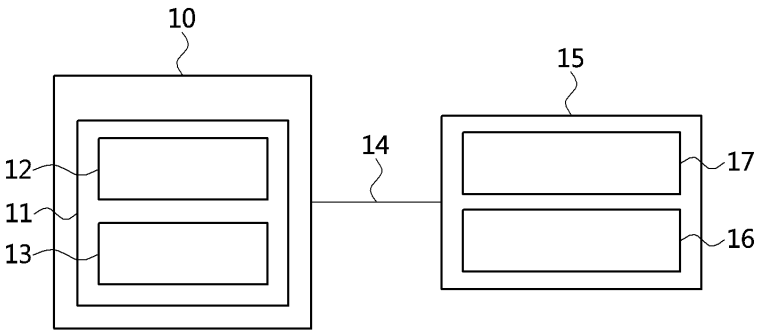
도면2



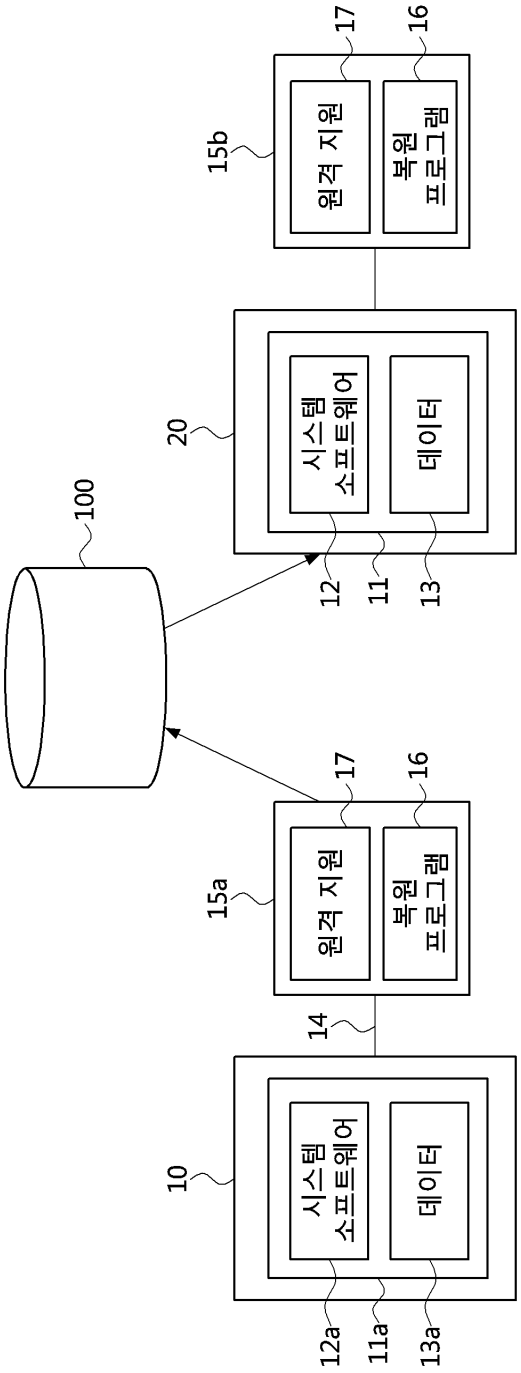
도면3



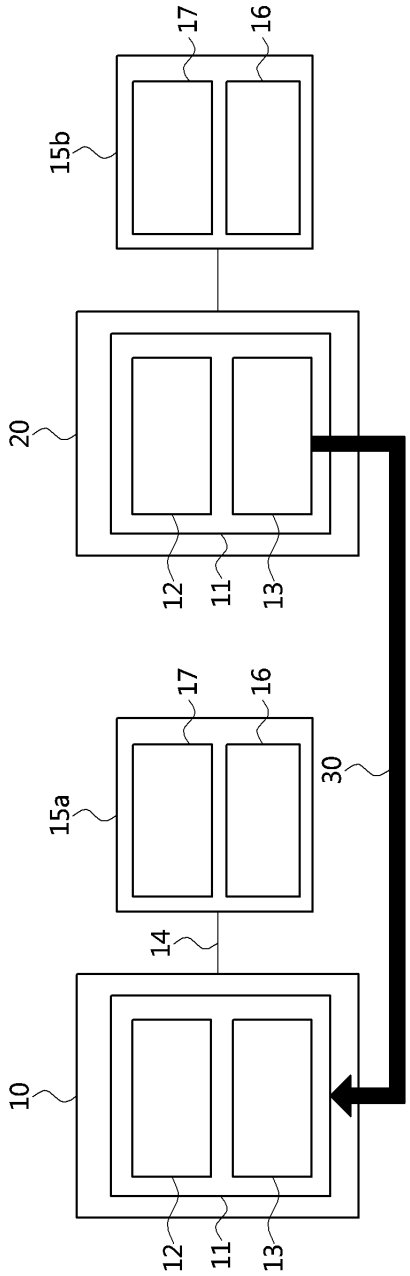
도면4



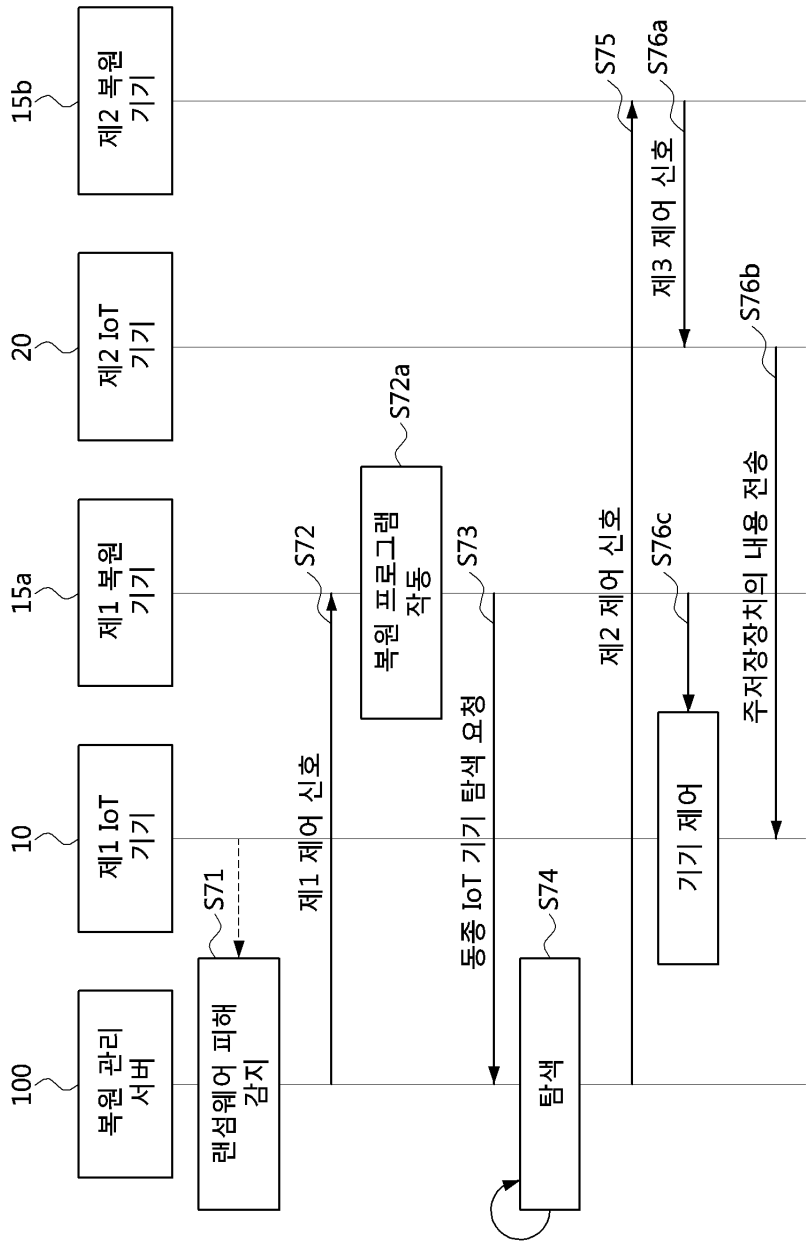
도면5


100
10
시스템 소프트웨어
데이터
12a
11a
13a
14
15a
원격 지원
복원 프로그램
17
16
20
시스템 소프트웨어
데이터
12
11
13
15b
원격 지원
복원 프로그램
17
16

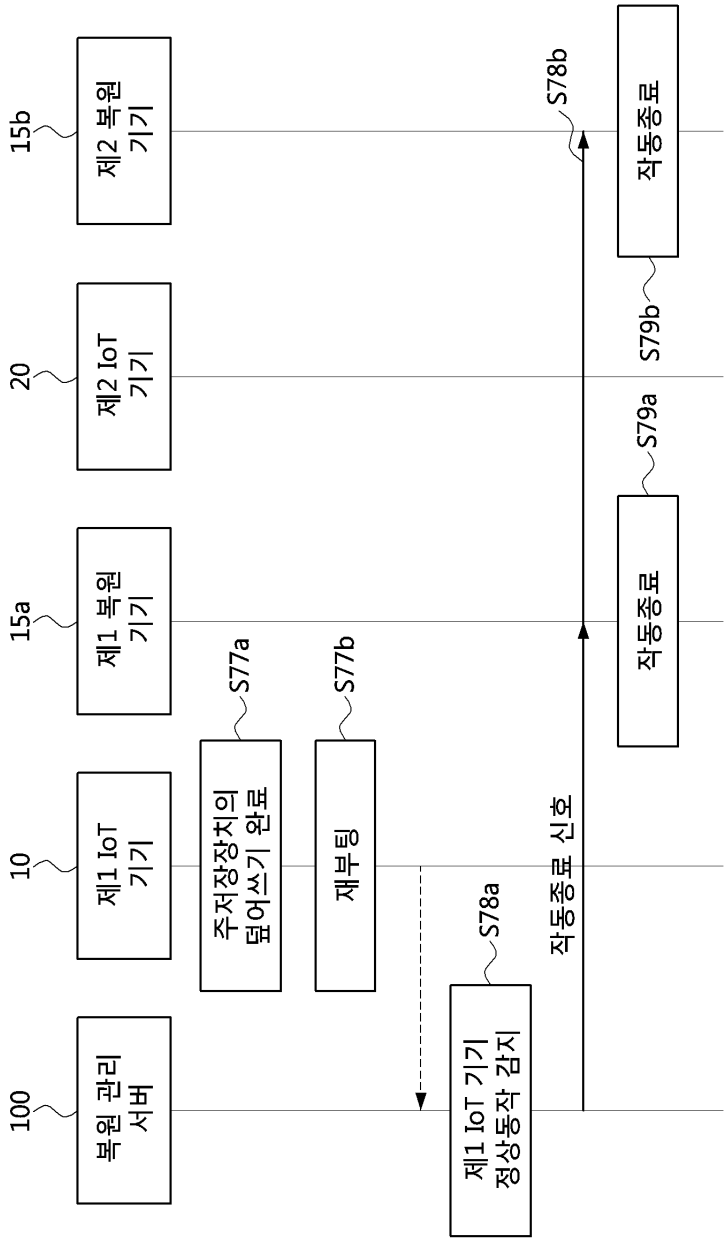
도면6



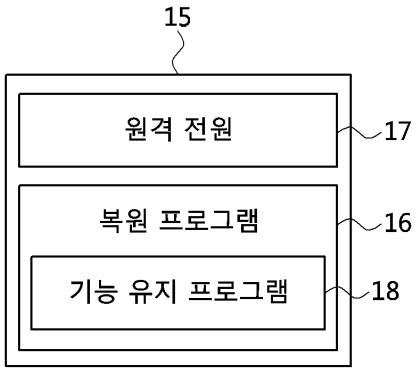
도면7a


100
복원 관리 서버
10
제1 IoT 기기
15a
제1 복원 기기
20
제2 IoT 기기
15b
제2 복원 기기
랜섬웨어 피해 감지
S71
제1 제어 신호
S72
복원 프로그램 작동
S72a
동종 IoT 기기 탐색 요청
S73
탐색
S74
제2 제어 신호
S75
제3 제어 신호
S76a
기기 제어
S76c
주저장장치의 내용 전송
S76b

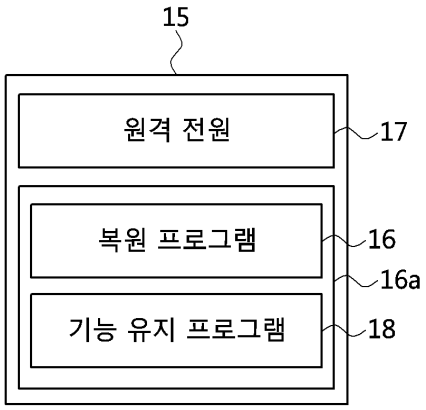
도면7b


15b
제2 복원 기기
20
제2 IoT 기기
15a
제1 복원 기기
10
제1 IoT 기기
100
복원 관리 서버
S77a
주저장장치의 덮어쓰기 완료
S77b
재부팅
S78a
제1 IoT 기기 정상동작 감지
작동종료 신호
S78b
작동종료
S79b
S79a
작동종료

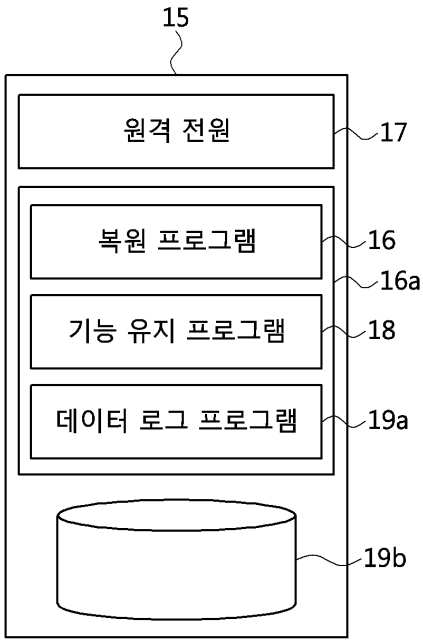
도면8


15
원격 전원
17
복원 프로그램
16
기능 유지 프로그램
18

도면9



도면10



도면11