Cloud Computing offers SaaS, PaaS, and IaaS as cost effective ways of doing computation. The recent rapid deployment of Cloud Computing comes with a cost that can leave users open to vulnerabilities such as: Disruptions that may shutdown 24x7 computation availability of essential services since the concentration of government and or multiple businesses resources at a single site is a convenient target for effective cyber-terrorist attacks; Possible theft of Cloud resident software Intellectual Property and confidential Personal Information; and the unwarranted invasions of user data privacy. While this mini-track cannot adequately cover all of the issues with respect to “Secure Cloud Computing,” the presentations of the following five papers will address several of them.

The first paper, “Analysis of Implementations to Secure Git for use as an Encrypted, Distributed Version Control System,” by Russell Shirey, et al., analyzes two existing methods for securing Git repositories, Git-encrypt and Git-crypt, by comparing their performance to the default Git implementation, and examines the tradeoffs made for added security.

The second paper, “DDoS Attacks in Service Clouds,” by Sarra Alqahtani and Rose Gamble of the University of Tulsa, advocates a DDoS detection approach for service clouds, and develops efficient algorithms to resolve the originating service for the attack.

The third paper, “Cloud Incident Data Analytics: Change Point Analysis and Text Visualization,” by Hsia-Ching Chang of the University of North Texas, and Chen-Ya Wang of the National Open University, Taiwan, uses Bayesian change-point analysis to identify the salient changes in cloud incident count data from the Cloutage.org database, as well as text mining techniques with word clouds to visualize non-obvious patterns in this data, to discover both qualitative and quantitative insights into cloud security vulnerabilities.

The forth paper, “What is Really Going On at Your Cloud Service Provider? Creating Trustworthy Certifications by Continuous Auditing” by Sebastian Lins of the University of Cologne, et al., argues that continuous auditing of selected certification criteria is required to assure continuously reliable, as well as trustworthy secure cloud services.

The fifth paper, “PiMiCo: Privacy Preservations via Migration in Collaborative Mobile Clouds,” by Kaushik Ravichandran of the Georgia Institute of Technology, et al, describes work that has as a goal to introduce and discuss the design of a privacy preserving, data centric programming model for building collaborative applications in large scale mobile clouds.