



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0146076
(43) 공개일자 2022년11월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) G06F 12/084 (2016.01)
G06N 20/00 (2019.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 12/084 (2013.01)
(21) 출원번호 10-2021-0052916
(22) 출원일자 2021년04월23일
심사청구일자 2021년04월23일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김호동
경기도 이천시 대산로247번길 50, 103동 706호
허준범
경기도 용인시 기흥구 보정로 30, 119동 201호(보정동, 동아솔레스티아파트)
(74) 대리인
김홍석

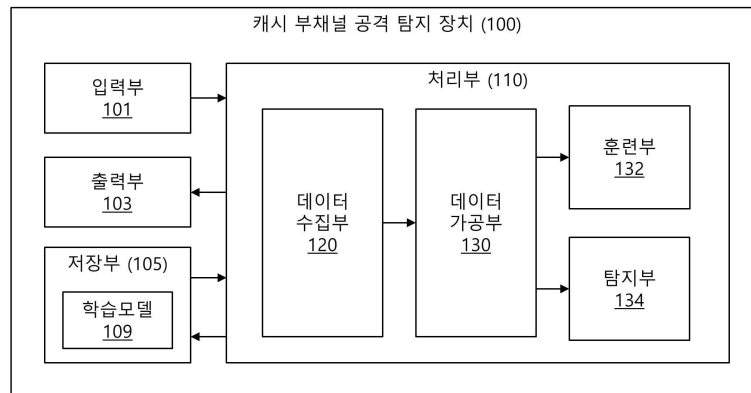
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 캐시 부채널 공격 탐지 장치 및 방법

(57) 요약

캐시 부채널 공격에 대한 탐지를 높은 정확도로 실시간으로 신속하게 수행할 수 있는 캐시 부채널 공격 탐지 장치 및 방법에 관한 것으로, 캐시 부채널 공격 탐지 장치는 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로 부터 데이터를 각각 수집하는 데이터 수집부 및 적어도 하나의 훈련된 학습 모델을 이용하여 상기 데이터에 대응하는 탐지 결과를 획득하는 탐지부를 포함할 수 있다.

대표도 - 도1



(52) CPC특허분류

G06N 20/00 (2021.08)

G06F 2207/7219 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093605
과제번호	2019-0-00533-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	컴퓨터 프로세서의 구조적 보안 취약점 검증 및 공격 탐지대응
기 여 율	1/1
과제수행기관명	고려대학교산학협력단
연구기간	2019.04.01 ~ 2019.12.31

명세서

청구범위

청구항 1

코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 데이터 수집부; 및
적어도 하나의 훈련된 학습 모델을 이용하여 상기 데이터에 대응하는 탐지 결과를 획득하는 탐지부;를 포함하는
캐시 부채널 공격 탐지 장치.

청구항 2

제1항에 있어서,

상기 데이터 수집부는,

코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 하드웨어의 활동에 대한 데이터를 획득하여 기록하는
하드웨어 성능 카운터;를 포함하는 캐시 부채널 공격 탐지 장치.

청구항 3

제1항에 있어서,

상기 데이터에 대해 상관 관계 분석을 수행하여 상기 데이터를 가공하는 데이터 가공부;를 더 포함하는 캐시 부
채널 공격 탐지 장치.

청구항 4

제1항에 있어서,

상기 데이터를 이용하여 적어도 하나의 학습 모델을 훈련시켜 상기 적어도 하나의 훈련된 학습 모델을 획득하는
훈련부;를 더 포함하는 캐시 부채널 공격 탐지 장치.

청구항 5

제4항에 있어서,

상기 데이터는, 캐시 부채널 공격이 부재한 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나
로부터 획득된 비공격 데이터; 및

모의 공격이 존재하는 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 모의 공
격 데이터;를 포함하는 캐시 부채널 공격 탐지 장치.

청구항 6

제4항에 있어서,

상기 적어도 하나의 학습 모델은, 다층 퍼셉트론(Multi-layer Perceptron), 서포트 벡터 머신(SVM: support
vector machine), 심층 신경망(DNN, Deep Neural Network), 컨볼루션 신경망(CNN, Convolutional Neural
Network), 순환 신경망(RNN, Recurrent Neural Network), 심층 신뢰 신경망(DBN, Deep Belief Network), 심층
Q-네트워크(Deep Q-Networks), 장단기 메모리(LSTM: Long short term memory), 생성적 적대 신경망(GAN:
Generative Adversarial Network) 및 조건적 생성적 적대 신경망(cGAN: Conditional GAN) 중 적어도 하나의 기
계 학습 모델을 포함하는 캐시 부채널 공격 탐지 장치.

청구항 7

코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 단계; 및

적어도 하나의 훈련된 학습 모델을 이용하여 상기 데이터에 대응하는 탐지 결과를 획득하는 단계;를 포함하는

캐시 부채널 공격 탐지 방법.

청구항 8

제7항에 있어서,

상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 단계는,

코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 하드웨어의 활동에 대한 데이터를 획득하여 기록하는 단계;를 포함하는 캐시 부채널 공격 탐지 방법.

청구항 9

제7항에 있어서,

상기 데이터에 대해 상관 관계 분석을 수행하여 상기 데이터를 가공하는 단계;를 더 포함하는 캐시 부채널 공격 탐지 방법.

청구항 10

제7항에 있어서,

상기 데이터를 이용하여 적어도 하나의 학습 모델을 훈련시켜 상기 적어도 하나의 훈련된 학습 모델을 획득하는 단계;를 더 포함하는 캐시 부채널 공격 탐지 방법.

청구항 11

제10항에 있어서,

상기 데이터는, 캐시 부채널 공격이 부재한 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 비공격 데이터; 및

모의 공격이 존재하는 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 모의 공격 데이터;를 포함하는 캐시 부채널 공격 탐지 방법.

청구항 12

제11항에 있어서,

상기 적어도 하나의 학습 모델은, 다층 퍼셉트론, 서포트 벡터 머신, 심층 신경망, 콘볼루션 신경망, 순환 신경망, 심층 신뢰 신경망, 심층 Q-네트워크, 장단기 메모리, 생성적 적대 신경망 및 조건적 생성적 적대 신경망 중 적어도 하나의 기계 학습 모델을 포함하는 캐시 부채널 공격 탐지 방법.

발명의 설명

기술 분야

[0001] 본 발명은 캐시 부채널 공격 탐지 장치 및 방법에 관한 것이다.

배경 기술

[0002] 중앙처리장치(CPU: Central Processing Unit)는 연산의 고속 처리를 위해 임시 저장 매체인 캐시 메모리를 이용한다. 캐시 메모리는 프로그램의 구동 과정에서 빈번히 사용되거나 사용될 것으로 판단되거나 또는 곧 사용될 각종 데이터를 저장하고, 요청에 따라 저장한 데이터를 중앙처리장치에 제공함으로써 데이터 접근 시간이나 연산 시간을 단축시켜 중앙처리장치가 신속하게 연산 처리 동작을 수행할 수 있도록 한다.

[0003] 캐시 부채널 공격(Cache side-channel attack)은 중앙처리장치의 동작에 따라 캐시 메모리에 발생하는 각종 흔적(기록이나 삭제 등)들을 추출 및 분석하여 공격 대상 장치로부터 정보를 무단으로 획득하는 것을 의미한다. 데스크톱 컴퓨터, 랩톱 컴퓨터, 서버 컴퓨터 또는 스마트폰 등 다양한 전자 장치가 캐시 부채널 공격의 대상이 될 수 있으며, 암호화 비밀번호, 인터넷 브라우저 히스토리, 방화벽 규칙, 비밀번호 또는 휴대폰 잠금 패턴 등 다양한 정보가 공격 목표가 될 수 있다. 캐시 부채널 공격으로는 플러시+리로드 공격(Flush+Reload Attack)이나 프라임+어보트 어택(Prime+Abort Attack) 등이 있다. 플러시 리로드 공격은 공격자가 캐시 메모리의 데이터를

삭제한 후(플러시 과정) 삭제된 데이터에의 접근에 따른 소요 시간을 측정(리로드 과정)함으로써 공격 대상 장치의 실행 흐름에 대한 정보를 획득하는 방법이다. 프라임 어보트 어택은 공격자가 감시하고자 하는 캐시 집단에 데이터를 기록하고(프라임 과정), 희생자가 캐시에 데이터를 적재하기 위해 공격자가 기록한 데이터를 제거할 때(어보트 과정) 발생하는 트랜잭션 어보트 하드웨어 콜 백(Transaction abort hardware callback)을 이용하여 공격자가 대상의 실행 흐름을 파악하는 방법이다.

[0004] 이와 같이 캐시 부채널 공격에 의하면, 공격 대상 장치의 중요한 비밀 정보가 무단으로 노출될 수 있으므로, 캐시 부채널 공격을 탐지하고 차단하는 것은 하드웨어 장치의 보안에 있어서 매우 중요하다. 그러나, 캐시 부채널 공격 방법은 공격하고자 하는 하드웨어나 소프트웨어에 따라 그 세부적인 설정을 달리하기 때문에, 동일한 기법의 공격이라고 하더라도 공격 목표에 따라 외부에서 관측되는 현상은 상이할 수 있다. 이는 캐시 부채널 공격 여부의 탐지 및 판단에 고도의 전문성이 필요하다는 것을 의미할 뿐만 아니라, 종래의 정형화된 방법만으로는 높은 정확성의 공격 탐지를 기대하기 어렵다는 것도 의미한다. 또한, 캐시 부채널 공격은 기법에 따라 공격 대상 장치에 영향이 없거나 영향이 있다고 하더라도 미미하여 피해자가 공격 여부를 체감하지 못할 수도 있고, 체감이 가능하다고 하더라도 그 공격이 수초 이하의 매우 짧은 시간 동안 수행되므로 공격의 감지, 탐지 및 대응이 매우 어렵다는 문제점도 존재한다.

발명의 내용

해결하려는 과제

[0005] 해결하고자 하는 과제는 높은 정확도로 실시간으로 캐시 부채널 공격에 대한 탐지를 신속하게 수행할 수 있도록 하는 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법을 제공하는 것이다.

과제의 해결 수단

- [0006] 상술한 과제를 해결하기 위하여 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법이 제공된다.
- [0007] 캐시 부채널 공격 탐지 장치는 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 데이터 수집부 및 적어도 하나의 훈련된 학습 모델을 이용하여 상기 데이터에 대응하는 탐지 결과를 획득하는 탐지부를 포함할 수 있다.
- [0008] 상기 데이터 수집부는 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 하드웨어의 활동에 대한 데이터를 획득하여 기록하는 하드웨어 성능 카운터를 포함할 수 있다.
- [0009] 캐시 부채널 공격 탐지 장치는 상기 데이터에 대해 상관 관계 분석을 수행하여 상기 데이터를 가공하는 데이터 가공부를 더 포함할 수 있다.
- [0010] 캐시 부채널 공격 탐지 장치는 상기 데이터를 이용하여 적어도 하나의 학습 모델을 훈련시켜 상기 적어도 하나의 훈련된 학습 모델을 획득하는 훈련부를 더 포함할 수 있다.
- [0011] 상기 데이터는 캐시 부채널 공격이 부채널 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 비공격 데이터 및 모의 공격이 존재하는 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 모의 공격 데이터를 포함할 수 있다.
- [0012] 상기 적어도 하나의 학습 모델은 다층 퍼셉트론(Multi-layer Perceptron), 서포트 벡터 머신(SVM: support vector machine), 심층 신경망(DNN, Deep Neural Network), convolutional 신경망(CNN, Convolutional Neural Network), 순환 신경망(RNN, Recurrent Neural Network), 심층 신뢰 신경망(DBN, Deep Belief Network), 심층 Q-네트워크(Deep Q-Networks), 장단기 메모리(LSTM: Long short term memory), 생성적 적대 신경망(GAN: Generative Adversarial Network) 및 조건적 생성적 적대 신경망(cGAN: Conditional GAN) 중 적어도 하나의 기계 학습 모델을 포함할 수 있다.
- [0013] 캐시 부채널 공격 탐지 방법은 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 단계 및 적어도 하나의 훈련된 학습 모델을 이용하여 상기 데이터에 대응하는 탐지 결과를 획득하는 단계를 포함할 수 있다.
- [0014] 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 데이터를 각각 수집하는 단계는, 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 하드웨어의 활동에 대한 데이터를 획득하여 기록하는 단계를 포함할 수 있다.

- [0015] 캐시 부채널 공격 탐지 방법은 상기 데이터에 대해 상관 관계 분석을 수행하여 상기 데이터를 가공하는 단계를 더 포함할 수 있다.
- [0016] 캐시 부채널 공격 탐지 방법은 상기 데이터를 이용하여 적어도 하나의 학습 모델을 훈련시켜 상기 적어도 하나의 훈련된 학습 모델을 획득하는 단계를 더 포함할 수 있다.
- [0017] 상기 데이터는 캐시 부채널 공격이 부재한 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로 부터 획득된 비공격 데이터 및 모의 공격이 존재하는 상황에서 상기 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득된 모의 공격 데이터를 포함할 수 있다.
- [0018] 상기 적어도 하나의 학습 모델은 다층 퍼셉트론, 서포트 벡터 머신, 심층 신경망, 콘볼루션 신경망, 순환 신경망, 심층 신뢰 신경망, 심층 Q-네트워크, 장단기 메모리, 생성적 적대 신경망 및 조건적 생성적 적대 신경망 중 적어도 하나의 기계 학습 모델을 포함할 수 있다.

발명의 효과

- [0019] 상술한 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법에 의하면, 많은 전문 지식과 긴 분석 시간을 요구하는 캐시 부채널에 대한 공격 탐지를 높은 정확도로 짧은 시간 내에 수행할 수 있는 효과를 얻을 수 있다.
- [0020] 상술한 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법에 의하면, 다양한 방식/유형/과정의 공격에 용이하고 신속하게 대처할 수 있게 되며, 이에 따라 새로운 방식에 의거하는 공격에도 적절하게 탐지 및 대처할 수 있게 되어 공격 탐지의 유연성이 증진되는 효과도 가지고 있다.
- [0021] 상술한 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법에 의하면, 시스템에 영향이 없거나 체감하기 어려운 상황에서도 캐시 부채널에 대한 공격을 탐지할 수 있을 뿐만 아니라, 매우 짧은 시간동안 진행된 희생자의 정보 획득 등의 같은 공격에 대해서도 이를 신속하게 탐지 및 대응할 수 있는 장점도 얻을 수 있다.
- [0022] 상술한 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법에 의하면, 기업, 관공서 또는 인터넷 데이터 센터(IDC: Internet Data Center) 등에서 이용되는 컴퓨터 또는 서버 장치나, 개인용 통신 기기나, 공용 컴퓨터 장치나, 포스(POS) 장치나, 공장 등에서 이용되는 전자 장치나, 차량이나, 유인 비행체나 또는 무인 비행체 등과 같이 다양한 전자 장치의 데이터를 안전하고 신뢰도 높게 보호할 수 있는 효과도 얻을 수 있다.
- [0023] 상술한 캐시 부채널 공격 탐지 장치 및 캐시 부채널 공격 탐지 방법은, 높은 이식성을 가지고 있어 다양한 플랫폼에 적용될 수 있다는 장점도 가지고 있다.

도면의 간단한 설명

- [0024] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 캐시 부채널 공격 탐지 장치의 일 실시예에 대한 블록도이다.
- 도 2는 처리 장치로부터 데이터를 수집하는 과정의 일례를 설명하기 위한 도면이다.
- 도 3은 학습 모델의 훈련 과정의 일례를 설명하기 위한 도면이다.
- 도 4는 학습 모델 기반 탐지 과정의 일례를 설명하기 위한 도면이다.
- 도 5는 캐시 부채널 공격 탐지 방법의 일 실시예에 대한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0025] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.
- [0026] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

- [0027] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.
- [0028] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0029] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 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 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0031] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.
- [0032] 이하 도 1 내지 도 4를 참조하여, 캐시 부채널 공격 탐지 장치의 일 실시예에 대해서 설명하도록 한다.
- [0033] 도 1은 캐시 부채널 공격 탐지 장치의 일 실시예에 대한 블록도이다.
- [0034] 도 1에 도시된 바에 의하면, 캐시 부채널 공격 탐지 장치(100)는 입력부(101), 출력부(103), 저장부(105) 및 처리부(110)를 포함할 수 있다. 여기서, 입력부(101), 출력부(103), 저장부(105) 및 처리부(110) 중 적어도 둘은 케이블이나 회로선 등을 통해 일방으로 또는 상호 간에 데이터 또는 지시/명령 등을 전달할 수 있도록 마련된다. 필요에 따라서, 입력부(101), 출력부(103) 및 저장부(105) 중 적어도 하나는 생략될 수도 있다.
- [0035] 입력부(101)는 설계자, 사용자 또는 외부의 다른 장치(미도시)로부터 데이터, 지시/명령 또는 프로그램(앱, 애플리케이션 또는 소프트웨어 등으로 지칭 가능함) 등을 수신하고, 수신한 데이터, 지시/명령 또는 프로그램 등을 저장부(105) 및 처리부(110) 중 적어도 하나로 전달할 수 있다. 예를 들어, 입력부(101)는 학습 모델(109)의 훈련을 위해 행해지는 캐시 부채널 공격(이하 모의 공격)을 위한 알고리즘, 이에 대한 데이터 및/또는 이에 대한 명령 등을 수신할 수도 있다. 또한, 입력부(101)는 다른 정보 처리 장치(미도시)에 의해 훈련된 적어도 하나의 학습 모델(도 3 또는 도 4의 109a)를 수신할 수도 있다. 입력부(101)는 실시예에 따라서 캐시 부채널 공격 탐지 장치(100)와 일체형으로 마련된 것일 수도 있고 또는 물리적으로 분리 가능하게 마련된 것일 수도 있다. 입력부(101)는, 예를 들어, 키보드, 마우스, 태블릿, 감압 센서, 동작 센서, 광 센서, 터치 스크린, 터치 패드, 스캐너, 영상 촬영 모듈, 마이크로 폰, 트랙볼 및/또는 트랙패드 등을 포함할 수 있으며, 또한 외부의 장치(메모리 장치 등)로부터 데이터 등의 수신 가능한 데이터 입출력 단자나, 외부의 다른 장치와 유무선 통신 네트워크를 통해 연결되는 유선 또는 무선 통신 모듈(일례로 랜 카드, 근거리 통신 모듈 또는 이동 통신 모듈 등) 등을 포함할 수도 있다.
- [0036] 출력부(103)는 처리부(110)의 처리 결과를 외부로 출력할 수 있도록 마련된다. 예를 들어, 출력부(103)는 처리부(110)에 의한 캐시 부채널 공격의 탐지 과정에 대한 정보, 탐지 결과 또는 이에 대응하는 경고 메시지를 시각적 또는 청각적으로 외부로 출력하여 캐시 부채널 공격 탐지 장치(100)의 관리자나 사용자 등에게 알려줄 수도 있고, 및/또는 탐지 결과나 경고 메시지 등을 외부의 다른 전자 장치(예를 들어, 스마트 폰이나 데스크톱 컴퓨터 등)로 전송할 수도 있다. 필요에 따라서, 출력부(103)는 처리부(110)에 의해 훈련된 학습 모델(109a)를 외부

의 다른 정보 처리 장치(미도시, 일례로 다른 캐시 부채널 공격 탐지 장치)로 송신하는 것도 가능하다. 이 경우, 외부의 다른 정보 처리 장치는 캐시 부채널 공격 탐지 장치(100)로부터 수신한 훈련된 학습 모델(109a)을 이용하여 후술하는 바와 동일하거나 또는 일부 상이한 방법을 통해 캐시 부채널 공격에 대한 탐지를 수행할 수도 있다. 출력부(103)는, 예를 들어, 디스플레이 장치(모니터 장치 등), 프린터 장치, 스피커 장치, 영상 출력 단자, 데이터 입출력 단자, 유선 통신 모듈 및/또는 무선 통신 모듈 등을 포함할 수 있으나, 이에 한정되는 것은 아니다.

[0037] 저장부(105)는 캐시 부채널 공격 탐지 장치(100)와 관련된 적어도 하나의 정보나 프로그램 등을 일시적 또는 비 일시적으로 저장할 수 있다. 예를 들어, 저장부(105)는 캐시 부채널 공격의 탐지 결과, 탐지 결과에 대응하는 경고 메시지, 탐지 과정에 대한 히스토리, 훈련 전 학습 모델(109) 및/또는 훈련된 학습 모델(109a) 등을 저장할 수 있다. 여기서, 훈련 전 학습 모델(109) 및/또는 훈련된 학습 모델(109a)은, 다층 퍼셉트론(Multi-layer Perceptron), 서포트 벡터 머신(SVM: support vector machine), 심층 신경망(DNN, Deep Neural Network), 콘볼루션 신경망(CNN, Convolutional Neural Network), 순환 신경망(RNN, Recurrent Neural Network), 심층 신뢰 신경망(DBN, Deep Belief Network), 심층 Q-네트워크(Deep Q-Networks), 장단기 메모리(LSTM: Long short term memory), 생성적 적대 신경망(GAN: Generative Adversarial Network) 및/또는 조건적 생성적 적대 신경망(cGAN: Conditional GAN) 등과 같이 설계자가 고려 가능한 적어도 하나의 기계 학습 모델을 기반으로 구현된 것일 수 있다. 또한, 저장부(105)는 캐시 부채널 공격 탐지를 위해 처리부(110)에 의해 구동될 적어도 하나의 프로그램을 저장할 수도 있다. 여기서, 적어도 하나의 프로그램은, 예를 들어, 성능 카운터 감시(PCM, Performance Counter Monitor) 프로그램 및/또는 훈련 전 학습 모델(109) 또는 훈련된 학습 모델(109a) 등을 단독으로 또는 조합하여 구현된 것일 수 있다. 적어도 하나의 프로그램은, 예를 들어, 캐시 부채널 공격 탐지를 위해 특별히 고안된 별도의 프로그램일 수도 있고, 또는 캐시 부채널 공격 탐지 동작을 포함하여 설계, 제작된 실시간 공격 탐지 프로그램이나 백신 프로그램 등일 수도 있다. 적어도 하나의 프로그램은 설계자에 의해 직접 작성되어 저장부(105)에 입력, 저장 또는 수정될 수도 있고, 또는 유선 또는 무선 통신 네트워크를 통해 접속 가능한 전자 소프트웨어 유통망을 통하여 획득 또는 갱신될 수도 있다.

[0038] 저장부(105)는 주기억장치 및 보조기억장치 중 적어도 하나를 이용하여 구현될 수 있다. 여기서, 주기억장치는 롬(ROM)이나 램(RAM) 등의 반도체 저장 매체를 포함할 수 있고, 보조기억장치는 플래시 메모리 장치, SD(Secure Digital) 카드, 솔리드 스테이트 드라이브(SSD, Solid State Drive), 하드 디스크 드라이브(HDD, Hard Disc Drive), 콤팩트 디스크(CD), 디브이디(DVD), 광자기 디스크 및/또는 플로피 디스크 등과 같이 데이터를 영구적 또는 반영구적으로 저장할 수 있는 적어도 하나의 저장 매체를 포함할 수 있다.

[0039] 처리부(110)는 캐시 부채널 공격을 탐지하고 탐지 결과를 획득 및 출력할 수 있도록 마련된다. 또한, 처리부(110)는 채널 부채널 공격의 탐지에 이용될 학습 모델(109)의 훈련 처리를 더 수행할 수도 있다. 필요에 따라, 처리부(110)는 캐시 부채널 공격 탐지 장치(100)의 전반적인 또는 부분적인 동작에 관한 연산, 판단이나 제어 처리를 수행할 수도 있다. 이 경우, 처리부(110)는 저장부(105)에 저장된 적어도 하나의 프로그램을 동시에 또는 순차적으로 구동시켜 상술한 동작을 수행할 수도 있다.

[0040] 처리부(110)는, 예를 들어, 중앙 처리 장치(CPU: Central Processing Unit), 마이크로 컨트롤러 유닛(MCU: Micro Controller Unit), 마이컴(Micom: Micro Processor), 애플리케이션 프로세서(AP: Application Processor), 전자 제어 유닛(ECU: Electronic Controlling Unit) 및/또는 각종 연산 처리 및 제어 신호의 생성이 가능한 다른 전자 장치 등을 포함할 수 있다. 이들 장치는, 예를 들어, 하나 또는 둘 이상의 반도체 칩 등을 이용하여 구현된 것일 수 있다.

[0041] 일 실시예에 의하면, 처리부(110)는 도 1에 도시된 바와 같이 데이터 수집부(120), 데이터 가공부(130), 훈련부(132) 및 탐지부(134)를 포함할 수 있다.

[0042] 도 2는 처리 장치로부터 데이터를 수집하는 과정의 일례를 설명하기 위한 도면이다.

[0043] 데이터 수집부(120)는 캐시 부채널 공격의 탐지 및 판단에 필요한 적어도 하나의 데이터를 수집 및 획득하고, 수집 및 획득한 적어도 하나의 데이터를 데이터 가공부(130), 훈련부(132) 및 탐지부(134) 중 적어도 하나로 직접 또는 다른 장치를 경유하여 전달할 수 있다. 일 실시예에 의하면, 데이터 수집부(120)는 프로세서(일례로 중앙처리장치) 등과 같은 하드웨어의 동작과 연관된 데이터를 수집할 수 있다. 여기서, 프로세서는 데이터 수집부(120), 데이터 가공부(130), 훈련부(132) 및/또는 탐지부(134)의 동작 및 기능을 수행하도록 마련된 것일 수 있다. 다시 말해서, 데이터 수집부(120)의 데이터 수집 대상이 되는 프로세서는, 처리부(110)일 수도 있으며, 이 경우 처리부(110, 즉, 데이터 수집부(120))는 자신의 활동에 대한 정보를 수집하게 된다. 또한, 실시예에 따라

서, 데이터 수집부(120)의 데이터 수집 대상이 되는 프로세서는 처리부(110)와 별도로 마련된 다른 하나 이상의 프로세서(미도시)일 수도 있으며, 처리부(110)는 다른 프로세서로부터 다른 프로세서의 동작에 관한 정보를 수집할 수도 있다.

[0044] 데이터 수집 대상인 프로세서는, 실시예에 따라, 도 2에 도시된 바와 같이, 연산/처리를 수행하는 적어도 하나의 코어(91: 91-1, 91-2)와, 적어도 하나의 코어(91: 91-1, 91-2) 각각에 대응하는 적어도 하나의 L1 캐시(92: 92-1, 92-2)를 포함할 수 있다. 또한, 데이터 수집 대상이 되는 프로세서는 적어도 하나의 코어(91: 91-1, 91-2) 각각에 대응하는 적어도 하나의 L2 캐시(93: 93-1, 93-2) 및/또는 다수의 코어(91)에 대응하는 적어도 하나의 L3 캐시(94)를 더 포함할 수도 있다. 적어도 하나의 L2 캐시(93: 93-1, 93-2)나 적어도 하나의 L3 캐시(94)는 중앙처리장치와 일체적으로 마련된 것일 수도 있고 또는 물리적으로 분리되어 마련된 것일 수도 있다. 데이터 수집부(120)는, 이와 같이 적어도 하나의 코어(91: 91-1, 91-2), 적어도 하나의 L1 캐시(92: 92-1, 92-2), 적어도 하나의 L2 캐시(93: 93-1, 93-2) 및 적어도 하나의 L3 캐시(94) 중 적어도 하나로부터 활동에 대응하는 데이터(예를 들어, 중앙처리장치의 활동에 대응하여 기록된 값)를 획득함으로써 캐시 부채널 공격의 탐지 및 판단에 필요한 데이터를 수집할 수 있다. 만약 복수의 코어(91: 91-1, 91-2)가 마련되어 있다면, 데이터 수집부(120)는 사용자의 선택이나 미리 설정된 바 등에 따라 복수의 코어(91: 91-1, 91-2) 모두로부터 하드웨어의 활동에 대응하는 데이터를 획득할 수도 있고 또는 복수의 코어(91: 91-1, 91-2) 중 일부로부터 하드웨어의 활동에 대응하는 데이터를 획득할 수도 있다. 동일하게 복수의 L1 캐시(92: 92-1, 92-2), 복수의 L2 캐시(93: 93-1, 93-2) 및/또는 복수의 L3 캐시(94)가 존재하는 경우라면, 데이터 수집부(120)는 모든 L1 캐시(92: 92-1, 92-2), 모든 L2 캐시(93: 93-1, 93-2) 및/또는 모든 L3 캐시(94)로부터 데이터를 획득할 수도 있고, 또는 일부의 L1 캐시(92: 92-1, 92-2), 일부의 L2 캐시(93: 93-1, 93-2) 및/또는 일부의 L3 캐시(94)로부터 데이터를 획득할 수도 있다.

[0045] 일 실시예에 따르면, 코어(91: 91-1, 91-2), L1 캐시(92: 92-1, 92-2), L2 캐시(93: 93-1, 93-2) 및 L3 캐시(94) 중 적어도 하나로부터 공격 탐지에 관한 데이터를 수집하기 위해, 데이터 수집부(120)는 하드웨어 성능 카운터(HPC: Hardware Performance Counter, 하드웨어 카운터로 지칭 가능함, 121) 및 성능 카운터 감시부(PCM: Performance Counter, 123) 중 적어도 하나를 포함할 수 있다. 하드웨어 성능 카운터(121)는 프로세서 등과 같은 하드웨어의 활동에 관련된 값(일례로 하드웨어의 활동에 대한 계수 결과)를 기록하도록 마련된 것일 수 있다. 하드웨어 성능 카운터(121)는 일 군의 레지스터를 이용하여 구현된 것일 수 있다. 여기서, 일 군의 레지스터는 동작에 따른 계수 결과를 저장하기 위해 특별히 마련된 것일 수 있으며, 중앙처리장치 등과 같은 프로세서 내에 내장된 것일 수도 있다. 일 군의 레지스터의 개수는 프로세서의 종류나 제조사 등에 따라 다양할 수 있다. 또한, 하드웨어와 관련된 활동은, 예를 들어, L1 캐시 미스(L1 cache miss), L2 캐시 미스, L3 캐시 미스, L2 캐시 미스나 L3 캐시 미스에 기인한 중앙 처리 장치 사이클의 비율, L2 히트(L2 HIT), L3 히트, 메모리 컨트롤러 등으로부터 읽거나 메모리 컨트롤러에 기록한 데이터 크기 및/또는 분기 예측 오류 등과 같은 다양한 이벤트를 포함할 수 있다. 성능 카운터 감시부(123)는 프로세서 등의 활동을 분석할 수 있다. 구체적으로 예를 들어, 성능 카운터 감시부(123)는 하드웨어 성능 카운터(121)에 저장된 값을 이용하여 각각의 코어(91: 91-1, 91-2)마다 하드웨어의 활동과 관련된 값들을 획득하고 이를 사용자 등이 확인할 수 있는 형태의 수치로 변환하거나 획득된 수치 등을 기반으로 그래프 등을 구성할 수도 있다. 또한, 성능 카운터 감시부(123)는 획득한 값들을 소정 포맷(예를 들어, CSV 포맷 등)의 데이터로 생성하여 출력할 수도 있다. 성능 카운터 감시부(123)는 실시예에 따라 하드웨어적으로 또는 소프트웨어적으로 구현될 수 있으며, 필요에 따라 생략될 수도 있다. 하드웨어 성능 카운터(121)나 성능 카운터 감시부(123)가 획득한 데이터는 데이터 가공부(130)로 전달될 수 있다.

[0046] 도 1에 도시된 바를 참조하면, 데이터 가공부(130)는, 일 실시예에 있어서, 데이터 수집부(120)가 수집한 데이터를 수신하고, 사용자나 설계자 등에 의해 미리 정의된 바에 따라 또는 임의적 설정에 따라 수신한 데이터를 가공하여 가공된 데이터를 획득할 수 있다. 일례로, 데이터 가공부(130)는 데이터 수집부(120)가 수집한 데이터를 분석하고 데이터 수집부(120)가 수집한 데이터 중에서 필요도나 중요도가 높은 데이터를 선택하는 과정을 통해 데이터 수집부(120)가 수집한 데이터를 가공할 수도 있다. 이 경우, 선택되지 않은 데이터는 필요에 따라 제거될 수도 있다. 일 실시예에 의하면, 데이터 가공부(130)는 데이터 수집부(120)가 수집한 데이터 각각의 필드를 획득하고, 각각의 필드와 공격 여부 간의 상관 관계 분석(correlation analysis)을 수행함으로써 필요도나 중요도가 높은 필드의 데이터를 선택할 수도 있다. 예를 들어, 데이터 필드와 공격 여부의 간의 상관 관계에 대한 연산 결과가 미리 정의된 임계 값(예를 들어, 0.3)을 초과하는 경우에는 해당 데이터 필드의 데이터(들)을 선택하고 그 외의 데이터 필드의 데이터들은 삭제함으로써 가공된 데이터를 획득할 수 있다. 실시예에 따라서는, 데이터 가공부(130)는 생략 가능하다. 데이터 수집부(120)가 수집한 데이터 또는 데이터 가공부(130)가 획득한

가공된 데이터는 훈련부(132) 및 탐지부(134) 중 적어도 하나로 전달될 수 있다.

[0047] 도 3은 학습 모델의 훈련 과정의 일례를 설명하기 위한 도면이다.

[0048] 훈련부(132)는 도 3에 도시된 바와 같이 데이터 수집부(120) 또는 데이터 가공부(130)로부터 데이터를 수신하고 수신한 데이터를 기반으로 학습 모델(109)에 대한 훈련을 수행하여 훈련된 학습 모델(109a)을 획득할 수 있다.

[0049] 보다 상세하게 예를 들어, 먼저 데이터 수집부(120)는 공격이 부재한 상황 하에서의 하드웨어의 활동에 관련된 데이터(이하 비공격 데이터(d1))를 수집하고, 이를 데이터 가공부(130)로 또는 훈련부(132)로 전달할 수 있다. 데이터 가공부(130)는 비공격 데이터(d1) 중에서 특정한 데이터(일례로 중요한 필드의 데이터)를 선별하고 선별된 데이터를 훈련부(132)로 전달할 수 있다. 훈련부(132)는 비공격 데이터(d1) 또는 비공격 데이터(d1)로부터 선별된 데이터를 학습 모델(109)에 입력함으로써 공격이 부재한 상황에 대해 학습 모델(109)을 훈련시킨다. 또한, 이에 선행하거나, 후행하거나 및/또는 동시에 데이터 수집부(120)는 모의 공격 하에서의 하드웨어의 활동에 대한 데이터(이하 모의 공격 데이터(d2))를 더 수집하고, 수집한 모의 공격 데이터(d2)를 데이터 가공부(130) 또는 훈련부(132)로 전달할 수도 있다. 데이터 가공부(130)는 상술한 바와 동일하게 또는 일부 변형된 형태로 모의 공격 데이터(d2)로부터 특정 필드의 데이터를 선별하고, 선별된 데이터를 훈련부(132)로 전달할 수 있다. 모의 공격 데이터(d2)로부터 선별된 데이터와 비공격 데이터(d1)로부터 선별된 데이터는 상호 대응할 수 있으며, 예를 들어, 동종의 데이터일 수 있다. 훈련부(132)는 모의 공격 데이터(d2) 또는 모의 공격 데이터(d2)로부터 선별된 데이터를 기반으로 모의 공격 상황에서의 학습 모델(109)에 대한 훈련을 수행한다. 이와 같은 과정에 의해, 공격이 존재하는 상황에서 하드웨어가 어떻게 동작하는지 또는 공격이 부재한 상황에서 하드웨어가 어떻게 동작하는지를 파악하여 공격 여부를 탐지할 수 있도록 훈련된 학습 모델(109a)이 획득 가능하게 된다. 훈련된 학습 모델(109a)은 비공격 데이터(d1, 또는 비공격 데이터(d1)로부터 선별된 데이터) 및/또는 모의 공격 데이터(d2, 또는 모의 공격 데이터(d2)로부터 선별된 데이터)의 반복적 입력에 의해 지속적으로 훈련될 수 있다. 또한, 훈련된 학습 모델(109a)은 후술하는 캐시 부채널 공격의 탐지 과정에서도 더 훈련될 수도 있다.

[0050] 일 실시예에 의하면, 훈련부(132)는 서로 상이한 다수의 학습 모델(109)을 훈련시키는 것도 가능하다. 여기서, 서로 상이한 다수의 학습 모델(109)은 이종의 학습 모델(들)을 기반으로 구현된 것일 수도 있고, 동종의 학습 모델을 기반으로 구현된 것일 수도 있다. 예를 들어, 훈련부(132)는 다수의 학습 모델(109) 각각을 비공격 데이터(d1, 또는 비공격 데이터(d1)로부터 선별된 데이터) 및 모의 공격 데이터(d2, 또는 모의 공격 데이터(d2)로부터 선별된 데이터)를 이용하여 훈련시킬 수 있다. 실시예에 따라서, 훈련부(132)는 각각의 학습 모델(109)의 훈련 과정에서 판단된 각 학습 모델(109)의 정확도(즉, 비공격 또는 모의 공격 여부에 대한 정답율 등)를 기반으로 각 학습 모델(109)을 비교 평가하여 정확도가 우수한 학습 모델(109)을 하나 이상 선별하거나, 및/또는 정확도에 따라 순차적으로 각 학습 모델(109)에 대한 순위를 결정 및 부가할 수도 있다.

[0051] 도 4는 학습 모델 기반 탐지 과정의 일례를 설명하기 위한 도면이다.

[0052] 도 4에 도시된 바와 같이 일 실시예에 따르면, 탐지부(134)는 데이터 수집부(120) 또는 데이터 가공부(130)로부터 공격 발생 여부 탐지를 위한 데이터(이하 현재 데이터(d3))를 수신하고, 훈련된 모델(109a)을 이용하여 캐시 부채널 공격의 발생 여부를 탐지하고 탐지 결과(139)를 획득할 수 있다.

[0053] 구체적으로 데이터 수집부(120)는 코어(91: 91-1, 91-2), L1 캐시(92: 92-1, 92-2), L2 캐시(93) 및 L3 캐시(94) 중 적어도 하나로부터 공격 탐지를 위한 현재 데이터(d3)를 수집하고, 수집한 현재 데이터(d3)를 데이터 가공부(130)로 또는 훈련부(132)로 전달할 수 있다. 데이터 가공부(130)는 현재 데이터(d3)를 가공하고 이를 탐지부(134)로 전달할 수 있으며, 예를 들어 현재 데이터(d3) 중에서 필요도나 중요도가 높은 필드의 데이터 등과 같은 소정의 데이터를 선별하고 선별된 데이터를 탐지부(134)로 전달할 수 있다. 실시예에 따라 데이터 수집부(120) 또는 데이터 가공부(130)가 획득한 데이터는 훈련부(132)로도 함께 전달될 수도 있다. 탐지부(134)는 데이터 수집부(120)가 획득한 현재 데이터(d3)나 현재 데이터(d3) 중에서 데이터 가공부(130)에 의해 선별된 데이터를 훈련된 학습 모델(109a)에 입력할 수 있다. 훈련된 학습 모델(109)은 입력 받은 데이터(d3 등)를 기반으로 입력 받은 데이터(d3 등)에 대응하는 탐지 결과(139)를 획득할 수 있다. 이때, 만약 프로세서 등의 하드웨어에 캐시 부채널 공격이 존재하는 경우라면, 훈련된 학습 모델(109a)은 입력 받은 데이터(d3 등)에 대응하여 공격이 발생하였다는 탐지 결과(139)를 출력하고, 반대로 하드웨어에 캐시 부채널 공격이 부재한 경우라면, 훈련된 학습 모델(109a)에는 캐시 부채널 공격이 존재하는 경우와 상이한 데이터(d3 등)가 입력되며, 이에 대응하여 훈련된 학습 모델(109a)은 공격이 없다는 탐지 결과(139)를 출력하게 된다. 훈련부(132)는 실시예에 따라 생략될 수도 있으며, 이 경우, 탐지부(134)는 입력부(101) 등을 통해 다른 정보 처리 장치나 메모리 장치로부터 훈련된 학습 모델(109a)을 획득할 수도 있다.

- [0054] 이와 같이 탐지부(134)는 사전에 훈련된 학습 모델(109a)을 기반으로 탐지를 수행하기 때문에 캐시 부채널 공격이 종료되기 전에 캐시 부채널 공격 탐지의 전 과정이 처리될 수 있으며, 이에 따라 캐시 부채널 공격에 대한 실시간 탐지가 가능해진다.
- [0055] 상술한 캐시 부채널 공격 탐지 장치(100)는 설계자나 사용자의 선택에 따라 캐시 부채널 공격의 대상이 되는 적어도 하나의 정보 처리 장치를 이용하여 구현되거나 및/또는 캐시 부채널 공격의 대상이 되는 정보 처리 장치와 통신 가능하게 연결된 다른 적어도 하나의 정보 처리 장치를 이용하여 구현될 수 있다. 여기서, 적어도 하나의 정보 처리 장치는, 예를 들어, 데스크톱 컴퓨터, 랩톱 컴퓨터, 스마트 폰, 태블릿 피씨, 스마트 시계, 두부 장착형 디스플레이(HMD: Head Mounted Display) 장치, 내비게이션 장치, 휴대용 게임기, 디지털 텔레비전, 셋톱박스, 가전 기기(냉장고나 로봇 청소기 등), 인공 지능 음향 재생 장치(인공 지능 스피커), 차량, 유인 또는 무인 비행체, 로봇, 산업용 기계 또는 전자 광고판 등을 포함할 수 있으나, 이에 한정되는 것은 아니다. 상술한 캐시 부채널 공격 탐지 방법이 하드웨어적으로 구현될 수 있거나 또는 설계자 또는 사용자의 임의적 선택에 따라서 상술한 캐시 부채널 공격 탐지 방법을 위한 프로그램이 설치 및 탑재 가능한 다양한 정보 처리 장치가 상술한 캐시 부채널 공격 탐지 장치(100)로 적용될 수 있다.
- [0056] 이하 도 5를 참조하여 캐시 부채널 공격 탐지 방법의 일 실시예를 설명한다.
- [0057] 도 5는 캐시 부채널 공격 탐지 방법의 일 실시예에 대한 흐름도이다.
- [0058] 도 5에 도시된 바에 의하면, 먼저 프로세서 등과 같은 하드웨어로부터 비공격 데이터 및 모의 공격 데이터 중 적어도 하나가 수집 및 획득될 수 있다(200). 이 경우, 비공격 데이터 및 모의 공격 데이터는 순차적으로 또는 교차적으로 수집될 수 있다. 여기서, 모의 공격 데이터의 획득을 위한 모의 공격은 설계자 또는 사용자 등에 의해 수행된 것일 수 있다. 비공격 데이터 또는 모의 공격 데이터는 중앙처리장치 등의 코어, L1 캐시, L2 캐시 및 L3 캐시 중 적어도 하나로부터 획득될 것일 수 있으며, 장치에 복수의 코어, 복수의 L1 캐시, 복수의 L2 캐시 및/또는 복수의 L3 캐시가 마련되어 있다면, 비공격 데이터 또는 모의 공격 데이터는 모든 코어, 모든 L1 캐시, 모든 L2 캐시 및/또는 모든 L3 캐시로부터 획득될 것일 수도 있고, 또는 일부의 코어, 일부의 L1 캐시, 일부의 L2 캐시 및/또는 일부의 L3 캐시로부터 획득될 것일 수도 있다. 비공격 데이터 및/또는 모의 공격 데이터의 획득은 하드웨어 성능 카운터(일례로 특별히 고안된 일 군의 레지스터)를 이용하여 수행될 수 있으며, 필요에 따라 성능 카운터 감시부 등과 같은 소정의 프로그램을 더 이용하여 수행될 수도 있다.
- [0059] 수집된 비공격 데이터 및 모의 공격 데이터는 필요에 따라 더 가공될 수도 있다(202). 예를 들어, 수집된 모든 또는 일부의 비공격 데이터와 모든 또는 일부의 모의 공격 데이터 각각에 대한 분석을 통해, 모든 또는 일부의 비공격 데이터와 모든 또는 일부의 모의 공격 데이터 각각으로부터 필요도나 중요도가 높은 데이터가 선별될 수 있다. 데이터의 선별은 상관 관계 분석을 기반으로 수행될 수도 있다. 데이터에 대한 가공 과정(202)은 실시예에 따라 생략 가능하다.
- [0060] 이어서, 비공격 데이터 및 모의 공격 데이터를 이용하거나 및/또는 가공된 데이터를 이용하여 적어도 하나의 학습 모델이 훈련될 수 있다(204). 이에 따라 적어도 하나의 훈련된 학습 모델이 획득된다. 여기서, 학습 모델은, 예를 들어, 다층 퍼셉트론, 서포트 벡터 머신, 심층 신경망, 콘볼루션 신경망, 순환 신경망, 심층 신뢰 신경망, 심층 Q-네트워크, 장단기 메모리, 생성적 적대 신경망 및/또는 조건적 생성적 적대 신경망 등과 같은 적어도 하나의 기계 학습 모델을 포함할 수 있다.
- [0061] 상술한 데이터 수집 내지 학습 모델 훈련 과정(200 내지 204)은 상황, 조건 또는 설계자의 임의적 선택 등에 따라서 비공격 데이터에 대해 먼저 수행된 후 순차적으로 모의 공격 데이터에 대해 수행될 수도 있고, 모의 공격 데이터에 대해 먼저 수행된 후 순차적으로 비공격 데이터에 대해 수행될 수도 있으며, 비공격 데이터 및 모의 공격 데이터에 대해 동시에 수행될 수도 있고, 또는 데이터의 종류와 무관하게 임의적으로 수행될 수도 있다.
- [0062] 현재 데이터가 수집 및 획득된다(208). 현재 데이터의 수집은 상술한 비공격 데이터 또는 모의 공격 데이터의 수집과 동일하게 또는 일부 상이한 방법을 통해 수행될 수 있다. 예를 들어, 현재 데이터는 적어도 하나의 코어, 적어도 하나의 L1 캐시, 적어도 하나의 L2 캐시 및/또는 적어도 하나의 L3 캐시로부터 하드웨어 성능 카운터를 이용하거나 성능 카운터 감시부 등을 더 이용하여 획득될 것일 수 있다.
- [0063] 수집된 현재 데이터도 가공될 수 있다(210). 만약 비공격 데이터 또는 모의 공격 데이터가 가공된 후 학습 모델의 훈련에 이용되었다면, 이에 대응하여 수집된 현재 데이터도 가공되어 학습 모델에 이용될 수 있다. 현재 데이터의 가공은, 예를 들어, 상관 관계 분석을 기반으로 하는 데이터 선별을 포함할 수 있다.

- [0064] 순차적으로, 수집된 현재 데이터 또는 가공된 현재 데이터를 이용하여 캐시 부채널 공격의 탐지가 진행된다(212). 캐시 부채널 공격의 탐지는 수집된 현재 데이터 또는 가공된 현재 데이터를 상술한 바와 같이 훈련된 학습 모델에 적용함으로써 수행될 수 있다. 이에 따라 현재 데이터 또는 가공된 현재 데이터에 대응하는 캐시 부채널 공격의 존재 여부가 판단되게 된다.
- [0065] 탐지 결과는 시각적 또는 청각적으로 외부로 출력되거나 필요에 따라 외부의 다른 전자 장치나 디스플레이 장치 등으로 전달될 수 있다(214). 또한, 탐지 결과는 출력 또는 전달 전에 일시적 또는 비일시적으로 저장부에 저장될 수도 있다.
- [0066] 상술한 비공격 데이터/모의 공격 데이터의 수집 내지 학습 모델 훈련 과정(200 내지 204)과 상술한 현재 데이터 수집 내지 탐지 수행 과정(208 내지 212)은 실시예에 따라 동일한 정보 처리 장치에 의해 처리될 수도 있고, 또는 서로 상이한 정보 처리 장치에 의해 처리될 수도 있다. 이 경우, 서로 상이한 정보 처리 장치는 통신 가능하게 연결된 것일 수 있으며, 하나 또는 둘 이상의 정보 처리 장치는 비공격 데이터/모의 공격 데이터의 수집 내지 학습 모델 훈련 과정(200 내지 204)을 수행하여 훈련된 학습 모델을 획득하고, 훈련된 학습 모델을 하나 또는 둘 이상의 다른 정보 처리 장치로 전달하고, 하나 또는 둘 이상의 다른 정보 처리 장치는 훈련된 학습 모델을 이용하여 상술한 현재 데이터 수집 내지 탐지 수행 과정(208 내지 212)을 수행할 수도 있다.
- [0067] 상술한 실시예에 따른 캐시 부채널 공격 탐지 방법은 컴퓨터 장치에 의해 구동될 수 있는 프로그램의 형태로 구현될 수 있다. 여기서 프로그램은 프로그램 명령, 데이터 파일 및 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 프로그램은 기계어 코드나 고급 언어 코드를 이용하여 설계 및 제작된 것일 수 있다. 프로그램은 상술한 방법을 구현하기 위하여 특별히 설계된 것일 수도 있고, 컴퓨터 소프트웨어 분야에서 통상의 기술자에게 공지되어 사용 가능한 각종 함수나 정의를 이용하여 구현된 것일 수도 있다. 또한, 여기서, 컴퓨터 장치는 프로그램의 기능을 실현 가능하게 하는 프로세서나 메모리 등을 포함하여 구현된 것일 수 있으며, 필요에 따라 통신 장치를 더 포함할 수도 있다.
- [0068] 상술한 캐시 부채널 공격 탐지 방법을 구현하기 위한 프로그램은 컴퓨터에 의해 판독 가능한 기록 매체에 기록될 수 있다. 컴퓨터에 의해 판독 가능한 기록 매체는, 예를 들어, 솔리드 스테이트 드라이브(SSD), 롬, 램 또는 플래시 메모리 등과 같은 반도체 저장 장치, 하드 디스크나 플로피 디스크 등과 같은 자기 디스크 저장 매체, 콤팩트 디스크나 디브이디 등과 같은 광 기록 매체, 플롭티컬 디스크 등과 같은 자기-광 기록 매체 및 자기 테이프 등 컴퓨터 등의 호출에 따라 실행되는 특정 프로그램을 저장 가능한 적어도 한 종류의 물리적 장치를 포함할 수 있다.
- [0069] 이상 캐시 부채널 공격 탐지 장치 및 방법의 여러 실시예에 대해 설명하였으나, 캐시 부채널 공격 탐지 장치 및 방법은 오직 상술한 실시예에 한정되는 것은 아니다. 해당 기술 분야에서 통상의 지식을 가진 자가 상술한 실시예를 기초로 수정 및 변형하여 구현 가능한 다양한 장치나 방법 역시 상술한 캐시 부채널 공격 탐지 장치 및 방법의 일례가 될 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나 다른 구성 요소 또는 균등물에 의하여 대치되거나 또는 치환되더라도 상술한 캐시 부채널 공격 탐지 장치 및 방법의 일 실시예가 될 수 있다.
- [0070] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 컨트롤러, 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(Operation System, 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 기술 분야에서 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 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.
- [0071] 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, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 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.

[0072] 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), 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

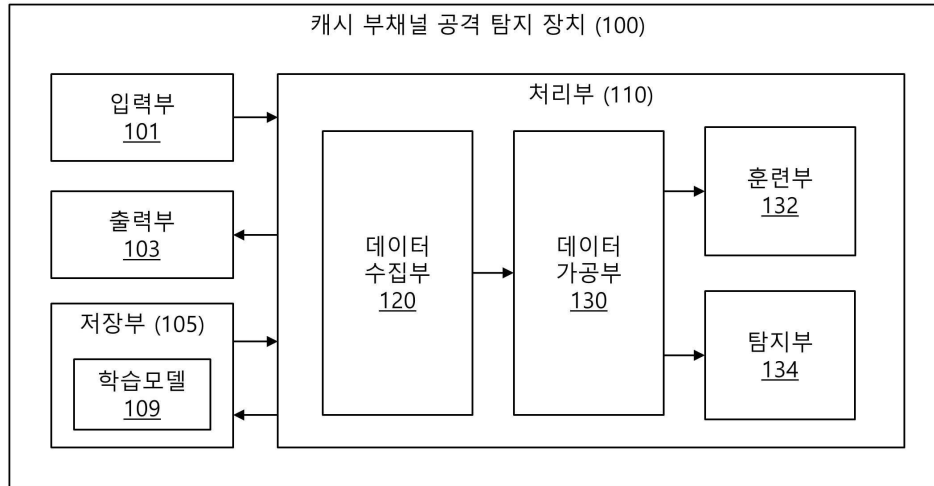
[0073] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

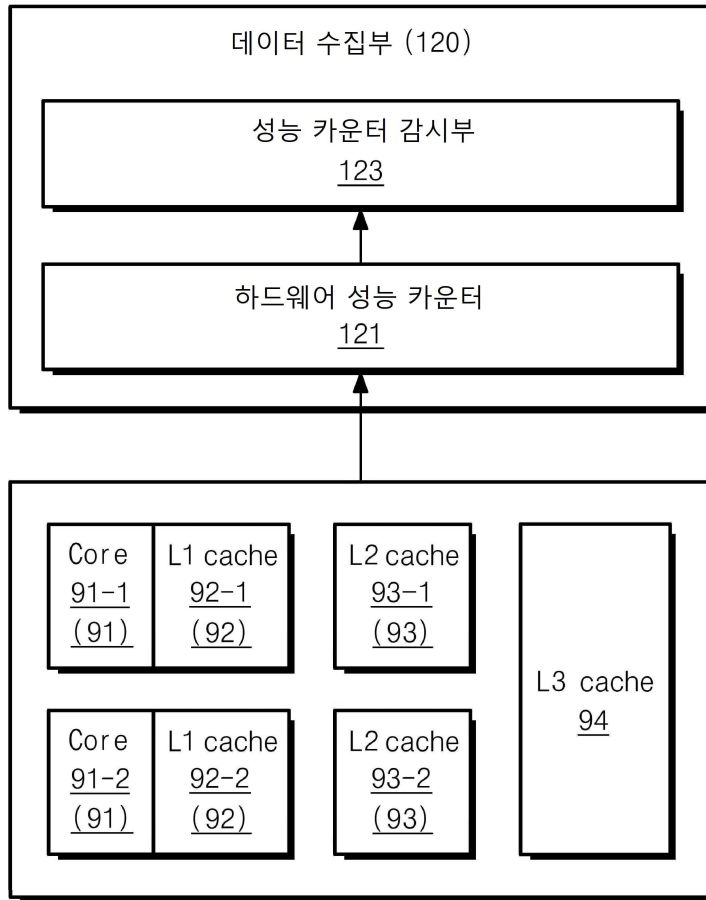
[0074] 91: 코어 92: L1 캐시
93: L2 캐시 94: L3 캐시
100: 캐시 부채널 공격 탐지 장치 101: 입력부
103: 출력부 105: 저장부
109: 학습모델 110: 처리부
120: 데이터 수집부 121: 하드웨어 성능 카운터
123: 성능 카운터 감시부 130: 데이터 가공부
132: 훈련부 134: 탐지부

도면

도면1



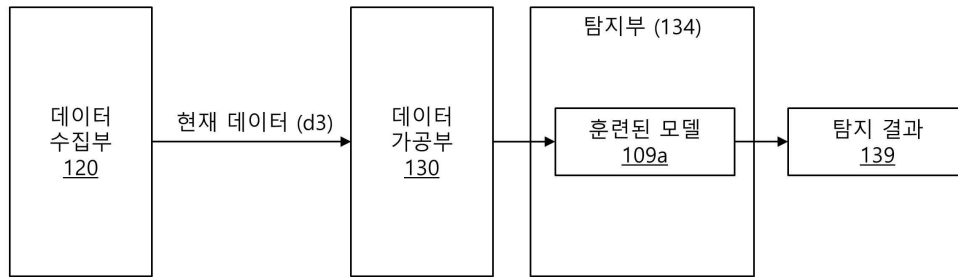
도면2



도면3



도면4



도면5

