Detect & Adapt: A Resiliency Enhancement Mechanism for Space Computing Platforms

#SAND2023-11822A

Shafkat Islam (Purdue, USA), Nagender Aneja (Purdue, USA), Ruy de Oliveira (IFMT-Brazil)
Sandhya Aneja(Marist College, USA), Bharat Bhargava (Purdue, USA), Jason Hamlet (Sandia), Chris Jenkins (Sandia)

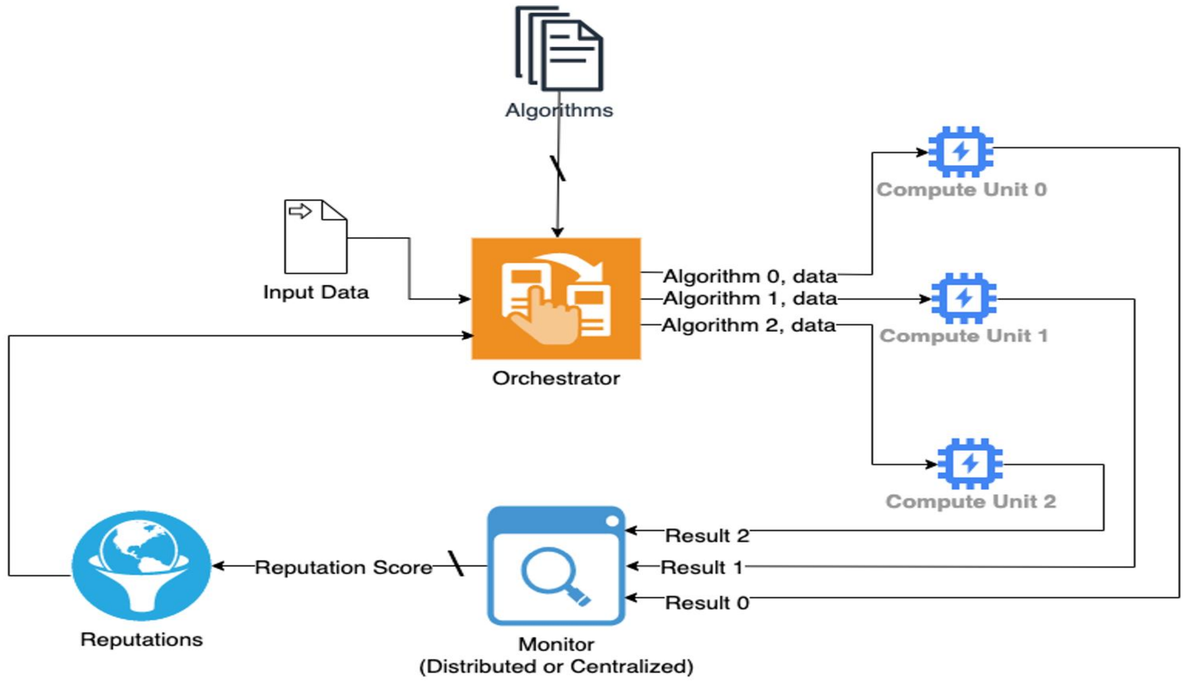
MOTIVATION

- Space systems have been widely used in navigation, communication, weather forecasting, and remote sensing
- Space systems use Heterogeneous computing platforms (HCPs) for faster computation
- HCPs use commercially available off-the-shelf processing units, i.e., CPU, GPU, FPGA, DSP.
- HCP lacks in built-in security features

INTRODUCTION

- Applications of HCP outside of space: critical infrastructure, autonomous vehicles, edge AI
- HCP integrates different processing units into single chip
- Provides efficient computing in terms of performance and power consumption
- HCP executes computation without the supervision of any central entity
- Gap exists in the literature regarding the security features of HCP platform in space systems
- There is a pressing need to explore ways to develop security solutions for the HCP-based computing environment

Proposed HCP Orchestration & Monitoring Mechanism



HCP Orchestration & Monitoring

- Orchestrator assigns: data, algorithm, and task
- Compute units: execute task and send the result to the monitor
- Monitor: verifies results from each compute unit, outputs the final compute result, evaluates performance of each compute unit, and sends the evaluation summary to the orchestrator

HCP Threat Model

- Trustworthy: Orchestrator and monitor
- Attacks: manipulation of results and degradation of performance
- Manipulation of results: data manipulation, output alteration, packet drop
- Degradation of performance: algorithmic trojan and packet drop

HCP Computing Strategy

- Computation Partition
- Triple modular redundancy
- Triple modular diversity
- Hybrid

HCP Detection Strategy

- Hierarchical detection
- Brute force approach
- Probabilistic approach
- Fingerprinting approach
- Hashing based approach
- Attribute based checksum approach

HCP Orchestration

- Machine learning based adaptation
- Rule based adaptation
- Random orchestration
- Round robin orchestration

CONCLUSIONS

- Conducted preliminary experiments using sorting
- It can defend abnormalities even if two-thirds of the units are compromised
- Future work: Implement colluding attacks and adaptive orchestration
- Target applications: sorting, compression, gradient descent, machine learning application