Method and Electronic Device for mitigating Micro-Architectural side-channel attack by Dynamic Resource Allocation

IITM Technology Available for Licensing

Problem Statement

- The problem statement discussed in the present invention is ***how to prevent the micro-architectural attacks*** wherein the system incur high overheads and other issues related to system performance issues & etc.
- Hence, subject invention addresses the issue efficiently.

Technology Category/ Market

Technology:; Method & Electronic Device for mitigating Micro-Architectural side-channel attack;
Industry/Application: Computer Technology, Hardware, Software, & Algorithm, Servers, Cloud, Storage, Networking Devices, & etc.;
Market: The global high performance computing market is projected to reach at a **CAGR** of **7.5%** during the period **(2024-30).**

Technology

- Present patent describes a **method** & **device** that uses **hardware performance counters to detect malicious tasks** with **micro-architectural attack-like behavior**. (Refer Fig.1 & Fig.2)
- Upon detection, the proposed method provides a mechanism **to degrade and upgrade malicious program threads** based on their behavior.
- This significantly **reduces the impact** of the **false-positives on benign applications**, while detecting **malicious threads** with high accuracy using features implemented in the hardware.
- The method for mitigating a micro-architectural side-channel attack by dynamically allocating resources to a plurality of applications by an electronic device, comprising a few steps shown in Fig.2.

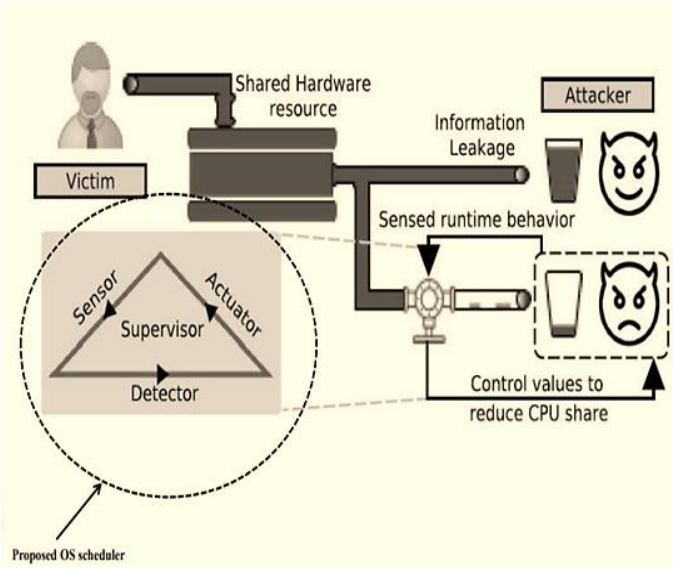

Fig.1 depicts an overview of the method for the mitigating micro-architectural side-channel attack by dynamically allocating resources to the plurality of threads by an electronic device;

- The **electronic device** includes **a communicator , a memory** and **a processor.**
- Said communicator is configured to perform **communications with the virtual machines (VMs)** which share the **physical resources of the electronic device.**

TRL (Technology Readiness Level)

TRL-4, Technology validated in Lab;

Intellectual Property

IITM IDF Ref. 1998; Patent No.495535

Research Lab

Prof. Chester Dominic Rebeiro,
Dept. of Computer Science & Engineering

CONTACT US
Dr. Dara Ajay, Head TTO
Technology Transfer Office,
IPM Cell- IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: headtto-icsr@icsrpis.iitm.ac.in
tto-mktg@icsrpis.iitm.ac.in
Phone: +91-44-2257 9756/ 9719

Images

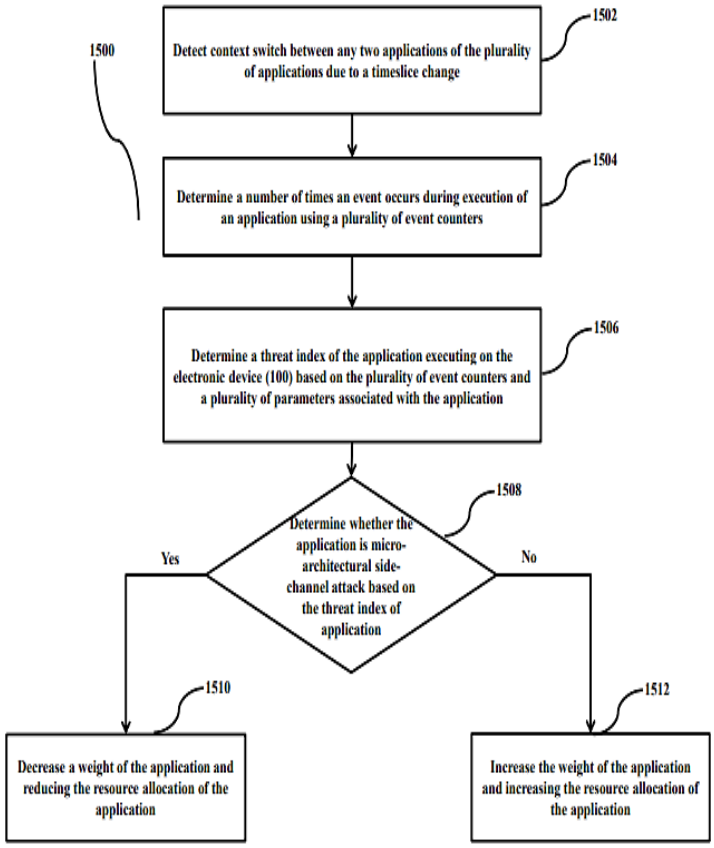

Fig.2 depicts flowchart of the method for mitigating the micro-architectural side-channel attack by dynamically allocating resources to the plurality of applications;

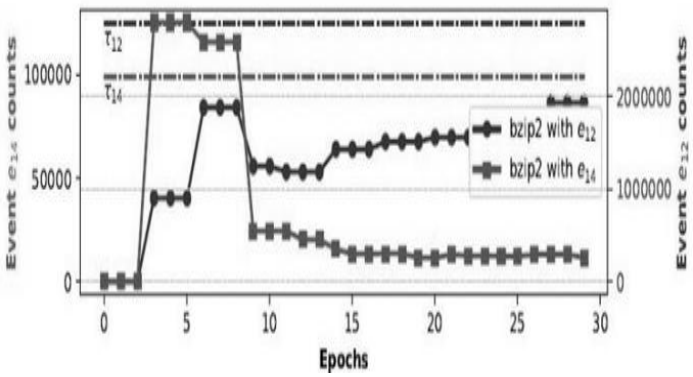

Fig.3 depicts timing diagram illustrating a benign thread breaching the threshold & being penalized for a brief period of time;

Key Features / Value Proposition

The proposed method selectively penalizes applications that behave maliciously & the most benign applications are not affected.

Said method can be easily adapted for new attacks as long as there are at least one of a plurality of hardware performance counters/ plurality of event counters that can detect them.

- **The electronic device may be a cloud infrastructure provider which provides dynamic computing resources which allows virtual machines (VMs) from multiple customers to share physical resources such as servers, a server, a computer, a laptop, etc.**

Efficiently brings down the cost of a false penalization.

Once a benign thread which is erroneously flagged, is unflagged, the benign thread regains the CPU share and executes without any additional overheads.

CONTACT US
Dr. Dara Ajay, Head TTO
Technology Transfer Office,
IPM Cell- IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: smipm-icsr@icsrpis.iitm.ac.in
sm-marketing@imail.iitm.ac.in
Phone: +91-44-2257 9756/ 9719