Update from the Director

It is my pleasure to communicate with you through UA NSFCAC Tecnews of the UA site of the NSF Center on Autonomic Computing (NSF CAC). The NSF CAC is a center funded through the NSF Industry/University Cooperative Research Centers program, industry, government agencies and matching funds from member universities, which currently include the University of Florida (Lead), the University of Arizona, Rutgers, The State University of New Jersey and the Mississippi State University (MSU).

I am pleased with the quality of the ongoing research projects and the strong support from our industrial and government members. We have built state of the art test-beds to support our research activities in Cyberinfrastructure security, critical infrastructure protection, and high performance cloud computing and data centers that are critically important to develop and demonstrate the capabilities of our projects.

As we move forward, we would like to invite you to join the center so together we can develop innovative autonomic technologies that will revolutionize how to design and deploy next generation information and communications services.

Salim Hariri, UA Site Director
Autonomic Management Technologies: Integrated, Proactive and Automated

by Salim Hariri

Advances in information, communication, Internet and social networking technologies have lead to rapid deployment of cyberinfrastructure services that are pervasive and ubiquitous and touch all aspects of our life. However, these advances have increased the control and management complexity of cyberinfrastructures by several orders of magnitude. Current control and management technologies are mainly labor-intensive, ad-hoc and cannot manage the exponential increase in complexity, dynamism, and unpredictable behaviors of cyberinfrastructure resources and services in a timely manner. These technologies made cyberinfrastructure resources and services unmanageable and insecure. In fact, as shown in Figure 1, they suffer from what I call *click-and-view syndrome*. By the time the users and system administrators recognize the problem, it is already too late. Recently, on May 6\textsuperscript{th} 2010, the U.S. equity markets experienced the worse decline and reversal since 1929! Within 10 minutes, the Dow Jones Industrial Average plunged about 900 points, around one billion stop loss orders were executed and that resulted in individual investors losing more than $200 million on that day. This event can be recreated by cyberattacks if we keep using the current click-and-view technologies and will severely impact our financial systems and their dependability.

“Current control and management technologies are mainly labor-intensive, ad-hoc and cannot manage the exponential increase in complexity, dynamism, and unpredictable behaviors of cyberinfrastructure resources and services in a timely manner. These technologies made cyberinfrastructure resources and services unmanageable and insecure.”
In contrast to static, manual and labor intensive, and heuristic control and management approaches, we need to adopt a paradigm shift based on autonomic computing principle inspired by human nervous systems. In autonomic computing management, the cyberinfrastructure resources and services will be seamlessly managed (self-management) with little involvement by users and system administrators to adopt policies and control algorithms to meet their performance requirements (self-optimize), reconfigure to tolerate hardware and/or software faults (self-heal), and stop and/or mitigate the impacts of threats and cyber attacks (self-protect). The salient features of this paradigm are its capabilities to deliver 1) **Integrated management solutions** to address performance, faults, security and misconfiguration; 2) **Proactive management solutions** that use data mining, information theory and statistical techniques to aggregate and correlate monitored features so they can detect and predict accurately and anomalous behavior that might have been triggered by attacks, faults and/or accidents or disasters; and 3) **Automated management solutions** that will to significant reduction in operational costs due to automated and also provide the required timely responses to anomalous events to stop and/or prevent rapid propagation of attacks/faults and mitigate their impacts on normal system operations and services.

Autonomic management technologies shown in Figure 2 will require the development of continuous monitoring and online behavior analysis, risk and impact analysis and automated/semi-automated recovery actions to achieve effective and efficient resilient operations against any types of faults, accidents, threats or exploitations of hardware/software vulnerabilities.

**Figure 2.** Autonomic management technologies are integrated, proactive and automated.

“In autonomic computing management, the cyberinfrastructure resources and services will be seamlessly managed (self-management) with little involvement by users and system administrators to adopt policies and control algorithms to meet their performance requirements (self-optimize), reconfigure to tolerate hardware and/or software faults, and stop and/or mitigate the impacts of threats and cyber attacks.”
Autonomic Cloud Management Services (ACMS)
Project PIs: Drs. Salim Hariri, Youssif Al-Nashif and Ali Akoglu
Graduate Students: Shitao Li, Farah Alfay, and Shafiul Islam

**Motivation:** As the internet system and applications continue to grow at a rapid rate, balancing the power consumption of the memory and processor subsystems and the performance of the server systems has become an utmost concern for the HPC community. The power and performance optimization for cloud computing systems and large-scale data centers is a challenging research problem that can be addressed efficiently by applying autonomic management solutions.

**Goals/Objectives:** Our goal is to extend our theoretical framework and general methodology for autonomic power and performance management for large scale data centers in order to 1) autonomically scale-up/down cloud resources (cores, storage, I/O devices) to meet multi-objective requirements (performance, energy, availability, etc.), 2) identify the cloud workload characteristics and their requirements at run-time, 3) identify the features to be monitored and analyzed at run-time for accurate characterization of the current operation region of cloud services, and 4) identify the structures (AppFlow, VmFlow, ServFlow, etc.) that can be used to steer the platform autonomic manager architecture. This approach will enable effective use of hardware resources under varying workload conditions so that idle hardware could be put to a low-power state and the power consumption of the system could be managed.
**Current State:** We have developed a framework to simulate the behavior of a computing system at server, memory/processor subsystem and core levels. We designed a workload generator for CPU, Memory and I/O intensive operations. We developed algorithms to autonomously scale CPUs and DRAMs allocated to the system for power management under various execution modes. We developed mechanisms for monitoring and collecting data on features such as CPU load, memory usage, page faults, I/O reads/writes etc. We developed the AppFlow tool for tracking and predicting application/platform behavior. AppFlow successfully characterizes the dynamic behavior of applications with respect to key features being monitored. With AppFlow, we can track the changes in the behavior of the applications and thereby take proactive measures to ensure the optimum performance/utility for the applications.

**Research Issues/Tasks:**
- How do you autonomically scale up/down cloud resources (cores, storage, I/O devices) to meet multi-objective requirements (performance, energy, availability, etc.)?
- How do we identify the cloud workload characteristics and their requirements at run-time?
- What are the features that are needed to be monitored and analyzed at run-time to accurately characterize the current operation region of cloud services and/or applications?
- What data structures (AppFlow, VmFlow, PlatFlow, etc.) can be used to steer the Platform Autonomic Manager (PAM) architecture?

**Operating point**
\[ OP_{vm} = (OP_{cpu}, OP_{mem}, OP_{i/o}, OP_{throughput}, OP_{time}) \]

*n*-dimensional space at any instant of time during application’s lifetime

Operating Point drifting to Undesired/Unsafe Zone

Shafiul “Jacky” Islam  
Farah Alfay  
Zhitao Li
Autonomic Virtual Cloud Management Services (AVCMS)

by Salim Hariri and Youssif Al-Nashif

Cloud Computing is the new paradigm shift in the field of distributed systems, which aims at delivering computing as a utility. It refers to the concept of dynamically assigning applications, processing time and storage space from a ubiquitous ‘cloud’ of computational resources to the end-users. It involves the delivery of both the applications, as the service, along with the hardware and systems software in the datacenters that provide these services. Some important aspects of Cloud Computing are: the illusion of infinite computing resources available on demand, the elimination of an up-front commitment by Cloud users, and the ability to pay for use of computing resources as needed [cloud,1]. Cloud facilitates Utility Computing without long-term commitment or contract between the provider and user, thereby making it an excellent platform to build applications on top. Organizations and individuals can benefit from mass computing and storage, provided by large companies with stable and strong cloud architectures.

There is a strong interest within the DoD to extend cloud computing services to tactical users so that they have access to shared data, applications, storage and computing resources regardless of their location, while at the same time not jeopardizing the security and the mission of tactical environment resources and their users (warfighters as well as mobile assets). The current cloud computing services focused on providing web applications (e.g., Google Office, storage, emails, etc.) that can be accessed from mainly wired networks. To extend cloud applications to tactical environments and users, the following limitations must be addressed: 1) Tactical resources and users are easy targets to malicious attacks that exploit vulnerabilities in mobile devices and resources as well in the wireless communications networks used to interconnect the tactical resources and users; and 2) Efficient on-demand allocation of cloud services when these services are accessed from mobile assets and users with limited computing power, storage capacity and bandwidth limitation.

AVCMS Architecture

Our approach to develop the AVCMS architecture is based on Autonomic and Cloud Computing, and Virtualization technology. In this project, we will develop and demonstrate the key functionalities and services to implement on-demand cloud computing services in tactical environments. The cloud environment to be considered in this project is composed of geographically dispersed Clouds of different types (e.g., military, private, community clouds), each of which runs its own Cloud Management Server (CMS) that acts as a proxy for the Autonomic Virtual Cloud Manager (AVCM) that autonomically manages all the cloud resources and services for a given a cloud application as shown in Figure above.
In this environment, users who can be fixed or mobile, can login to AVCMS to develop and/or run network centric collaborative applications that can run on fixed or mobile cloud computing resources. Consequently, one can view the AVCMS environment as an integrated adaptive high performance distributed computing environment that provides all the required services, software tools to develop, schedule, run and visualize collaborative applications on geographically dispersed and heterogeneous clouds that can be fixed or mobile. The proposed autonomic virtual cloud management services will support the following types of transparency:

**Access Transparency:** The users can login and access all the cloud resources (mobile and/or fixed) regardless of their locations.

**Mobile Transparency:** AVCS supports in a transparent manner mobile and fixed users and resources.

**Configuration Transparency:** The resources allocated to run a cloud application can be dynamically changed in a transparent manner; that is the applications or users do not need to make any adjustment to reflect the changes in the resources allocated to them.

**Fault-Tolerance Transparency:** The execution of a parallel and distributed application can tolerate failures in the resources allocated to run that application. The number of faults that can be tolerated depends on the redundancy level used to run the application.

**Performance Transparency:** The resources allocated to run a given cloud application might change dynamically and in a transparent manner to improve the application performance.

**AVCMS Implementation Approach**

The figure on the side shows the architecture that will be used to implement the AVCS services. The users and/or applications (mobile or stationary) can login to the environment through a general set of cloud front end services that provide them with all the required tools to authenticate users, provide them with the appropriate security tools to meet the desired confidentiality, integrity and availability requirements. In addition, users and/or applications will be provided with a wide range of tools and services to enable them to access and run cloud services as well as develop new ones. The adaptability of applications will be supported using AVIRTEK autonomic management tools and services (e.g., Autonomia) that can provide programmable management services to achieve the required capabilities with respect to self-configuration, self-healing, self-optimizing and self-protecting [references to autonomy]. Once these are selected to meet each cloud user and/or application, the autonomic management of the cloud resources will be delegated to an Autonomic Virtual Cloud Manager (AVCM) that will be responsible to maintain these requirements at runtime. Specifically, the AVCM will be responsible for setting up all the clouds to be used and integrate them into one virtual cloud and then run and manage the execution of the application. In setting up the application execution environment that might span several clouds, the AVCM will collaborate with a proxy server (Cloud Management Server (CMS)) at each cloud to control and manage the cloud resources used.
Autonomic Cyber Phyasical System for Biosphere 2 Landscape Observatory Research

Project PIs: Drs. Salim Hariri, Steve DeLong, and Ali Akoglu

Graduate Students: Venkata Krishna, and Shafiul Islam

Motivation: Interaction of hydrological cycle with other global changes is affecting ecosystems on Earth. Landscape Evolution Observatory (LEO) is an interdisciplinary project at Biosphere 2 aimed to quantify the interactions between soils, biological, hydrological, geological and atmospheric processes. To develop a good understanding of these interactions of processes, there is a pressing need for development of experimental infrastructure which can couple complex physical systems with hydrological models. An ability to control the physical systems based on the information from monitoring systems equipped with a variety of field instrumentation, will considerably accelerate the discovery cycle by iteratively testing models against experimental system.

To this date, there is no complete solution to control and manage computational models and experimental test bed in a closed loop form with the autonomic sensing, data-model fusion, autonomic workflows and online analysis capabilities. Such a solution will accelerate research and discovery for grand Earth science challenges, and as well as many other cyber physical systems such as intelligent transportation systems, greenhouses, etc.

Design of the B2 Landscape Evolution Observatory. Construction of this facility will continue through 2011.
**Background and Current State:** LEO experiments are characterized by large amounts of the data streaming and processing to effectively study hydrological cycles and their interactions with environment. Ring Buffer Network Bus (RBNB) Data Turbine is an open source initiative to develop an infrastructure for data management, processing and synchronization. Kepler is another open software tool for scientific workflow management. In parallel we also set up a physical experimental testbed in the B2. The test bed consists of 30 sensors to monitor features such as the weight, water flow, and conductivity with an operational infrastructure to simulate rain on the test bed. National Instrument’s Compact RIO is programmed with the LabView to collect and store data in real time. However, the experimental test bed and the workflow management components have not been integrated yet.

**Project Goals:** To enable seamless coupling of computational models with the unique experimental infrastructure of Biosphere 2 (B2). We propose a service-oriented cyber-infrastructure shown in figure 1 for establishing a distributed system which integrates physical infrastructure at B2 with data assimilation models executing on a virtualized cloud platform with hundreds of cores available at Autonomic Computing Lab at University of Arizona. Our objective is to develop strategies for robust data acquisition, autonomic decision making in sensing, data-model fusion, analysis and visualization to support accelerate research and discovery.

**Research Tasks:**

- **B2-LEO Sensor Network Design:** The current implementation of our sensor networks can be accessed online to keep track of real time data generated from the soil test-bed which is available at [http://ponderosa.b2science.org:8080/SensorPlots/RTSDPs_exp3.jsp](http://ponderosa.b2science.org:8080/SensorPlots/RTSDPs_exp3.jsp).
- **Sensor Data Streaming and Architecture**
- **Echohydrological Modeling**
- **Model Calibration and Improved Estimates through Assimilation of Data and Model**
- **Autonomic Control, Analysis, and Visualization Dashboard**

---

**Online access to sensor data**

**Industry Partners**

- IBM
- AVIRTEK

---

**Venkata Krishna Nimmagadda, M.S. Student, UA**

**Steve DeLong, Asst. Research Professor, Biosphere 2.**

**Ali Akoglu, Asst. Professor, ECE, UA**

**Shafiul “Jacky” Islam, M.S. Student, UA**

**Salim Hariri, Professor, ECE, UA**
Wireless Autonomic Protection System (WAPS)

Project PIs: Drs. Salim Hariri and Youssif Al-Nashif

Graduate Student: Hamid Alipour

Motivation: The fast and vast deployment of wireless networks and their different applications have changed the structure of ubiquitous network services and the defense strategies for network security. Wireless networks can range from 10 meters as in the case of wireless personal area networks (WPAN) to 100km as in the case of wireless regional area networks (WRAN). Advances in wireless technology have enabled portable devices to become essential part of our daily life, while we use them to access our critical information like banking accounts, credit cards or email addresses. While wireless networks are taking a progressively crucial role in modern society, the lack of effective and affordable security measures made them easy targets for intruders.

State Of the Art: Current wireless network-defense tools rely primarily on pre-defined signatures for attack detection. While these methods can successfully detect commonly known attacks, they cannot recognize abnormal behaviors caused by new and sophisticated attacks until it is likely too late to take any useful action. The studies show that current wireless intrusion detection systems can detect up to around 40% of the current wireless attacks and fail to detect complex, dynamic, and knowledgeable attacks.

Project Goal: Our goal is to find innovative ways to secure the wireless networks. Our objective is to build a state-of-the-art anomaly-based Wireless Autonomic Protection System (WAPS). Protection will be achieved by 1) monitoring multiple channels concurrently in real time, 2) detecting the anomalies due to exploitation of the wireless communication protocol by the intruder, 3) taking proactive actions to isolate and quarantine the intruder. WAPS monitors wireless networks, extracts the network features, tracks wireless-network-state machine violations (Behavioral Analysis Engine - BAE), generates wireless network flows (WNetFlow) for multiple time windows, and uses the dynamically updated rules to detect complex known and unknown wireless attacks. The Prediction Engine combines the results of WNetFlow with the output of the BAE to achieve low false positive, and enables taking appropriate actions proactively.
Project Methodology: Our approach is based on collected appropriate features and aggregate them into a data structure that we refer to as Wireless Network Flow (WNetFlow) to characterize the behavior of wireless traffic. WNetFlow is a technology used to monitor wireless network behavior, designed at University of Arizona CAC site. A WNetFlow is an n-dimensional data structure of monitored traffic such as a timestamp, key features (to identify the flow, i.e srcAddr, destAddr, bssid) and a set of features related to frame, MAC addresses, frame header, and wireless communication technologies properties.

Current State of the Project: Currently we have built a wireless testbed consisting of two Access Points (APs) operating at the channels 3 and 8 respectively. These APs are configured to work with WEP and WPA security enabled. The testbed uses high gain antennas for channel monitoring. The normal data is collected using some normal stations and the attacker can launch attacks on APs.

Research Tasks:

- We will first design the Runtime Protection Unit which involves the Behavioral Analysis Unit (BAU) to model the temporal behavior of the protocol, Prediction Engine to predict the anomaly score of the activities, and Impact Analyzer to determine the impact of the detected attack on the protected network.

- We will design and develop strategies for the Action Handler unit to take proactive actions and mitigate the attack impact. The integrated Anomaly-based Wireless Self-Protection System (WSPS) will detect the attacks in early steps, identify new attacks and take proactive actions.
Autonomic Critical Infrastructure Protection (ACIP) Test-bed

Graduate Students: Don Cox and Malaz Mallouhi

As energy critical infrastructures (power, water, gas and oil) starting to modernize their industrial control systems to build what is referred to as “Smart Grid” that uses advanced computing and communications technologies to bring knowledge to power grid so it can operate far more efficiently. The widespread use of Supervisory Control and Data Acquisition (SCADA) systems in critical energy infrastructures (gas, oil, and electrical power) makes them vulnerable to both internal and external attacks. To make the matter even worse, SCADA systems were never designed with security in mind and securing them is a challenging research problem. Consequently, SCADA networks become a prime target for cyber attacks due to the profound and catastrophic impacts they can inject to our economy and all aspects of our life.

SCADA systems can be viewed as distributed control systems where human operators control the environment through Human-Machine Interfaces (HMI). Through the HMI, the operators can control the SCADA subsystems that include Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). With the use of information technology in SCADA systems, they become susceptible to all cyber attacks that might control all SCADA programs from remote sites located on the Internet. Current commercial intrusion detection and protection tools and techniques have failed to secure and protect our cyber infrastructure as will be explained below. Attack detection techniques can be classified into three categories: signature-based and norm-based detection. Signature-based detection and forensics are reactive approaches to security. To be effective, signature-based systems rely on large databases of known attacks, which require continuous updates as new exploits are identified. If an attack does not match closely enough a known signature, the signature-based system will miss it entirely. Norm-based systems rely on training data representing normal behavior profiles in order to detect activity that is “outside the norm.” While these systems are good at detecting new exploits, they require collecting large body of data to build their models of normal behavior. In addition, norm-based systems suffer from high false positives.

A new innovative approach based on autonomic computing technology that 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 is being developed by the University of Arizona Center for Autonomic Computing, AVIRTEK and Raytheon. The Autonomic Critical Infrastructure Protection (AutoCIP) will utilize autonomic agents, online monitoring, feature selection based on information theory, multi-level behavior analysis of SCADA systems and networks, decision fusions based on statistical and data mining techniques, automated/semi-automated protection actions, visualization and adaptive learning.

The approach adheres to the Three Tenets of Cyber Security [19] and can be highlighted as follows: 1) System Susceptibility- By continuously monitoring and fixing discovered vulnerabilities, we will be able to reduce system susceptibility to cyber attacks (Tenet 1); Access to Flaw – By using multilevel behavior analysis of SCADA applications and networks, we will be able to proactively detect anomalous activities triggered by malicious access to the
system and thus prevent attackers from accessing to the SCADA resources and applications (Tenet 2); Capability to Exploit the Flaw – By proactively detecting the attacks and responding to them right from the beginning, (within a minute) we will be able to significantly mitigate their impacts and ability to continue with their attacks (Tenet 3).

The topology of the Industrial Control System test-bed that is currently implemented by Raytheon, AVIRTEK, and University of Arizona is shown below. The main goal of the testbed is to experiment with and evaluate the integration of Raytheon and AVIRTEK technologies and Autonomic agents developed at the Center to achieve the following objectives: 1) Autonomic control and management of different power generation technologies; 2) Integrate Raytheon technologies with AVIRTEK Autonomic Software Protection System (ASPS) and Autonomic agents to build the next generation of Autonomic Critical Infrastructure Protection (AutoCiP) system; and 3) Evaluate the autonomic protection strategies against cyber and physical attacks. The test-bed will be an invaluable resource to develop, experiment with and evaluate the security and protection functions and services. The test-bed will address the following issues:

1. **Process Control Zone**: The process control zone provides the main control and management services and functions for the SCADA systems. Typically, it consists of the SCADA Human Machine Interface (HMI) to control and manage the grid resources. The HMI commands include read bus line status, read transformer status, read/ change magnitude and phase angle of the bus have been implemented. The HMI also displays the response received from the Modbus server. Historical data is stored in a database.

2. **Electrical Grid**: We will build a mixed emulation and simulation of electrical grid networks. PowerWorld simulation tools will be used to simulate electrical networks. The PowerWorld is a commercially available simulation program for simulating the operations of large scale power distribution systems. The PowerWorld will be used to simulate the impacts of cyber-attacks on the operations of the electrical grid and also will be used to show how the ASPS-S appliance to secure and protect the electrical grid operations against these attacks.

3. **Internet (WAN) Zone**: This represents the connectivity of smart grids to standard computer networks and Internet. We use OPNET Modeler to simulate a large scale wide area network. We use the system-in-the-loop (SITL) module of OPNET to connect to the control HQ and also the modbus server. These two modules communicate over the simulator network in real-time using modbus over TCP/IP protocol. The simulator also provides statistics and information about the traffic.

4. **Attacks Library**: Some of the common types of attacks on TCP networks are: 1) **Spoofing (Replay attack)**: In this form of attack, captured data from the control/HMI is modified to instantiate activity when received by the device controller.; 2) **Communications hijacking (or man-in-the-middle)**: Involves sending false messages to the MODBUS slave or master by changing the MODBUS packet.

---

Don Cox, Raytheon, and Ph.D Student at UA  
Malaz Mallouhi, Master Student at UA
### Alumni Corner

We are very pleased to see the graduates from our Autonomic Computing Laboratory (previously known as High Performance Distributed Computing (HPDC) Lab, and Internet Technology Laboratory) are doing very well and to connect with them and let them know that we are proud of their achievements and successes. I am sure I missed some of our graduates, please email me your information so we can accurately account for all our Almnis. We will update the list in the next issue and we will put your information on our website at nsfcac.arizona.edu

<table>
<thead>
<tr>
<th>Name</th>
<th>Year of Graduation</th>
<th>Affiliation</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weiming Wang</td>
<td>2001-2002</td>
<td>Dean, Zhejiang Gongshang University</td>
<td><a href="mailto:wmwang@mail.zjgsu.edu.cn">wmwang@mail.zjgsu.edu.cn</a></td>
</tr>
<tr>
<td>Dong xiangdong</td>
<td>2001-2002</td>
<td>Beijing, China</td>
<td><a href="mailto:dongnansheng@hotmail.com">dongnansheng@hotmail.com</a></td>
</tr>
<tr>
<td>Subhra Saha</td>
<td>M.S., 2003</td>
<td>Adtran Inc</td>
<td><a href="mailto:subhrasaha@gmail.com">subhrasaha@gmail.com</a></td>
</tr>
<tr>
<td>Fahd Rasul</td>
<td>M.S., 2005</td>
<td>MBA 2010-2011, Cranfield School of Management</td>
<td><a href="mailto:fahdrasul@gmail.com">fahdrasul@gmail.com</a></td>
</tr>
<tr>
<td>Byoung Uk Kim</td>
<td>Ph.D, 2008</td>
<td>Senior Research Engineer, Ridgetop Group, Inc.</td>
<td><a href="mailto:kimbu0219@gmail.com">kimbu0219@gmail.com</a></td>
</tr>
<tr>
<td>Youssif Al-Nashif</td>
<td>Ph.D., 2008</td>
<td>the Univ. of Arizona Assistant Research Professor</td>
<td><a href="mailto:alnashif@ece.arizona.edu">alnashif@ece.arizona.edu</a></td>
</tr>
<tr>
<td>Dongxiangdong</td>
<td>Ph.D., 2001</td>
<td>Beijing, China</td>
<td><a href="mailto:dongnansheng@hotmail.com">dongnansheng@hotmail.com</a></td>
</tr>
<tr>
<td>Traian Avram</td>
<td>M.S., 2006</td>
<td>EXL Service ROMANIA</td>
<td><a href="mailto:traian.avram@exlservice.com">traian.avram@exlservice.com</a></td>
</tr>
<tr>
<td>Mohamed Djunaedi</td>
<td>M.S., 2001</td>
<td>EMC Corporation</td>
<td><a href="mailto:djunaedi_muhamad@emc.com">djunaedi_muhamad@emc.com</a></td>
</tr>
<tr>
<td>Ishtiaq Hossain</td>
<td>M.S., 2010</td>
<td>Telenav</td>
<td><a href="mailto:ishtiaq.jishan@gmail.com">ishtiaq.jishan@gmail.com</a></td>
</tr>
<tr>
<td>Huoping Chen</td>
<td>Ph.D., 2008</td>
<td>Microsoft/Research Software Design Engineer</td>
<td><a href="mailto:huoping.chen@microsoft.com">huoping.chen@microsoft.com</a></td>
</tr>
<tr>
<td>Byung Uk Kim</td>
<td>Ph.D, 2008</td>
<td>Senior Research Engineer, Ridgetop Group, Inc.</td>
<td><a href="mailto:kimbu0219@gmail.com">kimbu0219@gmail.com</a></td>
</tr>
<tr>
<td>Subhra Saha</td>
<td>M.S., 2003</td>
<td>Adtran Inc</td>
<td><a href="mailto:subhrasaha@gmail.com">subhrasaha@gmail.com</a></td>
</tr>
</tbody>
</table>
Name: Samer Fayssal  
Year of Graduation: Ph.D., 2008  
Affiliation: World Avenue Inc., Florida  
Contact: samerfayssal@gmail.com

Name: Tushneem Dharmagadda  
Year of Graduation: M.S., 2003  
Affiliation: Sr. Intellectual Property Design and Software Applications Engineer, Analog Devices Inc.  
Contact: tushneem@gmail.com

Name: Sridhar H  
Year of Graduation: M.S., 2001  
Affiliation: Sr. Engr. at Silicon Labs, Austin, TX  
Contact: sridhar_125@hotmail.com

Name: Bihika Khargharia  
Year of Graduation: Ph.D., ?  
Affiliation: CISCO  
Contact: bkharhga@cisco.com

Name: Aarthi Arun Kumar  
Year of Graduation: M.S., 2007  
Affiliation: Program Manager, Microsoft Corp  
Contact: aarthi28@gmail.com

Name: Kiran Kumar Modukuri  
Year of Graduation: M.S., ?  
Affiliation: NetApp Inc.  
Contact: kiran.modukuri@gmail.com

Name: Prasad Nellipudi  
Year of Graduation: M.S., 2000  
Affiliation: Technical Marketing Engineer, CISCO  
Contact: prasnell@yahoo.com

Name: Samantha Quadros  
Year of Graduation: M.S., 2001  
Affiliation: NetFlix, Sr. Software Engineer  
Contact: samquadros@yahoo.com

Name: Prasad Vadlamani  
Year of Graduation: M.S., 2004  
Affiliation: Texas Medicaid, Data/BI Architect  
Contact: prasadvadlamani@yahoo.com

Name: Radhakrishnan Vijay  
Year of Graduation: M.S., 2002  
Affiliation: Nokia Siemens Networks, Development Manager  
Contact: vijayr13@yahoo.com

Name: Richard Wang  
Visiting Scholar: 1998-2002  
Affiliation: ITPOINTS  
Contact: wangwei@nj.gov.cn

Name: Jingmei Yang  
Year of Graduation: M.S., 2006  
Affiliation: Care Everywhere  
Contact: jmyanglei@gmail.com

Name: George Zantis  
Year of Graduation: M.S., 2007  
Affiliation: Network Security Engineer  
Contact: gczenator@gmail.com

Name: Yan Wang  
Year of Graduation: M.S., 2006  
Affiliation: Qualcomm  
Contact: yanw@qualcomm.com

Name: Tushneem Dharmagadda  
Year of Graduation: M.S., 2003  
Affiliation: Sr. Intellectual Property Design and Software Applications Engineer, Analog Devices Inc.  
Contact: tushneem@gmail.com
Benefits of NSF CAC Membership

CAC members will have access to leading-edge developments in autonomic computing and to knowledge accumulated by academic researchers and other industry partners. New members will join a growing list of members that includes Intel, Microsoft, Northrop-Grumman, NEC, Raytheon, Xerox, AVIRTEK, Imaginestics, and ISCA Technologies. Benefits of membership include:

- Collaboration with faculty, graduate students, post-doctoral researchers and other center partners;
- Choice of project topics to be funded by members’ own contributions;
- Formal periodic project reviews along with continuous informal interaction and timely access to reports, papers and intellectual property generated by the center.
- Access to unique world-class equipment, facilities, and other CAC infrastructure;
- Internships and recruitment opportunities among excellent graduate students.
- Leveraging of investments, projects and activities by all CAC members.
- Spin-off initiatives leading to new partnerships, customers or teaming for competitive proposals to funded programs.

Funding

Per NSF guidelines, industry and government contributions in the form of annual CAC memberships ($35K/year per regular membership), coupled with baseline funds from NSF and university matching funds, directly support the Center’s expenses for personnel, equipment, travel, and supplies. Memberships provide funds to support the Center’s graduate students on a one-to-one basis, and thus the size of the annual membership fee is directly proportional to the cost of supporting one graduate student, while NSF and university funds support various other costs of operation. Multiple annual memberships may be contributed by any organization wishing to support multiple students and/or projects. The initial operating budget for CAC is projected to be approximately $1.5M/year, including NSF and universities contributions, in an academic environment that is very cost effective. Thus, a single regular membership is an exceptional value. It represents less than 3% of the projected annual budget of the Center yet reaps the full benefit of Center activities, a research program that could be significantly more expensive in an industry or government facility.

To Become a Member Contact us at

Director: Salim Hariri (520) 621-4378 hariri@ece.arizona.edu
Research Director: Youssif Al-Nashif (520)-621-9915 alnashif@ece.arizona.edu
ECE Dept. 1230 E. Speedway Tucson, AZ 85721-0104
http://nsfcac.arizona.edu

Members

![Member Logos](image1.png)