Session B: Dependable Computer Systems and Secure Semiconductor Chips

A provably correct fault-tolerant distributed framework

Corresponding Applicant: Amit Garg (University of Texas, Austin)

Co researcher: Jayadev Misra, Harrick Vin, Young-ri Choi, Siddhartha Rai
(University of Texas, Austin)

> *If the automobile had followed the same development cycle as the computer,*
> *a Rolls-Royce would today cost $100, get one million miles to the gallon,*
> *and explode once a year, killing everyone inside.*
>
> **Robert X Cringely**

Our goal is to prevent the explosion.

Goal & Contribution to well being for all humanity:

- ✓ Make it possible for the average programmer to easily build complex distributed systems.
- ✓ Our framework automatically verifies system properties, thus programmers will be able to offer guarantees about their applications' behavior.
- ✓ Fault-tolerance is built into the framework so that hardware failures are dealt with gracefully.
- ✓ Make provably correct applications for safety-critical applications available to everyone

Method / Approach:

- ✓ Confine our domain to modeling distributed workflows. We believe the majority of real systems can be expressed as a workflow, and this makes the verification process tractable (as opposed to modeling a general process network)
- ✓ Build upon the action system framework. It has a well-developed theory for proving safety and progress properties. Thus it is used to provide short and simple proofs for many hard problems in distributed computing.
- ✓ Create a proof checker for our framework. Actions systems are naturally amenable to automated proof checking. Their simplicity and expressiveness makes the proof checker powerful because complex systems can be verified rapidly.
- ✓ Collaborate with an industrial partner to model a real distributed workflow and prove its correctness.

Introduction / Position in the Session:

- ✓ Dependable computing often involves replication for fault tolerance. Although this works well in theory, in practice hardware costs and system administration overhead are often prohibitive, except for the most safety-critical applications.
- ✓ A common justification for replication is that it is not possible to build `correct systems' of any significant complexity. Our research seeks to demonstrate that for an important class of applications, this approach is indeed possible and even desirable.

Call for collaboration:

- ✓ In order to demonstrate the power of our framework, we wish to model a real world problem of significant complexity using it. Thus we want to collaborate with an industrial partner who feels that such a system would bring them significant value.