PI Information:
Gail-Joon Ahn
Arizona State University
gahn@asu.edu

Topics:
Cloud Architectures and Systems
Cloud Security, Privacy and Auditing

Current Research Activities:
1. Efficient Provable Data Possession for Hybrid Clouds: Provable data possession is a technique for ensuring the integrity of data in outsourcing storage service. In this work, we propose a cooperative provable data possession scheme in hybrid clouds to support scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data.
2. Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds: In this work, we propose a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. Our audit service is constructed based on the techniques, fragment structure, random sampling and index-hash table, supporting provable updates to outsourced data, and timely abnormal detection.
3. Information Flow Control in Cloud Computing: Even though cloud computing enables us to dynamically provide servers with the ability to address a wide range of needs, this paradigm brings forth many new challenges for the data security and access control as users outsource their sensitive data to clouds, which are beyond the same trusted domain as data owners. A fundamental problem is the existence of insecure information flows due to the fact that a service provider can access multiple virtual machines in clouds. Sensitive information may be leaked to unauthorized customers and such critical information flows could raise conflict-of-interest issues in cloud computing. We propose an approach to enforce the information flow policies at Infrastructure-as-a-Service (IaaS) layer in a cloud computing environment. Especially, we adopt Chinese Wall policies to address the problems of insecure information flow.
4. Realizing a Security Framework in an Education Program: This project aims to address the lack of adequate understanding of security and privacy issues in clouds and the need of high caliber professional ready to design, implement and manage cloud enabled applications and enterprise IT environments. In this work, we propose to develop an architectural framework for secure clouds that provides a basis for implementing a comprehensive educational program focused on security and privacy of cloud based IT infrastructures.

Publications:
1. Hassan Takabi, James Joshi, and **Gail-J. Ahn**, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, November/December 2010.
2. Yan Zhu, Huaixi Wang, Zexing Hu, **Gail-J. Ahn**, Hongxin Hu, Stephen S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. of the 26th ACM Symposium on Applied Computing (SAC), Tunghai University, TaiChung, Taiwan, March 21-24, 2011.
3. Ruoyu Wu, **Gail-J. Ahn**, Mukesh Singhal and Hongxin Hu, "Information Flow Control in Cloud Computing," Proc. of the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing, Chicago, Illinois, USA, October 9-12, 2010.
4. Yan Zhu, Huaixi Wang, Zexing Hu, **Gail-J. Ahn**, Hongxin Hu, and Stephen Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. of 17th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, October 4-8, 2010.

Research Plan:

We have recently observed a new direction in Cloud utilization that involves extensive collaboration among services offered by different Clouds. To take full advantage of collaboration, clients must be given the choice to demand on-the-fly collaborations and resource sharing among different applications, each running in different Clouds that might not have agreements and collaboration tools in place beforehand. To address this, we propose a multi-Cloud system that employs proxies for collaboration.

Although multiple CSPs coexist in clouds and collaborate to provide various services, they might have different security approaches and privacy mechanisms, so we must address heterogeneity among their policies in proxy-based Cloud computing. Proxy nodes need to compose multiple services to enable bigger application services. Therefore, mechanisms are necessary to ensure that such a dynamic collaboration is handled securely and that security breaches such as policy conflicts are effectively monitored during the interoperation process. Existing literature has shown that even though individual domain policies are verified, security violations can easily occur during integration. In Cloud networks, the interactions between different service domains driven by service requirements can be dynamic, transient, and intensive. Thus, policy integration tasks in a proxy node should be able to address challenges such as semantic heterogeneity, secure interoperability, and policy-evolution management. In this task, we focus on access control policies in Clouds so that proxy nodes can carefully manage access control policies while ensuring that policy integration does not lead to any security breaches.

For a collaborative project, a proxy node needs to deal with several registered services from multiple cloud nodes (as well as proxy nodes). This requires policy integration and decomposition to be conducted locally at different proxy nodes. Therefore, it is necessary to articulate the possible policy anomalies including "policy inconsistency" and "policy inefficiency. Policy integration aims to generate agreement on access rights for each party involved in a collaborative project.

Research Tasks:

1. Policy anomalies should be formally devised and corresponding anomaly detection mechanisms should be articulated. We will further articulate patterns of policy anomalies in Cloud computing and efficient detection algorithms will be implemented. In addition, corresponding conflict segmentation discovery module in composite policies will be implemented.
2. Correlated conflicting policies need an effective and efficient resolution approach. We plan to design and develop anomaly resolution mechanisms including effect constraint and resolution algorithms.
3. The policy management model will be a modular component which supports the integration, decomposition, and analysis of policies. During the deployment we will ensure that the policy management model is seamlessly integrated with proxy nodes in our cloud infrastructure. Hence, the outcome of our policy management model will accommodate existing mechanisms in Microsoft Windows Azure platform AppFabric (PaaS) and Cloud Management Console in Xen Server (IaaS). In addition, our modules will be evaluated based on real-world business scenarios as part of collaborative activities with HP labs. The Cloud testbed will be used to collaboratively conduct evaluation as well.