(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0106488
(43) 공개일자 2019년09월18일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
H04L 67/1008 (2013.01)
H04L 63/1441 (2013.01)
(21) 출원번호 10-2018-0028042
(22) 출원일자 2018년03월09일
심사청구일자 2018년03월09일

(71) 출원인
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
백웅기
울산광역시 울주군 언양읍 유니스트길 50 울산과학기술대학교
한명균
울산광역시 울주군 언양읍 유니스트길 50 울산과학기술대학교
유성대
울산광역시 울주군 언양읍 유니스트길 50 울산과학기술대학교
(74) 대리인
제일특허법인(유)

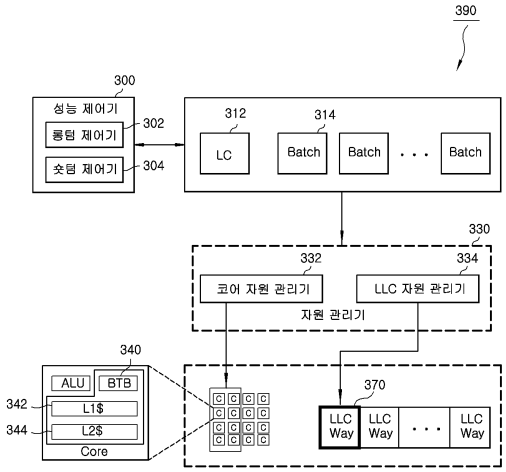
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **통합 서버의 자원 분배 관리장치 및 방법**

(57) 요 약

본 발명의 일실시예에 따르면, 가상머신 또는 컨테이너 기반 통합 서버의 자원 분배 관리에 있어서, 통합 서버의 실시간 작업으로 요청된 QoS를 만족시킬 수 있도록 하드웨어 자원을 동적으로 분배하여 자원 활용성을 높이며, 보안이 설정된 작업에 대해서는 하드웨어 자원의 분배 전에 기저장된 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 외부 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있다.

대 표 도 - 도3



(52) CPC특허분류
H04L 67/1076 (2013.01)
H04L 67/322 (2013.01)
H04L 2209/08 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711058252
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 SW전문인력역량강화
연구과제명 Peta Flops 스케일의 기계학습 프레임워크 개발
기 여 율 1/2
주관기관 울산과학기술원
연구기간 2017.08.01 ~ 2018.05.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711056733
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 SW컴퓨팅산업원천기술개발
연구과제명 빅데이터 처리 고도화 핵심기술개발 사업 총괄 및 고성능 컴퓨팅 기술을 활용한 성능 가속화 기술 개발
기 여 율 1/2
주관기관 울산과학기술원
연구기간 2017.06.01 ~ 2018.03.31

명 세 서

청구범위

청구항 1

통합 서버로 요청된 실시간 (latency-critical) 작업과 배치(batch) 작업을 모니터링하고, 상기 모니터링한 정보를 기반으로 실시간 작업에 대해 기설정된 QoS가 만족되도록 상기 통합 서버에 구비된 하드웨어 자원을 상기 실시간 작업과 상기 배치 작업에 동적으로 분배하는 성능 제어기와,

상기 실시간 작업 또는 상기 배치 작업이 보안이 설정된 작업인지 여부를 검사하고, 상기 보안이 설정된 경우 상기 실시간 작업 또는 상기 배치 작업에 분배된 하드웨어 자원의 재분배시 상기 재분배되는 하드웨어 자원에 저장된 데이터를 제3자가 인식할 수 없도록 보안 처리하는 자원 관리기를 포함하는

통합 서버의 자원 분배 관리장치.

청구항 2

제 1 항에 있어서,

상기 성능 제어기는,

소정의 주기로 상기 실시간 작업의 응답 속도를 측정하고, 상기 측정된 응답 속도와 상기 실시간 작업의 부하를 고려하여 상기 배치 작업에 분배되는 상기 하드웨어 자원의 양을 늘릴 것인지 여부를 결정하는 롱텀 제어기와,

상기 배치 작업에 상기 하드웨어 자원의 양을 늘리기로 결정된 경우, 상기 실시간 작업의 QoS가 만족되도록 상기 배치 작업에 새로이 분배할 코어 프로세서의 개수와 LLC way 개수를 설정하는 숏텀 제어기를 포함하는

통합 서버의 자원 분배 관리장치.

청구항 3

제 1 항에 있어서,

상기 자원 관리기는,

상기 재분배되는 하드웨어 자원 중 L1과 L2 캐시 및 BTB에 저장된 데이터에 대한 보안 처리를 수행하는 코어 자원 관리기와,

상기 재분배되는 하드웨어 자원 중 LLC 캐시에 대해서는 작업별 LLC way의 개수를 지정하고, 분배 대상 작업에 지정된 LLC way에 저장된 데이터 대한 보안 처리를 수행하는 LLC 자원 관리기를 포함하는

통합 서버의 자원 분배 관리장치.

청구항 4

제 3 항에 있어서,

상기 코어 자원 관리기는,

상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키며, 상기 BTB에 더미 데이터를 저장시켜 상기 보안 처리를 수행하는

통합 서버의 자원 분배 관리장치.

청구항 5

제 4 항에 있어서,

상기 코어 자원 관리기는,

wbinvd 명령어를 사용하여 상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는

통합 서버의 자원 분배 관리장치.

청구항 6

제 3 항에 있어서,

상기 LLC 자원 관리기는,

상기 분배 대상 작업에 지정된 상기 LLC way에 더미 데이터를 저장시켜 상기 보안 처리를 수행하는

통합 서버의 자원 분배 관리장치.

청구항 7

제 6 항에 있어서,

상기 LLC 자원 관리기는,

Intel CAT 기능을 이용하여 상기 LLC way에 더미 데이터를 저장시키는

통합 서버의 자원 분배 관리장치.

청구항 8

제 1 항에 있어서,

상기 실시간 작업은, 상기 통합 서버에서 기설정된 기준 시간 이내에 요청을 처리하도록 설정된 작업이며,

상기 배치 작업은, 상기 기준 시간에 관계 없이 처리하도록 설정된 작업인

통합 서버의 자원 분배 관리장치.

청구항 9

제 1 항에 있어서,

상기 통합 서버는,

가상 머신 기반 또는 컨테이너 기반에서 상기 하드 웨어 자원이 공유되도록 구현되는 서버인

통합 서버의 자원 분배 관리장치.

청구항 10

통합 서버에서 실행되는 실시간 작업과 배치 작업을 모니터링하는 단계와,

상기 모니터링한 정보를 기반으로 상기 실시간 작업의 기설정된 QoS가 만족되도록 상기 통합 서버에 구비된 하드웨어 자원을 상기 실시간 작업과 상기 배치 작업에 동적으로 분배하는 단계와,

상기 실시간 작업 또는 상기 배치 작업이 보안이 설정된 작업인지 여부를 검사하는 단계와,

상기 보안이 설정된 경우, 상기 실시간 작업 또는 상기 배치 작업에 분배된 하드웨어 자원의 재분배시 상기 재분배되는 하드웨어 자원에 저장된 데이터를 제3자가 인식할 수 없도록 보안 처리하는 단계를 포함하는

통합 서버의 자원 분배 관리방법.

청구항 11

제 10 항에 있어서,

상기 동적으로 분배하는 단계는,

소정의 주기로 상기 실시간 작업의 응답 속도를 측정하는 단계와,

상기 측정된 응답 속도와 상기 실시간 작업의 부하를 고려하여 상기 배치 작업에 분배되는 상기 하드웨어 자원의 양을 늘릴 것인지 여부를 결정하는 단계와,

상기 배치 작업에 상기 하드웨어 자원의 양을 늘리기로 결정한 경우, 상기 실시간 작업의 QoS가 만족되도록 상기 배치 작업에 새로이 분배할 코어 프로세서의 개수와 LLC way 개수를 설정하는 단계를 포함하는

통합 서버의 자원 분배 관리방법.

청구항 12

제 10 항에 있어서,

상기 보안 처리하는 단계는,

상기 재분배되는 하드웨어 자원 중 L1과 L2 캐시 및 BTB에 저장된 데이터에 대한 제1 보안 처리를 수행하는 단계와,

상기 재분배되는 하드웨어 자원 중 LLC 캐시에 대해서는 작업별 LLC way의 개수를 지정하는 단계와,

분배 대상 작업에 지정된 상기 LLC way에 저장된 데이터 대한 제2 보안 처리를 수행하는 단계를 포함하는

통합 서버의 자원 분배 관리방법.

청구항 13

제 12 항에 있어서,

상기 제1 보안 처리를 수행하는 단계는,

기설정된 명령어를 사용하여 상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는 단계와,

상기 BTB에 더미 데이터를 저장시키는 단계를 포함하는

통합 서버의 자원 분배 관리방법.

청구항 14

제 12 항에 있어서,

상기 제2 보안 처리를 수행하는 단계는,

상기 분배 대상 작업에 지정된 상기 LLC way에 더미 데이터를 저장시키는 단계인

통합 서버의 자원 분배 관리방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 가상머신 또는 컨테이너 기반 통합 서버의 자원 분배에 있어서, 특히 통합 서버의 실시간 작업으로 요청된 QoS를 만족시킬 수 있도록 하드웨어 자원을 실시간 작업과 배치 작업에 동적으로 분배하며, 보안이 설정된 작업에 대해서는 하드웨어 자원의 분배 전에 기저장된 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 사이드 채널 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있도록 하는 가상머신 또는 컨테이너기반 통합 서버의 자원 분배 관리장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 서버 통합(server consolidation)는 하드웨어 자원(hardware resource)을 여러 서버에서 공유하여 사용함으로써 자원의 효율성을 높이고자 하는 기술로, 큰규모의 데이터 센터(data center)나 클라우드(cloud) 환경에서 서버 자원의 활용성(utilization)을 최대화하기 위해 널리 사용되고 있다.

[0003] 그러나, 종래 서버 통합 기술이 적용된 통합 서버에서는 실시간(latency-critical) 작업과 배치(batch) 작업이 동일한 서버에 설행됨에 따라, 자원 활용성(resoure utilization)은 높아지지만 하드웨어 자원 공유로 인한 성능 간섭현상으로 인해 실시간 작업의 QoS(Quality of Service)를 보장하기 힘든 문제점이 있다.

[0004] 또한, 종래 서버 통합 기술에는 동적으로 하드웨어 자원이 분배될 때 공유되는 하드웨어 자원의 상태 정보를 통해 외부 공격자(attacker)가 공격 대상자(victim)의 특정 코드 또는 데이터의 접근 여부를 알아내는 사이드 채

널(side-channel) 공격 등에 취약한 문제점이 있다.

[0005] 이때, 사이드 채널 공격이라 함은 예를 들어, 도 1에서와 같이 공격자(attacker)(100)가 공유되는 캐시자원(120, 122)을 선점하여 미리 일정 데이터를 저장하여 놓은 상태에서, 도 2에서 보여지는 바와 같이 공격 대상자(victim)(150)가 자원 공유를 통해 캐시 자원(122)의 특정 캐시(170)에 저장된 데이터를 삭제하고 자신의 데이터를 저장하는 경우 공격자(100)의 캐시 사용을 인식하여 공격 대상자(170)의 데이터를 탈취하는 방법으로, 통합 서버에서 공유 하드웨어 자원 분배 과정에서의 취약점을 이용하는 공격 중 하나이다.

[0006] 이와 같이 종래에는 통합 서버의 자원 분배 과정에서의 취약점을 이용한 사이드 채널 공격 등과 같은 외부 공격의 위험성이 존재하여 실시간 작업의 QoS를 보장하며, 자원 활용성과 보안성을 모두 충족시키는 자원 분배 구현이 어려운 문제점이 있었다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 공개특허번호 10-2016-0050896호(공개일자 2016년 05월 11일)

발명의 내용

해결하려는 과제

[0008] 따라서, 본 발명의 일실시예에서는 통합 서버의 실시간 작업으로 요청된 QoS를 만족시킬 수 있도록 하드웨어 자원을 동적으로 분배하며, 보안이 설정된 작업에 대해서는 하드웨어 자원의 분배 전에 기저장된 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 외부 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있도록 하는 가상머신 또는 컨테이너 기반 통합 서버의 자원 분배 관리장치 및 방법을 제공하고자 한다.

과제의 해결 수단

[0009] 상술한 본 발명의 일실시예에 따른 통합 서버의 자원 분배 관리장치로서, 통합 서버로 요청된실시간(latency-critical) 작업과 배치(batch) 작업들을 모니터링하고, 상기 모니터링한 정보를 기반으로 실시간 작업에 대해 기설정된 QoS가 만족되도록 상기 통합 서버에 구비된 하드웨어 자원을 상기 실시간 작업과 배치 작업에 동적으로 하드웨어 자원을 분배하는 성능 제어기와, 상기 실시간 작업 또는 상기 배치 작업이 보안이 설정된 작업인지 여부를 검사하고, 상기 보안이 설정된 경우 상기 실시간 작업 또는 상기 배치 작업에 분배된 하드웨어 자원의 재분배시 상기 재분배되는 하드웨어 자원에 저장된 데이터를 제3자가 인식할 수 없도록 보안 처리하는 자원 관리기를 포함한다.

[0010] 또한, 상기 성능 제어기는, 소정의 주기로 상기 실시간 작업의 응답 속도를 측정하고, 상기 측정된 응답 속도와 상기 실시간 작업의 부하를 고려하여 상기 배치 작업에 분배되는 상기 하드웨어 자원의 양을 늘릴 것인지 여부를 결정하는 롱텀 제어기와, 상기 배치 작업에 상기 하드웨어 자원의 양을 늘리기로 결정된 경우, 상기 QoS가 만족되도록 상기 배치 작업에 새로이 분배할 코어 프로세서의 개수와 LLC way 개수를 설정하는 숏텀 제어기를 포함하는 것을 특징으로 한다.

[0011] 또한, 상기 자원 관리기는, 상기 재분배되는 하드웨어 자원 중 L1과 L2 캐시 및 BTB에 저장된 데이터에 대한 보안 처리를 수행하는 코어 자원 관리기와, 상기 재분배되는 하드웨어 자원 중 LLC 캐시에 대해서는 작업별 LLC way의 개수를 지정하고, 분배 대상 작업에 지정된 LLC way에 저장된 데이터 대한 보안 처리를 수행하는 LLC 자원 관리기를 포함하는 것을 특징으로 한다.

[0012] 또한, 상기 코어 자원 관리기는, 상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키며, 상기 BTB에 더미 데이터를 저장시켜 상기 보안 처리를 수행하는 것을 특징으로 한다.

[0013] 또한, 상기 코어 자원 관리기는, wbinvd 명령어를 사용하여 상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는 것을 특징으로 한다.

[0014] 또한, 상기 LLC 자원 관리기는, 상기 분배 대상 작업에 지정된 상기 LLC way에 더미 데이터를 저장시켜 상기 보안 처리를 수행하는 것을 특징으로 한다.

[0015] 또한, 상기 LLC 자원 관리기는, Intel CAT 명령어를 이용하여 상기 LLC way에 더미 데이터를 저장시키는 것을 특징으로 한다.

[0016] 또한, 상기 실시간 작업은, 상기 통합 서버에서 기설정된 기준 시간 이내에 요청을 처리하도록 설정된 작업이며, 상기 배치 작업은, 상기 기준 시간에 관계 없이 처리하도록 설정된 작업인 것을 특징으로 한다.

[0017] 또한, 상기 통합 서버는, 가상 머신 기반 또는 컨테이너 기반에서 상기 하드 웨어 자원이 공유되도록 구현되는 서버인 것을 특징으로 한다.

[0018] 또한, 본 발명의 일실시예에 따른 통합 서버의 자원 분배 관리방법으로서, 통합 서버에서 실행되는 실시간 작업과 배치 작업을 모니터링하는 단계와, 상기 모니터링한 정보를 기반으로 실시간 작업의 기설정된 QoS가 만족되도록 상기 통합 서버에 구비된 하드웨어 자원을 상기 실시간 작업과 상기 배치 작업에 동적으로 분배하는 단계와, 상기 실시간 작업 또는 상기 배치 작업이 보안이 설정된 작업인지 여부를 검사하는 단계와, 상기 보안이 설정된 경우, 상기 실시간 작업 또는 상기 배치 작업에 분배된 하드웨어 자원의 재분배시 상기 재분배되는 하드웨어 자원에 저장된 데이터를 제3자가 인식할 수 없도록 보안 처리하는 단계를 포함한다.

[0019] 또한, 상기 동적으로 분배하는 단계는, 소정의 주기로 상기 실시간 작업의 응답 속도를 측정하는 단계와, 상기 측정된 응답 속도와 상기 실시간 작업의 부하를 고려하여 상기 배치 작업에 분배되는 상기 하드웨어 자원의 양을 늘릴 것인지 여부를 결정하는 단계와, 상기 배치 작업에 상기 하드웨어 자원의 양을 늘리기로 결정한 경우, 상기 실시간 작업의 QoS가 만족되도록 상기 배치 작업에 새로이 분배할 코어 프로세서의 개수와 LLC way 개수를 설정하는 단계를 포함하는 것을 특징으로 한다.

[0020] 또한, 상기 보안 처리하는 단계는, 상기 재분배되는 하드웨어 자원 중 L1과 L2 캐시 및 BTB에 저장된 데이터에 대한 제1 보안 처리를 수행하는 단계와, 상기 재분배되는 하드웨어 자원 중 LLC 캐시에 대해서는 작업별 LLC way의 개수를 지정하는 단계와, 분배 대상 작업에 지정된 상기 LLC way에 저장된 데이터 대한 제2 보안 처리를 수행하는 단계를 포함하는 것을 특징으로 한다.

[0021] 또한, 상기 제1 보안 처리를 수행하는 단계는, 기설정된 명령어를 사용하여 상기 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는 단계와, 상기 BTB에 더미 데이터를 저장시키는 단계를 포함하는 것을 특징으로 한다.

[0022] 또한, 상기 제2 보안 처리를 수행하는 단계는, 상기 분배 대상 작업에 지정된 상기 LLC way에 더미 데이터를 저장시키는 단계인 것을 특징으로 한다.

발명의 효과

[0023] 본 발명의 일실시예에 따르면, 가상머신 또는 컨테이너 기반 통합 서버의 자원 분배 관리에 있어서, 통합 서버의 실시간 작업으로 요청된 QoS를 만족시킬 수 있도록 하드웨어 자원을 동적으로 분배하여 자원 활용성을 높이며, 보안이 설정된 작업에 대해서는 하드웨어 자원의 분배 전에 기저장된 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 외부 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있다.

도면의 간단한 설명

[0024] 도 1 내지 도 2는 종래 사이드 채널 공격 개념 예시도.

도 3은 본 발명의 일실시예에 따른 하드웨어 자원을 공유하는 통합 서버의 자원 분배 관리장치의 블록 구성도.

도 4는 본 발명의 일실시예에 따른 하드웨어 자원을 공유하는 통합 서버의 자원 분배 관리장치에서의 동작 제어 흐름도.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부된 도면을 참조하여 본 발명의 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운영자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0026] 도 3은 본 발명의 일실시예에 따른 하드웨어 자원을 공유하는 통합 서버의 자원 분배 관리장치의 블록 구성을 도시한 것이다.

[0027] 도 3을 참조하면, 본 발명의 일실시예에 따른 자원 분배 관리장치(390)는 성능 제어기(resource controller)(300), 자원 관리기(resource sanitizer)(330) 등을 포함할 수 있다.

[0028] 성능 제어기(300)는 통합 서버에서 실행되는 실시간 (latency-critical) 작업(312)과 배치(batch) 작업(314) 등을 모니터링(monitoring)하고, 모니터링한 정보를 기반으로 실시간 작업에 대해 기설정된 QoS가 만족되도록 통합 서버에 구비된 하드웨어 자원(hardware resource)을 실시간 작업(312)과 배치 작업(314)에 동적으로 분배한다.

[0029] 이때, 위와 같은 통합 서버는 가상 머신(virtual machine) 기반 또는 컨테이너(container) 기반에서 하드 웨어 자원이 공유되도록 구현되는 서버일 수 있으며, 성능 제어기(300)는 통합 서버에서 실행되는 실시간 작업과 배치 작업에 대해 주기적으로 모니터링을 수행하여, 통합 서버에서 하드웨어 자원이 가장 효율적으로 활용될 수 있도록 하드웨어 자원을 실시간 작업과 배치 작업에 동적으로 분배할 수 있다.

[0030] 여기서, 실시간 작업은 통합 서버에서 기설정된 기준 시간 이내에 요청을 처리하도록 설정된 작업으로 정의될 수 있으며, 이러한 실시간 작업은 예를 들어 웹서치(web search) 등이 될 수 있으나 이에 한정되는 것은 아니다. 이때, 웹서치는 예를 들어 사용자 단말(도시되지 않음)로부터 특정 키워드(keyword)에 대응되는 정보의 검색 요청을 수신하여 해당 키워드에 대응되는 정보를 검색하여 제공하는 작업을 의미할 수 있다. 또한, 배치 작업은 기준 시간에 관계 없이 처리하도록 설정된 작업으로 정의될 수 있으며, 예를 들어 머신 러닝(machine learning) 등과 같이 빨리 처리할 필요 없이 백그라운드(back ground)에서 오랫 동안 실행되는 것이 필요한 작업 등이 될 수 있다.

[0031] 또한, 하드웨어 자원이라 함은 통합 서버에 구비되는 코어 프로세서(core processor) 및 코어 프로세서에 할당되는 L1, L2, LLC(last level cache) way 캐시(cache), BTB(Branch Target Buffer) 등의 메모리 자원 등이 될 수 있으나, 이에 한정되는 것은 아니다.

[0032] 또한, 이러한 성능 제어기(300)는 롱텀 제어기(long-term controller)(302)와 숏텀 제어기(short-term controller)(304) 등을 포함할 수 있다.

[0033] 롱텀 제어기(302)는 예를 들어 소정의 주기마다 실시간 작업의 응답 속도를 측정할 수 있으며, 측정된 응답 속도와 실시간 작업의 현재 부하(load)를 고려하여 통합 서버의 전체 하드웨어 자원 분배 측면에서 배치 작업에 분배되는 하드웨어 자원의 양을 늘릴 것인지 여부를 결정할 수 있다.

[0034] 숏텀 제어기(304)는 롱텀 제어기(302)에서 통합 서버의 전체 하드웨어 자원 분배 측면을 고려하여 배치 작업에 분배되는 하드웨어 자원의 양을 늘리기로 결정한 경우, 통합 서버의 QoS가 만족되도록 배치 작업에 새로이 분배할 코어 프로세서의 개수, LLC way 개수 등을 설정할 수 있다. 이에 따라, 하드웨어 자원에 대한 재분배가 이루어질 수 있다.

[0035] 자원 관리기(330)는 실시간 작업 또는 배치 작업이 보안이 설정된 작업인지 여부를 검사하고, 보안이 설정된 작업에 대해서는 실시간 작업 또는 배치 작업에 분배된 하드웨어 자원의 재분배시, 해당 하드웨어 자원에 저장된 데이터를 제3자가 인식할 수 없도록 보안 처리한다.

[0036] 이때, 하드웨어 자원이 공유되는 통합 서버에서는 코어 프로세서 또는 L1, L2, LLC 등의 캐시가 재분배되는 과정에서 이전에 사용되었던 중요한 데이터가 사이드 채널(side-channel) 공격 등과 같은 외부 공격에 의해 탈취될 수 있는 위험이 있었음은 전술한 바와 같다. 이에 따라, 본 발명의 일실시예에 따른 자원 관리기(330)에서는 실시간 작업 또는 배치 작업에 분배되었던 하드웨어 자원를 재분배하는 경우 해당 하드웨어 자원에 기저장된 데이터를 제3자가 인식할 수 없도록 보안 처리한다.

[0037] 또한, 이러한 자원 관리기(330)는 코어 자원 관리기(core sanitizer)(332)와 LLC 자원 관리기(LLC sanitizer)(334) 등을 포함할 수 있다.

[0038] 먼저, 코어 자원 관리기(332)는 하드웨어 자원 중 L1과 L2 캐시 및 BTB 등에 저장된 데이터에 대한 보안 처리를 수행할 수 있다. 이때, 코어 자원 관리기(332)는 위와 같은 보안 처리를 수행함에 있어서, 예를 들어 L1과 L2 캐시에 대해서는 wbinvd 명령어를 사용하여 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는 방식으로 보안 처리를 수행할 수 있다. 또한, 코어 자원 관리기(332)는 BTB에 대해서는 현재 저장된 데이터 대신 더미값을 가지는 더미 데이터(dummy data)를 채워 넣는 방식으로 보안 처리를 수행할 수 있다.

[0039] 다음으로, LLC 자원 관리기(334)는 하드웨어 자원 중 LLC 캐시에 대해서는 코어 프로세서별 LLC way의 개수를

지정하고, 분배 대상 코어 프로세서에 지정된 LLC way에 저장된 데이터 대한 보안 처리를 수행할 수 있다.

[0040] 이때, LLC 자원 관리기(334)는 위와 같은 보안 처리를 수행함에 있어서, 예를 들어 Intel CAT 기능 등을 사용하여 분배 대상 코어 프로세서에 지정된 상기 LLC way(370)에 더미 데이터를 저장시켜 보안 처리를 수행할 수 있다.

[0041] 도 4는 본 발명의 일실시예에 따른 하드웨어 자원을 공유하는 통합 서버의 자원 분배 관리장치에서 QoS와 보안성을 고려하여 자원을 동적으로 분배하는 동작 제어 흐름을 도시한 것이다.

[0042] 먼저 자원 분배 관리장치(390)는 통합 서버로 요청된 실시간 작업과 배치 작업을 모니터링하고(S400), 모니터링한 정보를 기반으로 기설정된 QoS가 만족되도록 통합 서버에 구비된 하드웨어 자원을 실시간 작업과 배치 작업에 동적으로 분배한다(S402).

[0043] 이때, 위와 같은 통합 서버는 가상 머신 기반 또는 컨테이너 기반에서 상기 하드 웨어 자원이 공유되도록 구현되는 서버일 수 있으며, 자원 분배 관리장치(390)는 통합 서버에 생성된 크리티컬 작업과 배치 작업에 대해 주기적으로 모니터링을 수행하여, 통합 서버에서 하드웨어 자원이 가장 효율적으로 활용될 수 있도록 하드웨어 자원을 실시간 작업과 배치 작업에 동적으로 분배하는 것이다.

[0044] 또한, 자원 분배 관리장치(390)는 위와 같은 하드웨어 자원의 동적 분배 동작에 있어서, 예를 들어 소정의 주기마다 실시간 작업의 응답 속도를 측정하고, 측정된 응답 속도와 통합 서버의 현재 부하(load)를 고려하여 통합 서버의 전체 하드웨어 자원 분배 측면에서 배치 작업에 분배되는 하드웨어 자원의 양을 늘릴 것인지 여부를 결정할 수 있다. 이어, 배치 작업에 분배되는 하드웨어 자원의 양을 늘리기로 결정한 경우, 통합 서버의 QoS가 만족되도록 배치 작업에 새로이 분배할 코어 프로세서의 개수와 LLC way 개수 등을 설정하는 것을 통해 하드웨어 자원의 동적 분배를 수행할 수 있다.

[0045] 이어, 자원 분배 관리장치(390)는 실시간 작업 또는 배치 작업이 보안이 설정된 작업인지 여부를 검사한다(S404).

[0046] 이때, 하드웨어 자원이 공유되는 통합 서버에서는 코어 프로세서 또는 L1, L2, LLC 등의 캐시가 재분배되는 과정에서 이전에 사용되었던 중요한 데이터가 side-channel 공격 등과 같은 외부 공격에 의해 탈취될 수 있는 위험성이 있다.

[0047] 이에 따라, 자원 분배 관리장치(390)는 실시간 작업 또는 배치 작업이 보안이 설정된 경우에는(S406), 해당 실시간 작업 또는 배치 작업에 분배되었던 하드웨어 자원의 재분배시 해당 하드웨어 자원을 재분배하기 전에 해당 하드웨어 자원에 기저장된 데이터를 제3자가 인식할 수 없도록 보안 처리를 수행한다(S408).

[0048] 이때, 자원 분배 관리장치(390)는 보안 처리를 수행함에 있어서, 예를 들어 하드웨어 자원 중 L1과 L2 캐시에 대해서는 wbinvd 명령어를 사용하여 L1 및 상기 L2에 저장된 데이터를 모두 삭제시키는 방식으로 보안 처리를 수행할 수 있다. 또한, 자원 분배 관리장치는 BTB(Branch Target Buffer)에 대해서는 현재 저장된 데이터 대신 더미값을 가지는 더미 데이터를 채워 넣는 방식으로 보안 처리를 수행할 수 있다.

[0049] 또한, 자원 분배 관리장치(390)는 하드웨어 자원 중 LLC 캐시에 대해서는 코어 프로세서별 LLC way의 개수를 지정하고, 분배 대상 코어 프로세서에 지정된 LLC way(370)에 저장된 데이터 대한 보안 처리를 수행할 수 있다.

[0050] 이때, 자원 분배 관리장치(390)는 LLC 캐시에 대한 보안 처리에 있어서, 예를 들어 Intel CAT 기능 등을 사용하여 분배 대상 코어 프로세서에 지정된 상기 LLC way에 더미 데이터를 저장시켜 보안 처리를 수행할 수 있다.

[0051] 이에 따라, 실시간 작업 또는 배치 작업에 통합 서버의 하드웨어 자원을 재분배하는 과정에서 보안이 설정된 작업에 대해서는 하드웨어 자원의 재분배 전에 보안 처리를 수행하여 이전에 저장되었던 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 외부 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있다.

[0052] 상술한 바와 같이, 본 발명의 일실시예에 따르면, 가상머신 또는 컨테이너 기반 통합 서버의 자원 분배 관리에 있어서, 통합 서버의 실시간 작업으로 요청된 QoS를 만족시킬 수 있도록 하드웨어 자원을 동적으로 분배하여 자원 활용성을 높이며, 보안이 설정된 작업에 대해서는 하드웨어 자원의 분배 전에 기저장된 데이터를 삭제하거나, 더미 데이터로 채워 넣음으로써 외부 공격에 의한 데이터 노출의 위험성을 방지시킬 수 있다.

[0053] 본 발명에 첨부된 각 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를

통해 수행되는 그 인스트럭션들이 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 흐름도의 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0054] 또한, 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시예들에서는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0055] 한편 상술한 본 발명의 설명에서는 구체적인 실시예에 관해 설명하였으나, 여러 가지 변형이 본 발명의 범위에서 벗어나지 않고 실시될 수 있다. 따라서 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허청구범위에 의해 정하여져야 한다.

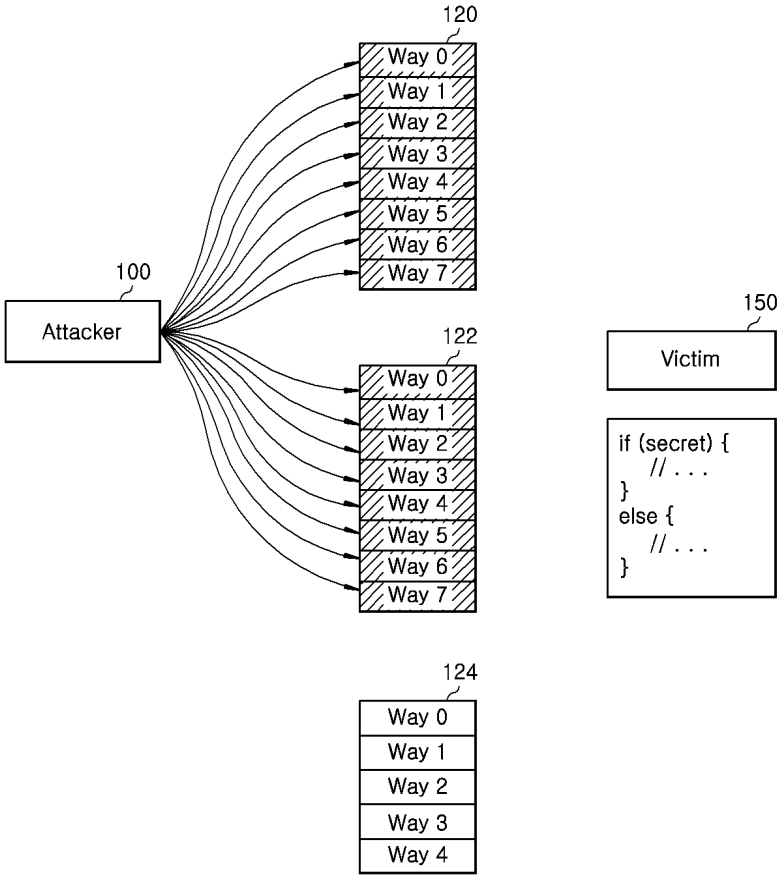
부호의 설명

[0056]

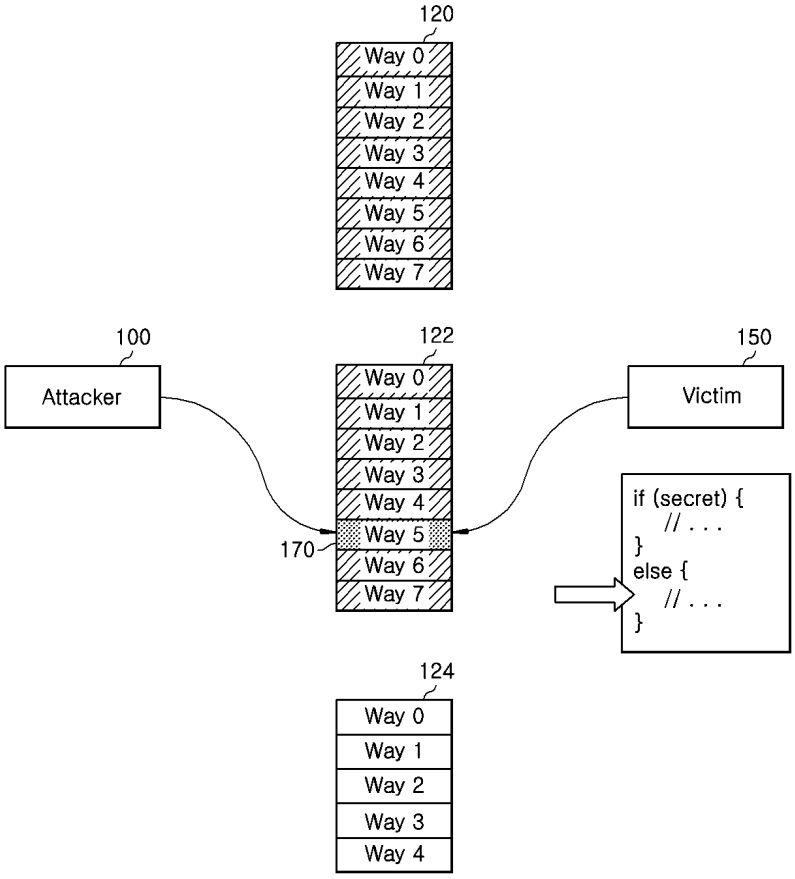
300 : 성능 제어기	302 : 롱텀 제어기
304 : 숏텀 제어기	312 : 실시간 작업
314 : 배치 작업	330 : 자원 관리기
332 : 코어 자원 관리기	334 : LLC 자원 관리기
340 : BTB	342, 344 : L1, L2
370 : LLC way	

도면

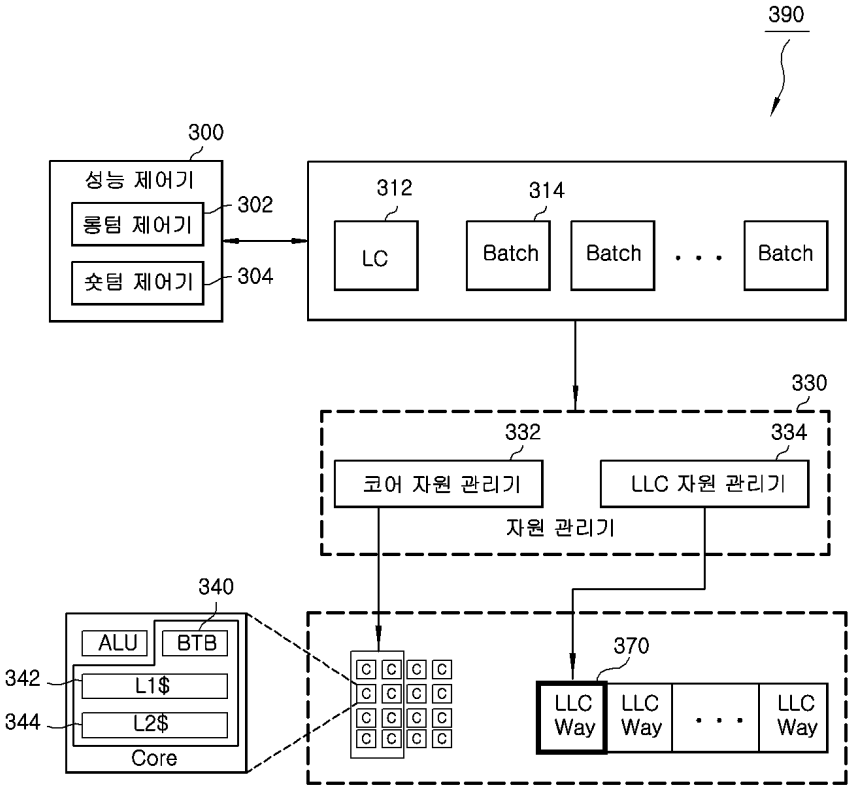
도면1


120
Way 0
Way 1
Way 2
Way 3
Way 4
Way 5
Way 6
Way 7
100
Attacker
122
Way 0
Way 1
Way 2
Way 3
Way 4
Way 5
Way 6
Way 7
150
Victim
if (secret) {
// . . .
}
else {
// . . .
}
124
Way 0
Way 1
Way 2
Way 3
Way 4

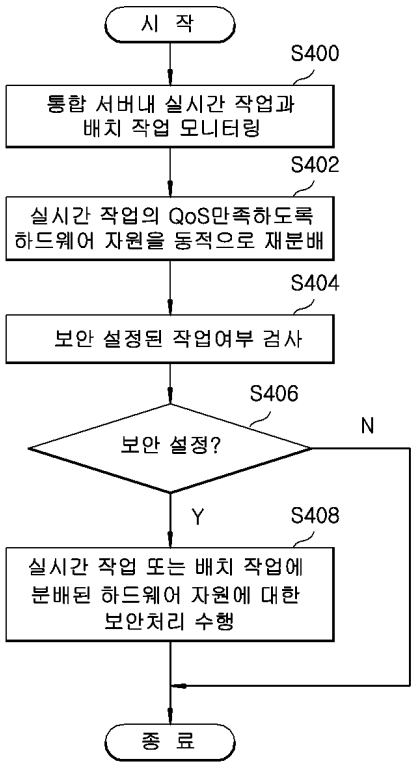
도면2


120
Way 0
Way 1
Way 2
Way 3
Way 4
Way 5
Way 6
Way 7
100
Attacker
122
Way 0
Way 1
Way 2
Way 3
Way 4
Way 5
Way 6
Way 7
170
150
Victim
if (secret) {
// . . .
}
else {
// . . .
}
124
Way 0
Way 1
Way 2
Way 3
Way 4

도면3


390
300
성능 제어기
302
롱텀 제어기
304
숏텀 제어기
312
LC
314
Batch
Batch
Batch
330
332
코어 자원 관리기
334
LLC 자원 관리기
자원 관리기
340
ALU
BTB
342
L1$
344
L2$
Core
370
LLC Way
LLC Way
LLC Way

도면4


시 작
S400
통합 서버내 실시간 작업과
배치 작업 모니터링
S402
실시간 작업의 QoS만족하도록
하드웨어 자원을 동적으로 재분배
S404
보안 설정된 작업여부 검사
S406
보안 설정?
N
Y
S408
실시간 작업 또는 배치 작업에
분배된 하드웨어 자원에 대한
보안처리 수행
종 료