(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년11월26일
(11) 등록번호 10-2331885
(24) 등록일자 2021년11월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/55 (2013.01) *G06F 21/56* (2013.01)
G06F 21/71 (2013.01)
(52) CPC특허분류
G06F 21/556 (2013.01)
G06F 21/56 (2013.01)
(21) 출원번호 10-2020-0020452
(22) 출원일자 2020년02월19일
심사청구일자 2020년02월19일
(65) 공개번호 10-2021-0105678
(43) 공개일자 2021년08월27일
(56) 선행기술조사문헌
KR1020110066700 A*
KR1020130118335 A*
Colin O'Flynn, "A Framework for Embedded Hardware Security Analysis"(2017.06.)
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
박기웅
서울특별시 광진구 능동로17길 21, 304호(화양동)
정혜림
서울특별시 동작구 사당로16사길 37, B01호 (사당동)
안성규
서울특별시 광진구 동일로56다길 3, B02호(군자동)
(74) 대리인
양성보

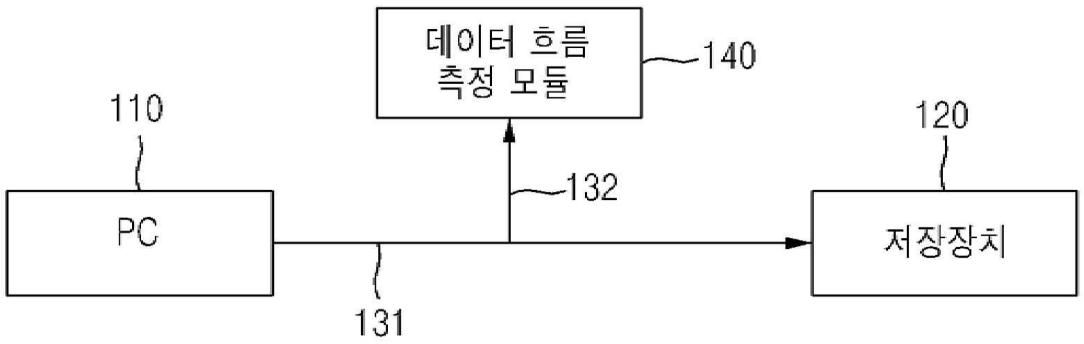
전체 청구항 수 : 총 6 항 심사관 : 정성훈

(54) 발명의 명칭 **커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법 및 이를 위한 매체**

(57) 요 약

커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법 및 장치가 제시된다. 본 발명에서 제안하는 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법은 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 데이터 흐름 측정 모듈을 통해 측정하는 단계, 데이터 흐름 측정 모듈을 통해 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의 커패시터에 입력되어 커패시터의 충전량이 변동되는 단계, 해당 커패시터들의 충전량을 측정하는 단계 및 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/71 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711093714
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 IoT 기반 이식-침습형 고위험 의료장치를 위한 능동형 킬 스위치 및 바이오 마커 활용 방어 시스템 개발
기 여 율 1/1
과제수행기관명 국민대학교산학협력단
연구기간 2019.04.01 ~ 2022.12.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

커패시터 모듈, 커패시터 충전량 측정 모듈, 표준편차 측정 모듈 및 타이머를 포함하는 데이터 흐름 측정 모듈의 비정상 데이터 흐름 검출 방법에 있어서,

외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 데이터 흐름 측정 모듈을 통해 측정하는 단계;

데이터 흐름 측정 모듈을 통해 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의 커패시터 모듈에 입력되어 커패시터 모듈 내 커패시터들의 충전량이 변동되는 단계;

해당 커패시터들의 충전량을 측정하는 단계; 및

측정된 커패시터들의 충전량을 이용하여 데이터 규칙성을 연산하는 단계

를 포함하고,

데이터 흐름을 측정하기 위한 복수의 데이터 채널에서 발생하는 미세전류를 데이터 흐름 측정 모듈의 커패시터 모듈에 입력하여 커패시터들의 충전량을 변동시키고,

상기 타이머에서 발생하는 타이밍에 따라 커패시터 충전량 측정 모듈에서 커패시터들의 충전량을 측정하며,

측정된 각 커패시터의 충전량의 표준편차를 표준편차 측정 모듈을 통해 연산하여 각각의 데이터가 어떠한 전류 패턴을 가지고 있는지 측정하고,

저장장치로의 규칙적인 데이터 입출력 과정에서 발생하는 미세전류를 이용하여, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터들의 충전량의 규칙성과 비례하는 데이터의 규칙성을 측정하는

비정상 데이터 흐름 검출 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서,

측정된 데이터의 규칙성을 통해 정상적인 파일, 정상적인 데이터의 입력 및 비정상 데이터의 입력 흐름을 구분하는

비정상 데이터 흐름 검출 방법.

청구항 5

제1항에 있어서,

측정된 커패시터들의 충전량을 이용하여 데이터 규칙성을 연산하는 단계는,

커패시터 모듈 내 커패시터들 중 충전량의 불규칙성이 미리 정해진 기준 보다 낮은 커패시터의 경우, 해당 커패시터는 랜섬웨어 감염을 포함하는 악성행위 또는 비정상 데이터 흐름이 발생하지 않은 것으로 판단하고, 충전량의 불규칙성이 미리 정해진 기준보다 높은 커패시터의 경우, 해당 커패시터는 암호화의 특징으로 인해 랜섬웨어

를 포함하는 악성행위 또는 비정상 데이터 흐름으로 저장장치의 데이터가 변화되는 것으로 판단하는

비정상 데이터 흐름 검출 방법.

청구항 6

외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 측정하는 데이터 흐름 측정 모듈

을 포함하고,

데이터 흐름 측정 모듈은,

측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 입력되어 충전량이 변동되는 복수의 커패시터들을 포함하는 커패시터 모듈;

해당 커패시터들의 충전량을 측정하는 커패시터 충전량 측정 모듈; 및

측정된 커패시터들의 충전량을 이용하여 데이터 규칙성을 연산하는 표준편차 측정 모듈

을 포함하고,

데이터 흐름을 측정하기 위한 복수의 데이터 채널에서 발생하는 미세전류를 데이터 흐름 측정 모듈의 커패시터 모듈에 입력하여 커패시터들의 충전량을 변동시키고,

데이터 흐름 측정 모듈의 타이머에서 발생하는 타이밍에 따라 커패시터 충전량 측정 모듈에서 커패시터들의 충전량을 측정하며,

측정된 각 커패시터의 충전량의 표준편차를 표준편차 측정 모듈을 통해 연산하여 각각의 데이터가 어떠한 전류 패턴을 가지고 있는지 측정하고,

저장장치로의 규칙적인 데이터 입출력 과정에서 발생하는 미세전류를 이용하여, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터들의 충전량의 규칙성과 비례하는 데이터의 규칙성을 측정하는

비정상 데이터 흐름 검출 장치.

청구항 7

삭제

청구항 8

삭제

청구항 9

제6항에 있어서,

측정된 데이터의 규칙성을 통해 정상적인 파일, 정상적인 데이터의 입력 및 비정상 데이터의 입력 흐름을 구분하는

비정상 데이터 흐름 검출 장치.

청구항 10

제6항에 있어서,

표준편차 측정 모듈은,

커패시터 모듈 내 커패시터들 중 충전량의 불규칙성이 미리 정해진 기준 보다 낮은 커패시터의 경우, 해당 커패시터는 랜섬웨어 감염을 포함하는 악성행위 또는 비정상 데이터 흐름이 발생하지 않은 것으로 판단하고, 충전량의 불규칙성이 미리 정해진 기준보다 높은 커패시터의 경우, 해당 커패시터는 암호화의 특징으로 인해 랜섬웨어를 포함하는 악성행위 또는 비정상 데이터 흐름으로 저장장치의 데이터가 변화되는 것으로 판단하는

비정상 데이터 흐름 검출 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 규칙성을 갖는 데이터 흐름에서 비정상적인 데이터 흐름을 탐지하기 위한 방법을 제시하는 발명으로 비정상적인 데이터 흐름의 예로 랜섬웨어를 들 수 있다.

[0003] 랜섬웨어는 컴퓨터에 잠입하여 사용자 저장장치에 저장된 문서들에 대해 암호화를 수행하여 사용자에게 금전 지불을 요구하고 그때 이를 해독해주는 악성 프로그램이다.

[0004] 커패시터는 하드웨어 소자로 회로에 흐르는 전류를 보완하는 기능으로 쓰이며 회로에 전류를 많을 경우 해당 소자에 충전하거나 회로에 전류가 부족한 경우 회로에 전류를 보충하는 기능을 수행한다.

[0005] 비정상 데이터 흐름이나 랜섬웨어를 탐지하고 이로 인한 불이익을 막기 위한 소프트웨어적 랜섬웨어 및 비정상 데이터 흐름 탐지 기술의 연구 및 발명도 진행되었지만, 랜섬웨어는 이를 회피하기 위해 진화되고 있다.

발명의 내용

해결하려는 과제

[0006] 규칙성을 갖는 데이터 흐름에서 비정상적인 데이터 흐름을 탐지하기 위한 방법을 제시하는 발명으로 비정상적인 데이터 흐름의 예로 랜섬웨어를 들 수 있다.

[0007] 랜섬웨어는 컴퓨터에 잠입하여 사용자 저장장치에 저장된 문서들에 대해 암호화를 수행하여 사용자에게 금전 지불을 요구하고 그때 이를 해독해주는 악성 프로그램이다.

[0008] 커패시터는 하드웨어 소자로 회로에 흐르는 전류를 보완하는 기능으로 쓰이며 회로에 전류를 많을 경우 해당 소자에 충전하거나 회로에 전류가 부족한 경우 회로에 전류를 보충하는 기능을 수행한다.

[0009] 비정상 데이터 흐름이나 랜섬웨어를 탐지하고 이로 인한 불이익을 막기 위한 소프트웨어적 랜섬웨어 및 비정상 데이터 흐름 탐지 기술의 연구 및 발명도 진행되었지만, 랜섬웨어는 이를 회피하기 위해 진화되고 있다.

과제의 해결 수단

[0010] 일 측면에 있어서, 본 발명에서 제안하는 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법은 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 데이터흐름 측정 모듈을 통해 측정하는 단계, 데이터 흐름 측정 모듈을 통해 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의 커패시터에 입력되어 커패시터의 충전량이 변동되는 단계, 해당 커패시터들의 충전량을 측정하는 단계 및 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 단계를 포함한다.

[0011] 복수의 데이터 채널에서 발생하는 전류를 데이터 흐름 측정 모듈의 커패시터에 입력하고 각 커패시터의 충전량의 표준편차를 연산하여 각각의 데이터가 어떠한 전류 패턴을 가지고 있는지 측정한다.

[0012] 저장장치로의 규칙적인 데이터 입출력 과정에서 발생하는 미세전류를 이용하여, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터의 충전량의 규칙성과 비례하는 데이터의 규칙성을 측정한다.

[0013] 측정된 데이터의 규칙성을 통해 정상적인 파일, 정상적인 데이터의 입력 및 비정상 데이터의 입력 흐름을 구분한다.

[0014] 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 단계는 커패시터의 충전량의 불규칙성이 미리 정해진 기준 보다 낮은 경우, 랜섬웨어 감염을 포함하는 악성행위 또는 비정상 데이터 흐름이 발생하지 않은 것

으로 판단하고, 커패시터의 충전량의 불규칙성이 미리 정해진 기준보다 높은 경우, 암호화의 특징으로 인해 랜섬웨어를 포함하는 악성행위 또는 비정상 데이터 흐름으로 저장장치의 데이터가 변화되는 것으로 판단한다.

[0015] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 장치는 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 측정하는 데이터 흐름 측정 모듈을 포함하고, 데이터 흐름 측정 모듈은 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 입력되어 충전량이 변동되는 커패시터 모듈, 해당 커패시터들의 충전량을 측정하는 커패시터 충전량 측정 모듈 및 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 표준편차 측정 모듈을 포함한다.

발명의 효과

[0016] 본 발명의 실시예들에 따르면 데이터 채널에서 발생하는 미세전류를 이용하여 커패시터를 통한 데이터 흐름의 규칙성을 판단하고 데이터 흐름이 불규칙하거나 비정상적일 경우를 탐지할 수 있어 랜섬웨어와 같은 암호화 공격에 대비할 수 있으며, 상기 저장장치에 있는 데이터를 보호할 수 있는 효과가 있다. 또한, 본 발명의 실시예에 따라 데이터 흐름 측정 모듈은 하드웨어 방식으로 구성되어 있어 소프트웨어 탐지 방법을 회피하는 악성행위를 근본적으로 차단할 수 있어 저장매체에 대한 보안이 향상되는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법이 적용되는 환경을 나타낸다.

도 2는 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름을 검출하기 위한 데이터 흐름 측정 모듈의 내부 구성을 나타낸다.

도 4는 본 발명의 일 실시예에 따른 정상적인 데이터 흐름이 수행될 때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

도 5는 본 발명의 일 실시예에 따른 비정상적인 데이터 흐름이 수행될 때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

도 6은 본 발명의 일 실시예에 따른 비정상적인 데이터 흐름 구분을 위한 매체의 구조를 나타낸다.

도 7은 본 발명의 일 실시예에 따른 정상적인 파일과 비정상적인 파일의 흐름을 비교하는 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법이 적용되는 환경을 나타낸다.

[0021] 본 발명에서는 저장장치에 흐르는 전류의 양으로 소자에 충전되는 전류양을 판단하여 데이터 흐름의 비정상 여부를 탐지하는 방법을 제안한다.

[0022] 도 1을 참조하면, 본 발명의 실시 예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 장치는 저장장치(120)로 데이터를 저장하기 위해 데이터 쓰기 연산을 수행하는 PC(110)와 데이터가 전송되는 데이터 채널(131), 데이터 저장장치(120), 데이터 채널(131)로부터 데이터를 측정할 부가적 채널(132), 데이터 흐름 측정모듈(140)을 포함하는 환경에서 적용된다.

[0023] 본 발명은 데이터 쓰기 연산을 수행하는 PC(다시 말해, 외부장치)(110)로부터 하드웨어 저장장치의 데이터 입출력을 수행하는 데이터 채널(131)에 데이터 흐름 측정모듈(140)을 부착하여 저장장치(120)에 기록되기 위한 데이터의 흐름을 커패시터 충전량으로 구분할 수 있다.

[0024] 저장장치(120), 데이터 채널(131)과 상기 데이터 흐름 측정 모듈(140)의 연결은 저장장치(120)에 규칙적인 데이터가 입출력되는 과정에서 발생하는 미세전류가 하드웨어 커패시터에 영향을 끼칠 수 있다.

[0025] 본 발명의 실시예에 따르면, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터의 충전량의 규칙성과 비례하여 입출력되는 데이터의 규칙성을 측정할 수 있으며, 이를 통해 정상적인 파일 또는 데이터의 입력과 비정상 데이터 입력 흐름을 구분할 수 있다.

[0027] 도 2는 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법을 설명하기 위한 흐름도이다.

[0028] 제안하는 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법은 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 데이터 흐름 측정 모듈을 통해 측정하는 단계(210), 데이터 흐름 측정 모듈을 통해 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의 커패시터에 입력되어 커패시터의 충전량이 변동되는 단계(220), 해당 커패시터들의 충전량을 측정하는 단계(230) 및 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 단계(240)를 포함한다.

[0029] 단계(210)에서, 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 데이터 흐름 측정 모듈을 통해 측정한다.

[0030] 단계(220)에서, 데이터 흐름 측정 모듈을 통해 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의 커패시터에 입력되어 커패시터의 충전량이 변동된다.

[0031] 단계(230)에서, 해당 커패시터들의 충전량을 측정하고, 단계(240)에서 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산한다.

[0032] 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 방법은 복수의 데이터 채널에서 발생하는 전류를 데이터 흐름 측정 모듈의 커패시터에 입력하고 각 커패시터의 충전량의 표준편차를 연산하여 각각의 데이터가 어떠한 전류 패턴을 가지고 있는지 측정한다.

[0033] 저장장치로의 규칙적인 데이터 입출력 과정에서 발생하는 미세전류를 이용하여, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터의 충전량의 규칙성과 비례하는 데이터의 규칙성을 측정한다.

[0034] 측정된 데이터의 규칙성을 통해 정상적인 파일, 정상적인 데이터의 입력 및 비정상 데이터의 입력 흐름을 구분한다.

[0035] 본 발명의 실시예에 따른 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산하는 단계(240)에서 커패시터의 충전량의 불규칙성이 미리 정해진 기준 보다 낮은 경우, 랜섬웨어 감염을 포함하는 악성행위 또는 비정상 데이터 흐름이 발생하지 않은 것으로 판단하고, 커패시터의 충전량의 불규칙성이 미리 정해진 기준보다 높은 경우, 암호화의 특징으로 인해 랜섬웨어를 포함하는 악성행위 또는 비정상 데이터 흐름으로 저장장치의 데이터가 변화되는 것으로 판단한다.

[0037] 도 3은 본 발명의 일 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름을 검출하기 위한 데이터 흐름 측정 모듈의 내부 구성을 나타낸다.

[0038] 본 발명의 실시예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상 데이터 흐름 검출 장치는 외부장치로부터 저장장치에 데이터 입력 시, 외부장치와 저장장치 사이에 데이터 채널을 통해 전송되는 데이터의 입력 전류를 측정하는 데이터 흐름 측정 모듈(300)을 포함한다.

[0039] 데이터 흐름 측정 모듈(300)은 커패시터 모듈(310), 커패시터 충전량 측정 모듈(320), 표준편차 측정 모듈(330) 및 타이머(340)를 포함한다.

[0040] 커패시터 모듈(310)은 측정된 입력 전류에 관한 각 데이터의 입력 미세전류가 입력되어 충전량이 변동된다.

[0041] 커패시터 충전량 측정 모듈(320)은 해당 커패시터들의 충전량을 측정한다.

[0042] 표준편차 측정 모듈(330)은 측정된 커패시터의 충전량을 이용하여 데이터 규칙성을 연산한다.

[0043] 타이머(340)에서 발생하는 타이밍에 따라 커패시터 충전량 측정 모듈(320)에 의해 커패시터 충전량이 측정되고 표준편차 측정 모듈(230)에 의해 커패시터 모듈(310)의 각 커패시터들 간의 편차를 계산한다.

[0044] 데이터 흐름 측정 모듈(300)은 복수의 데이터 채널에서 발생하는 전류를 데이터 흐름 측정 모듈의 커패시터에

입력하고 각 커패시터의 충전량의 표준편차를 연산하여 각각의 데이터가 어떠한 전류 패턴을 가지고 있는지 측정한다.

[0045] 저장장치로의 규칙적인 데이터 입출력 과정에서 발생하는 미세전류를 이용하여, 데이터 입출력 과정에서 측정된 각각의 복수의 데이터 채널에 연결된 하드웨어 커패시터의 충전량의 규칙성과 비례하는 데이터의 규칙성을 측정한다.

[0046] 측정된 데이터의 규칙성을 통해 정상적인 파일, 정상적인 데이터의 입력 및 비정상 데이터의 입력 흐름을 구분한다.

[0047] 표준편차 측정 모듈(330)은 커패시터의 충전량의 불규칙성이 미리 정해진 기준 보다 낮은 경우, 랜섬웨어 감염을 포함하는 악성행위 또는 비정상 데이터 흐름이 발생하지 않은 것으로 판단하고, 커패시터의 충전량의 불규칙성이 미리 정해진 기준보다 높은 경우, 암호화의 특징으로 인해 랜섬웨어를 포함하는 악성행위 또는 비정상 데이터 흐름으로 저장장치의 데이터가 변화되는 것으로 판단한다.

[0049] 도 4는 본 발명의 일 실시예에 따른 정상적인 데이터 흐름이 수행될 때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

[0050] 본 발명의 실시 예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 정상적인 데이터 흐름 수행때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

[0052] 도 5는 본 발명의 일 실시예에 따른 비정상적인 데이터 흐름이 수행될 때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

[0053] 본 발명의 실시 예에 따른 커패시터 소자 미세전류 충전량을 이용한 저장장치 쓰기 과정에서 비정상적인 데이터 흐름이 수행될 때의 데이터 흐름 측정 모듈 내부 커패시터의 미세전류 충전량 예시를 나타낸다.

[0054] 본 발명의 실시예에 따른 데이터 흐름 측정 모듈 또는 매체는 일반 PC 플랫폼에서 저장매체를 위한 읽기/쓰기 연산이 수행될 때 구동된다. 데이터를 측정할 부가적 채널을 통해 데이터 흐름 측정 모듈에 입력되는 미세전류는 데이터 흐름 측정 모듈 내부에 있는 커패시터 모듈 내부에 위치하는 커패시터의 충전량을 변동시키고 상기 타이머에서 발생하는 타이밍에 따라 커패시터 충전량 측정 모듈에서 커패시터 충전량 측정모듈에 의해 측정되고 표준편차 측정 모듈에 의해 각 커패시터들 간의 편차를 계산한다.

[0056] 도 6은 본 발명의 일 실시예에 따른 비정상적인 데이터 흐름 구분을 위한 매체의 구조를 나타낸다.

[0057] 도 6을 참조하면, 상기 목적의 달성을 위해 본 발명의 실시예에 따른 비정상 데이터 흐름 탐지 방법은 저장장치에 존재하는 복수의 데이터 채널에 데이터 흐름 측정 모듈을 장착하고 데이터 입출력 단계의 상기 커패시터 전하량을 측정하므로써, 전하량의 불규칙성이 낮아지는 경우에는 랜섬웨어 감염과 같은 악성행위나 비정상 데이터 흐름이 발생하지 않은 것으로 판단하며, 상기 커패시터에 축적된 전하량의 불규칙성이 높아지는 경우에는 암호화의 특징으로 인하여 랜섬웨어와 같은 악성행위나 비정상 데이터 흐름으로 인하여 저장장치의 데이터가 변화되는 것으로 판단하여 그 행위 여부를 판단할 수 있다.

[0058] 다시 말해, 데이터 채널(610)로부터 데이터를 측정할 부가적 채널을 통해 데이터 흐름 측정 모듈에 입력되는 미세전류는 데이터 흐름 측정 모듈 내부에 있는 NOT 게이트(630) 및 저항(640)을 거쳐 커패시터 모듈 내부에 위치하는 커패시터의 충전량을 변동시키고 상기 타이머에서 발생하는 타이밍에 따라 커패시터 충전량 측정 모듈에서 커패시터 충전량 측정모듈에 의해 측정되고 표준편차 측정 모듈에 의해 각 커패시터들 간의 편차를 계산한다. 그리고 결과를 상태 메모리(650)에 저장할 수 있다. 표준편차를 연산하여 하나의 데이터(파일)가 어떤 전류 패턴을 가지고 있는지 측정하고, 결과를 상태 메모리(650)에 저장할 수 있다.

[0059] 본 발명의 일 실시예에 따르면, 저장장치에 데이터가 저장되는 데이터 채널에 부착된 커패시터를 확인하여 전류 충전 수치를 통하여 하드웨어 방식으로 랜섬웨어를 탐지하기 때문에 소프트웨어 방식의 랜섬웨어 탐지보다 빠르게 수행할 수 있는 효과가 있다. 랜섬웨어가 소프트웨어 방식의 탐지 기술을 피해 변형이 되더라도 본 발명의 일 실시예에 따르면 하드웨어 방식의 탐지 기술로 변형된 랜섬웨어의 탐지를 수행할 수 있다.

[0060] 본 발명의 실시예에 따르면, 규칙성있는 데이터 흐름을 갖는 시스템에서 랜섬웨어와 같은 악성행위나 비정상적인 데이터 흐름을 빠르게 탐지되어야 하는 상황에서 빠르고 정확하게 탐지하여 문제를 해결할 수 있다.

[0062] 도 7은 본 발명의 일 실시예에 따른 정상적인 파일과 비정상적인 파일의 흐름을 비교하는 예시도이다.

[0063] 본 발명의 실시예에 따르면 데이터 채널을 통해 저장장치로 입력되는 데이터의 엔트로피를 측정하여 정상적인 파일과 비정상적인 파일의 흐름을 비교 할 수 있다.

[0064] 데이터 채널에서 저장장치로 입력되는 과정에 있어 데이터 채널에서 발생하는 전류를 커패시터 및 NOT 게이트를 통한 커패시터에 입력하고 각 커패시터의 충전량의 표준편차를 연산하여 하나의 데이터(다시 말해, 파일)가 어떤 전류 패턴을 가지고 있는지 측정할 수 있다.

[0065] 예를 들어 일반 파일과, 암호화 파일을 구분하고자 했을 때, 도 7의 왼쪽 프리퀀시(Frequency)와 같이 일반 파일의 경우 각 커패시터의 패턴이 불규칙 적으로 측정될 것이고, 도 7의 오른쪽 프리퀀시(Frequency)와 비정상 파일은 각 커패시터의 패턴이 유사하게 측정될 것이다.

[0067] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0068] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

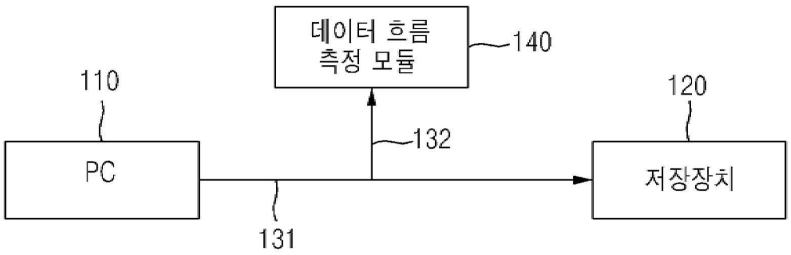
[0069] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0070] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

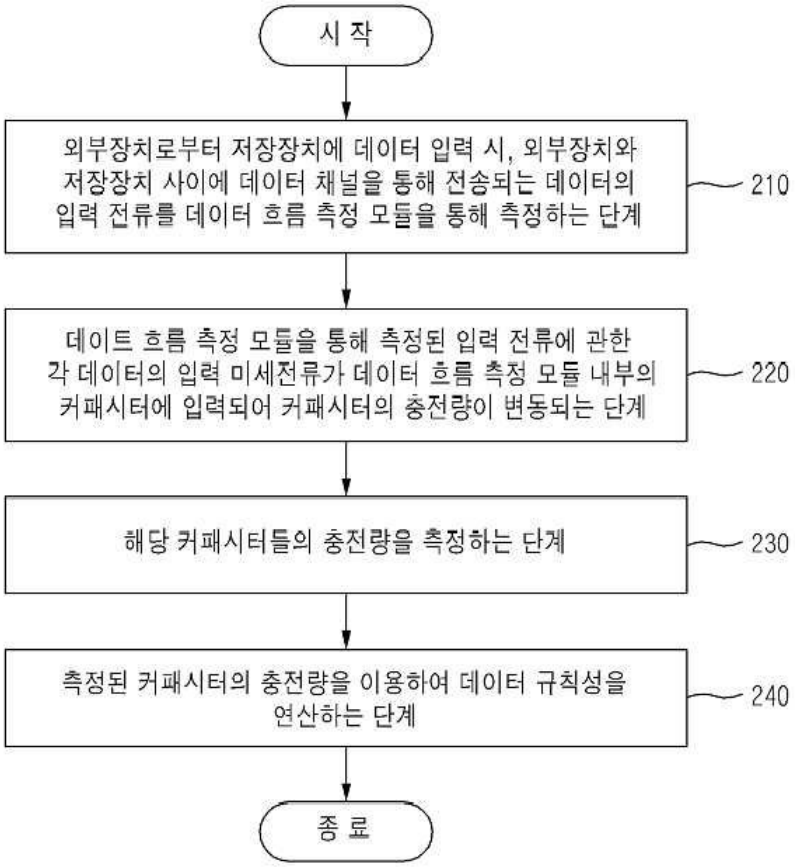
[0071] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

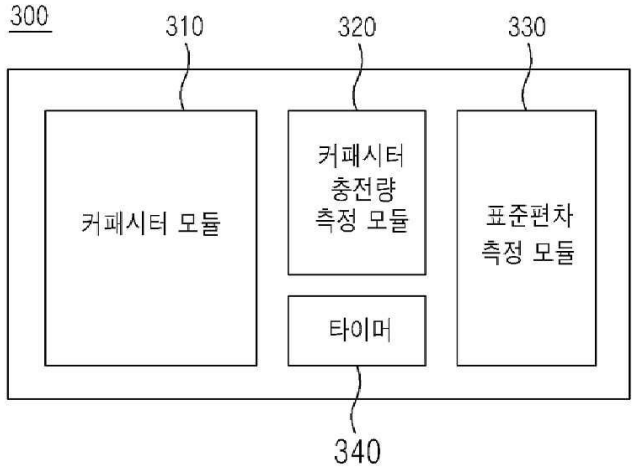
도면1


데이터 흐름
측정 모듈
140
110
120
132
PC
저장장치
131

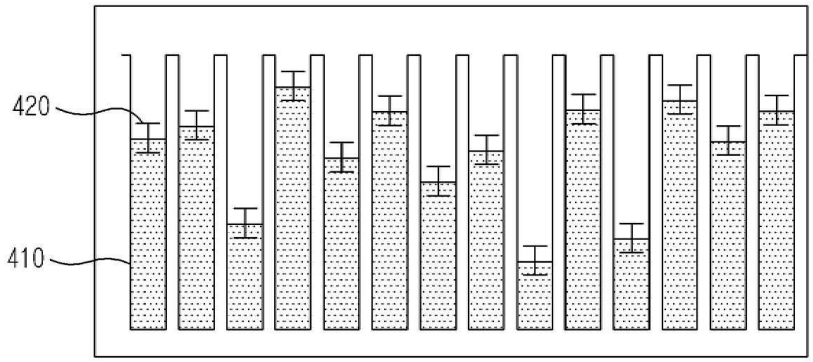
도면2


시 작
외부장치로부터 저장장치에 데이터 입력 시, 외부장치와
저장장치 사이에 데이터 채널을 통해 전송되는 데이터의
입력 전류를 데이터 흐름 측정 모듈을 통해 측정하는 단계
210
데이트 흐름 측정 모듈을 통해 측정된 입력 전류에 관한
각 데이터의 입력 미세전류가 데이터 흐름 측정 모듈 내부의
커패시터에 입력되어 커패시터의 충전량이 변동되는 단계
220
해당 커패시터들의 충전량을 측정하는 단계
230
측정된 커패시터의 충전량을 이용하여 데이터 규칙성을
연산하는 단계
240
종 료

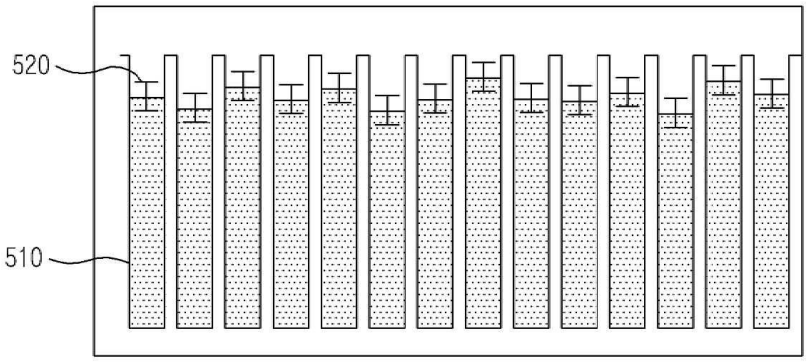
도면3


300
310
320
330
커패시터 모듈
커패시터 충전량 측정 모듈
표준편차 측정 모듈
타이머
340

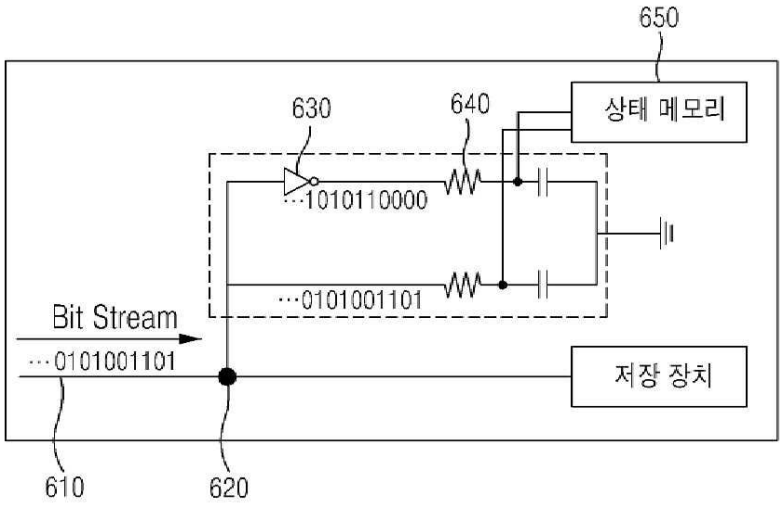
도면4


420
410

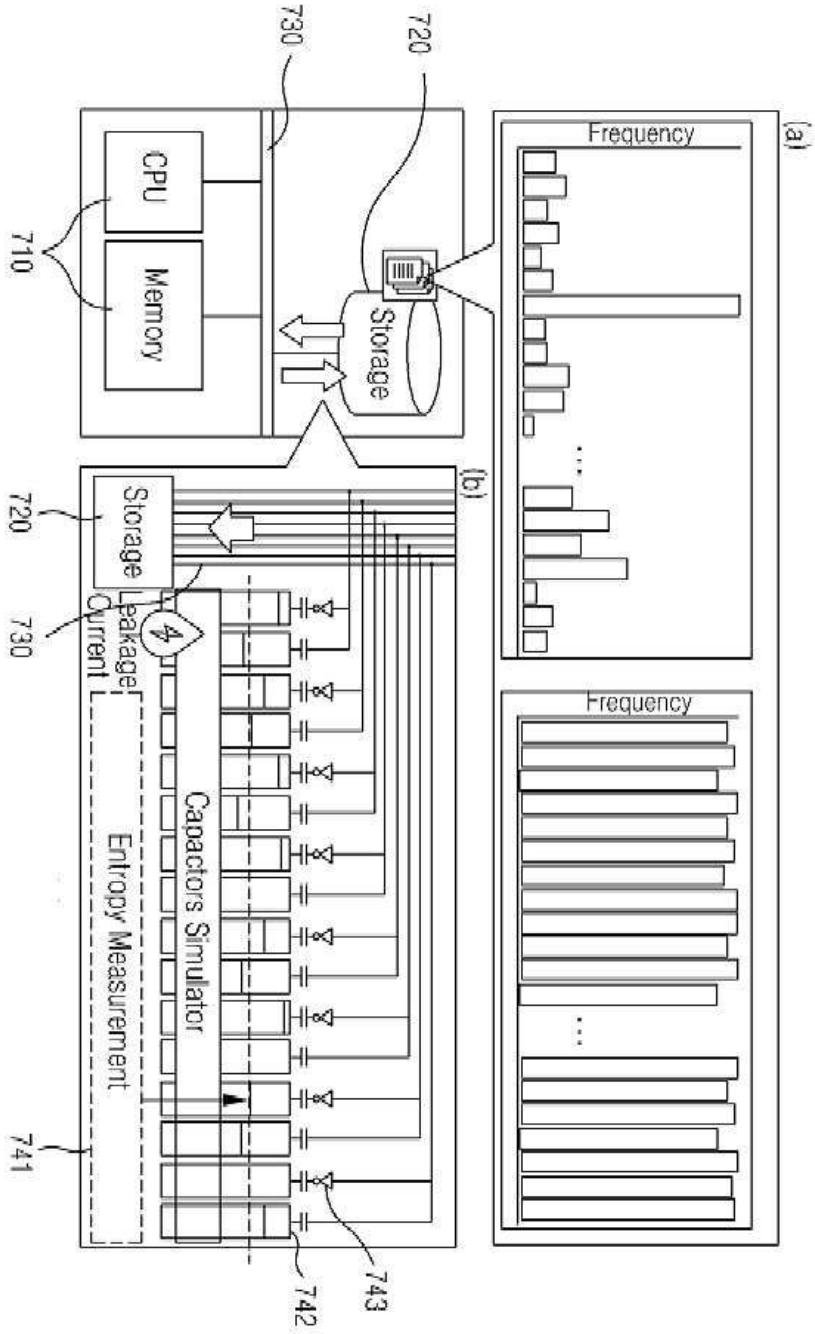
도면5


520
510

도면6


650
630
640
상태 메모리
…1010110000
…0101001101
Bit Stream
…0101001101
저장 장치
610
620

도면7


730
720
CPU
Memory
710
Storage
(a)
Frequency
(b)
720
Storage
730
Leakage Current
Capacitors Simulator
Entropy Measurement
741
742
743
Frequency