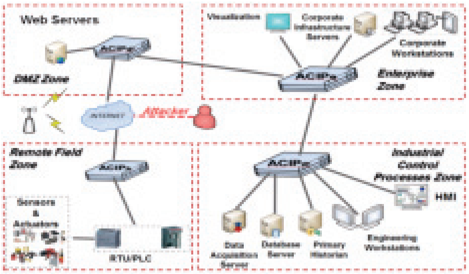
Center for Autonomic Computing (CAC)

A CISE-funded Center

University of Florida, Jose Fortes, 352.392.9265, fortes@ufl.edu
Rutgers University, Manish Parashar, 732.445.5388, parashar@caip.rutgers.edu
University of Arizona, Salim Hariri, 520.621.4378, hariri@ece.arizona.edu
Mississippi State University, Ioana Banicescu, 662.325.7508, ioana@cse.msstate.edu

Center website: http://www.nsfcac.org/

Autonomic Critical Infrastructure Protection System (ACIP)



Test bed based on SCADA systems provides a platform for testing both hardware and software.

A recent Forrester survey reported that 75% of organizations experienced Distributed Denial of Service Attacks (DDoS) even though they implemented cybersecurity solutions. One third of the organizations that were attacked experienced service disruption as a result of the attack. The problem is that many of these are ineffective against novel and well-organized attacks. The nation's critical energy infrastructures (power, water, gas and oil) are moving to modernize their industrial control systems to build what is referred to as "Smart Grids" that use advanced computing and communications technologies to bring knowledge so they can operate far more robustly and more efficiently. These developments have led to huge cybersecurity problems because of the widespread use of Supervisory Control and Data Acquisition (SCADA) systems that were never designed with security in mind. Consequently, SCADA systems become a prime target for cyberattacks due to the profound and catastrophic impacts they can have on our economy and on all aspects of our life. In fact, critical infrastructures have expanded to include not only the energy critical infrastructures, but also many process control systems, networks and infrastructures of which approximately 85% are privately owned.

Motivated by this need, researchers at the Center for Autonomic Computing (CAC) and industrial center members (Raytheon and AVIRTEK) are collaborating to develop an innovative cybersecurity approach based on autonomic computing technology. It is analogous to the human nervous system where computing systems and applications can be self-configured, self-optimized, self-healed and self-protected with little involvement from the users and/or system administrators. CAC has successfully developed and implemented an Autonomic Critical Infrastructure Protection (ACIP) appliance and currently being tested and evaluated. This involves evaluating appliance's self-protection capabilities using an industrial process control test bed that offers multiple capabilities for both hardware and software experimentation. This breakthrough technology is validating the thesis that autonomic paradigms have the potential to detect and mitigate cyber threats launched against industrial control systems. Responding faster than a human operator, SCADA and their associated control elements can effectively immunize against cyber malware and mitigate the effects of control element failures until human operators can take control.

> **Economic Impact:** A study conducted by the same group, Forrester Consulting, indicated that organizations that provide online services as their core business stand to lose millions of dollars per hour when their services are down. The ACIP technology when fully matured can be exploited by western world societies to immunize critical infrastructures against being targeted by malcontents and terrorists. Enhancing the ability of the nation to provide undisrupted service of electric power, clean potable water, transportation and other necessary societal support services, saves lives, preserves the domestic tranquility and can help protect industry's and the nation's economic vitality.

For more information, contact Salim Hariri, 520.621.4378, hariri@ece.arizona.edu.

Using CometCloud for Managing Scientific and Business Workflows on Multiple Clouds

Rutgers and Xerox collaborated to develop and deploy an innovative workflow management framework for federated cloud infrastructure using the CometCloud autonomic cloud engine. Public clouds have emerged as an important solution that enables the renting of resources on-demand, and supports a pay-as-you-go pricing policy. Furthermore, private clouds or data centers, which cater to a restricted set of users within an organizational domain, are exploring the possibility of scaling out to public clouds to respond to un-anticipated resource requirements. As a result, dynamically federated, hybrid cloud infrastructure, such as those enabled by CometCloud, which integrate private clouds, enterprise data centers and grids, and public clouds, are becoming increasingly important. An enterprise workflow typically consists of an ordered set of heterogeneous applications, each of which may have specific constraints on resource requirements, performance, completion time, cost, privacy, etc.

The breakthrough enabled Rutgers and Xerox to demonstrate the following capabilities for the first time in a single framework: 1) Dynamic cloud federation – managing resources across multiple private and public clouds in order to dynamically scale the execution of application workflows up, down, and/or out, according to high-level policies; 2) Programming management – resource scheduling and provisioning within the federated cloud infrastructure based on application requirements as well as system resource capabilities and availability, and within cost, time, and performance constraints, and; 3) Workflow deployment – deployment of real-world enterprise application workflows from Xerox executing on a federated cloud infrastructure. Specifically, the hybrid infrastructure used in the demonstration dynamically integrated private clouds at Rutgers and ACS with the Amazon EC2 public cloud.

Such an autonomic workflow framework can dynamically select an optimal mix of resource classes (clouds or grids provider, types of nodes, the number of nodes, etc.) based on application QoS and resources requirements, user policies, and constraints. The workflow framework can also monitor the execution of the applications services within the workflow, and can adapt both the resource provisioning as well as the services to ensure that the application requirements and user constraints continue to be satisfied. Adaptations may involve scaling resources up, down or out within the federated cloud infrastructure, and can allow the system to handle unanticipated situations such as workload bursts, system performance degradation, or resource failures.

> **Economic Impact:** This technology has the potential to reduce computational costs and improve efficiency of cloud computing service centers by enabling the construction of hybrid cloud infrastructures. These structures can support heterogeneous and dynamic workloads and on-demand cloud bridging. Federated cloud infrastructures also provide opportunities to improve application quality of service and lower cost by mapping applications of scientific or business workflows to appropriate resource providers.

For more information, contact Manish Parashar, 732.445.5388, parashar@rutgers.edu.

Demand-driven Service and Power Management in Data Center

Power consumption represents an increasingly significant percentage of the cost of operating large data centers. These data centers are used by banks, investment firms, IT service providers, and other large enterprises. One approach to reduce power consumption is to keep machines in standby or off modes except when the data center workload requires them to be fully on. This approach depends on being able to monitor performance, workload or resource demands and to anticipate the need for resources in order to meet service-level agreements of the users that generate the workload.

The results of this project include: mechanisms to monitor, model and predict workload associated with individual services, model and predict global resource demand, and dynamically allocate and de-allocate virtual machines to physical machines; management methods based on control theory and/or market-based approaches; mechanisms to minimize the cost of providing individual services while globally minimizing power consumption and delivering contracted service levels; and development and evaluation of software that implements these methods.

Ongoing experimental evaluations on an IBM BladeCenter have shown that the proposed approach can efficiently and stably reduce thermal hotspots, power consumption and performance degradation caused by virtual machine consolidation, while balancing conflicting objectives.

> **Economic Impact:** Annual energy and administration costs associated with today's data centers amount to billions of dollars: power and cooling rates are increasing by an alarming 8 fold every year and are becoming the dominant part of IT budgets. The high energy consumption of modern data centers also translates into excessive heat dissipation, which, in turn, increases cooling costs and server failure rates. One of CAC's main research thrusts aims to address this problem because doing so can lower the cost of ownership of data centers in all sectors of today's economy. It can also increase the reliability of the infrastructure that provides critical services.

For more information, contact Jose Fortes, 352.392.9265, fortes@ufl.edu.