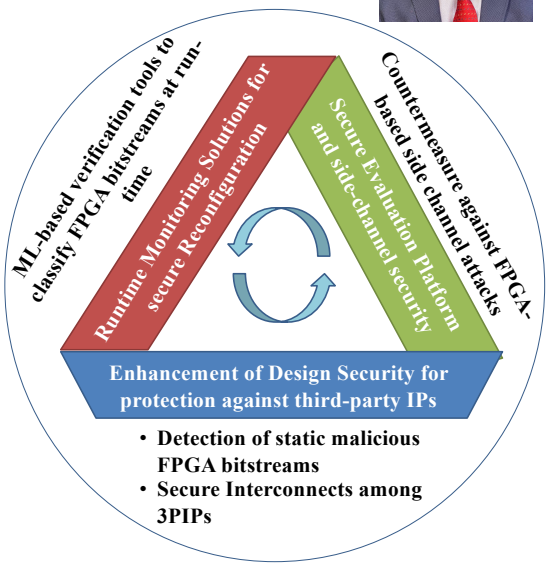
Security of FPGA-as-a-Service for Reconfigurable Systems: Securing FPGA bitstreams and Preventing IP Theft

PI: Krishnendu Chakrabarty, Duke University



Research Goals:

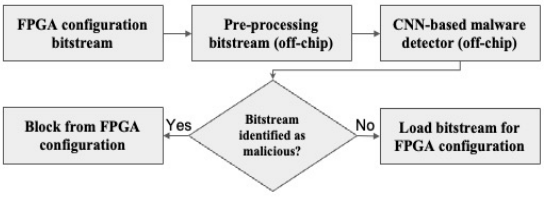
- Study security threats arising from third-party IPs (3PIPs) in FPGA-as-a-Service Platform.
- Static detection of malicious FPGA bitstreams using ML.
- Countermeasures to secure SoCs against attacks launched from untrusted 3PIPs.
- Secure interconnections between IPs to eliminate attacks launched through power distribution network, electromagnetic, and physical side-channels.

Scientific Impact:

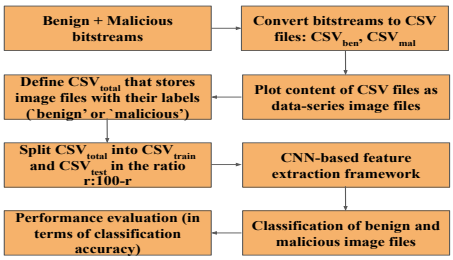
- Proposed methods relevant in securing hardware and hardware/software interactions in heterogeneous SoCs with integrated FPGAs.
- Support for attack modeling, prediction, detection, and protection for trustworthy cyberspace incorporating FPGA-as-a-Service.

Solution 1: Detecting Malicious FPGA Bitstreams using CNNs

- Detection of static malicious FPGA bitstreams using CNN-based learning
- Off-chip CNN pipeline for detecting malicious bitstreams before FPGA configuration
- Generalizable framework for multiple FPGA families, without the need for reverse-engineering



CNN pipeline for detecting malicious FPGA bitstreams

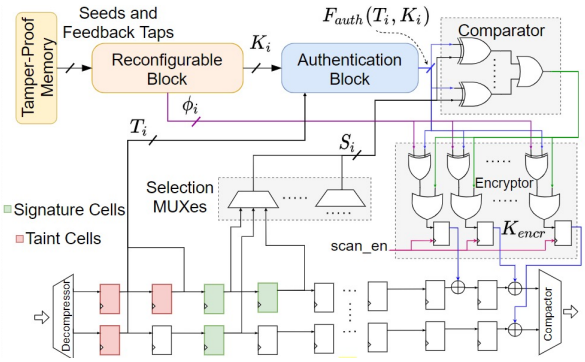


Evaluation of detection model

- True Positives (Percentage of malicious bitstreams correctly classified as malicious): **97.08%**
- False Positives (Percentage of benign bitstreams incorrectly classified as malicious): **4.29%**

Solution 2: Dynamic Cryptographic Test Data Authentication and Obfuscation

- Support for per-pattern dynamic test data authentication through embedded taint and signature bits.
- Support easy integration with existing test data protection schemes while protecting IP access.



Broader Impact on Research and Society

- ***Research Impact:*** Collaboration with industry partners and dissemination through workshops/tech transfers.
- ***Educational Impact:*** Multiple PhD students supported (including female student), incorporation in student projects, coursework, and guest lectures.