July 2014 Federal Cloud Computing Summit Summary

Karen Caraway, Don Faatz, Nancy Ross, Justin F. Brunelle
The MITRE Corporation

Tom Suder
The Advanced Technology Academic Research Center

Abstract

The latest installment of the Federal Cloud Computing Summit took place on July 8th-9th, 2014. The Summit began on July 8th with the MITRE-Advanced Technology Academic Research Center (ATARC) Collaboration Sessions that allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss the government's challenge areas in cloud computing. The goal of the collaboration sessions is to create a forum for an exchange of ideas and a way to create recommendations to further the adoption and advancement of cloud computing within the Government.

The MITRE Corporation is a not-for-profit company that operates multiple federally funded research and development centers (FFRDCs). ATARC is a non-profit organization that leverages academia to bridge between Government and Corporate participation. MITRE worked in partnership with the ATARC to host these collaborative sessions as part of the Federal Cloud Computing Summit. The invited collaboration session participants across Government, Industry and Academia worked together to address challenge areas in cloud computing, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce hire-ready graduates to advance the state of cloud computing in the government.

Several recommendations were made as a result of the exchange of ideas in the collaboration sessions. This white paper summarizes these results, as well as identifies recommendations for government and academia while identifying orthogonal points between challenge areas. It also recommends an increase in cross-government and academic collaboration to share best practices and address cross-cutting challenges.

Collaboration Session Outcomes

Each MITRE-ATARC Collaboration Session was a focused and moderated discussion among government, industry, academic, and MITRE representatives about a cloud computing challenge area.

Three separate sessions were held, individually focusing on:

- Cloud Computing in Austere Environments/Cloud Computing for the Mobile Worker
- Security as a Service
- Impact of Cloud Computing on the Enterprise

Participants discussed current problems, gaps in work programs, potential solutions, and ways forward for each of the challenge areas. This section outlines the goals, outcomes and summary of each of the collaboration sessions.

Cloud Computing in Austere Environments/Cloud Computing for the Mobile Worker Session

The joint Cloud Computing in Austere Environments/Cloud Computing for the Mobile Worker session was a consolidated session that discussed the challenges of utilizing cloud computing resources in austere environments (or disconnected, intermittent, and limited (DIL) environments) and utilizing cloud computing resources through mobile devices. The goal of the joint session was to outline recommendations for operating in tactical and network challenged environments, utilizing cloud resources from thin-client devices, and consuming cloud-based data and services through DIL networks. These goals all centered around utilizing elastic and scalable cloud computing resources in efficient ways regardless of client or access mechanism.

The goals of this session included discussions of the following:

- Recommendations for accessing cloud computing resources;
- Government challenges when accessing data;
- Network restrictions and access policies; and
- Convergence of mobile and cloud computing resources.

The discussions identified the following needs:

- Ability to prioritize messages and synchronize data efficiently;
- Push data to the point of need and ability to offload mobile data to a cloud;
- Protocol agnostic localized data dissemination and data pre-processing;
- Use clouds for decision making and mobile devices for data collection and consumption; and
- Utilization of federated technologies and federated clouds to achieve the mission.

The summary of the collaboration session is below:

The joint Cloud Computing in Austere Environments/Cloud Computing for the Mobile Worker session focused on the challenges with accessing cloud services from thin mobile clients and utilizing cloud services in DIL environments. Austere environments and access from mobile devices have similar challenges in that data must be prioritized for transmission and processed at a remote cloud because the local devices are limited in their capabilities. The session discussions identified two use cases: the need to access and synchronize data in a disconnected environment and the need to prioritize messages and data during consumption and transmission.

When using mobile devices and thin clients, particularly in DIL environments, the clients should be pre-populated with mission-critical data to maximize network efficiency and operational capability. That is, data should be pre-populated since it will assuredly be needed and pre-population will alleviate the load on the network. A multi-tiered cloud approach should be implemented in disconnected environments in which mobile devices synchronize locally with a limited capability cloud environment. This method of tiered synchronization with tiered clouds can provide a localized private cloud for immediate computation capability and mobile offloading of data. Mobile applications should be designed to prioritize data transmission to localize computing environments during offloading even when fully connected to ease the load on the network. The most important data should be offloaded to the cloud first, which requires data be prioritized on the client.

During points of connectivity, cloud environments should be able to consume and disseminate data agnostic to data protocols (e.g., wireless, 4G, cellular). Because mobile and thin client devices do not have the computational ability of a cloud environment or are limited because of their battery power, the mobile devices should be utilized for data creation and collection and the cloud should process the collected data to generate decisions. However, this creates two competing use cases: the need to aggregate information to draw conclusions and the need to decide what data is most important for offloading to the cloud. Some data becomes important only after aggregated with other data. As such, the joint mobile-cloud communication system should determine if a decision can be made using the local data, and in the absence of a decision should synchronize data with a higher-tiered cloud until a decision can be made.

The session attendees determined that a federated cloud (i.e., multiple providers, and multiple tiers of clouds that can be accessible across silos) is the best approach for mobile devices and austere environments. Additionally, the cloud enables the use of mobile technologies due to the increased computation power from the cloud. Ultimately, a federated approach incorporating emerging technologies (i.e., Internet of Things (IoT), mobile, and cloud computing) provides the highest impact system.

Top Discussion Points:

- Pre-populate mission critical data
- Collect at the mobile device, process in the cloud
- Data movement should be protocol-agnostic
- Lightweight “smart” analytics for local data processing on mobile devices

Security as a Service Session

The Security as a Service session was intended to explore security issues in the cloud as offered by third parties. The goal of the session was to outline recommendations for constructing contractual security agreements, accessing security by third party providers, and utilizing and extending security principles into cloud environments. These goals all centered on the need for common security policies and acquisition processes to ensure secure computing.

The goals of this session included:

- Identifying contractual considerations for ensuring security;
- The offer and inclusion of security services by third parties;
- Discussing FedRAMP and other standards; and
- Identifying how the adoption of cloud computing changes security considerations for the Government.

This session identified the following needs:

- The acquisition process needs to adapt to focus on services rather than "widgets;"
- Data is increasingly the focus of protection, and services should focus on it, as well;
- Agencies need standardized, common shared services with agency-specific security polices;
- CIO-level decision makers are not incentivized to accept the risks or give up the control that accompanies moving to a cloud; and
- Vendor services must be integrated to provide metrics for FISMA scoring.

The summary of the collaboration session is below:

The Security as a Service session discussions focused on incentivizing data protection and policy development. The general consensus was that the acquisition process plays a role in cloud security. The acquisition process – and therefore the security validation – can be improved by migrating away from the process used to acquire enterprise services and towards a more agile process for acquiring widgets. Widgets have different security needs than the enterprise services.

Data is the focus of data protection and should therefore be the central concept when defining security policy. This is the ultimate target of protection and security measures – the cloud services themselves are designed around data, and it follows that the security policies should also be designed around data protection.

Government organizations are increasingly defining in-house, customized security polices and services. To increase Government collaboration as well as reduce vetting and approval times, standardized security polices and services should be established. The overall consensus in the session is that FISMA scoring and FedRAMP are great initial steps, but there is work left to be done to refine the process and policies. For example, vendor services and other established practices have not yet been integrated into FISMA scoring.

A primary challenge of implementing cloud computing in a Government setting is that it introduces a level of risk into the practices (but not definitively more risk than legacy systems). Currently, decision makers are not incentivized to introduce risk or give up system control. A cultural shift to reward calculated risks that have potentially exponential benefit will help alleviate this challenge.

Finally, the session cited a lack of sharing and collaboration within the inter- and intra-organizational cultures. An effort should be made to enable sharing of ideas, best practices, and cross-cutting solutions within the Government.

Top Discussion Points:

- Acquisition must move to a more agile process for cloud capabilities without losing sight of security.
- Data should be the focus of security protections, and the services to process that data, rather than the current enterprise focus.
- Government policies and processes are making progress, but must continue to be refined and streamlined to reduce vetting and approval times
- Risk/reward ratios do not currently tip toward encouraging decision makers to utilize cloud computing

Impact of Cloud Computing on the Enterprise Session

The Impact of Cloud Computing on the Enterprise session was intended to explore the impact of cloud computing on government operations from both the practitioner (i.e., cloud developer, implementer, and user) and CIO levels. The goal of the session was to discuss challenges in and outline recommendations for budgeting, acquisition, and procurement of elastic and on-demand cloud computing resources. These goals all centered on the unique challenges that cloud computing introduces to these government processes and how to approach the challenges.

The goals of this session included:

- Discuss how the adoption of cloud computing changes enterprise-level operations;
- Identify and discuss budgeting, acquisition, and procurement challenges;
- Discuss how to enable the cultural shifts that will help ease the adoption of cloud; and
- Discuss how the practices of industry be adopted to help make cloud computing more realistic.

This session identified the following needs:

- Identify low risk/high value opportunities to allow starting small, failing fast, and rapid scaling;
- Share successes, best practices, and use cases across the Government to allow better communication;
- Reach beyond the federal level to the state and local levels of Government;
- Elevate the conversation beyond a technical issue to communicate challenges with security, business, needs, and agency level policy; and
- Re-tooling and re-training the practitioners, including the non-technical practitioners and decision makers.

The summary of the collaboration session is below:

The Impact of Cloud Computing on the Enterprise session discussions identified the current challenge areas of adopting cloud computing in the Government as procurement, security, training, finance, and policy. That is, there are challenges associated with selecting, vetting, and acquiring a cloud

service; identifying the security qualifications of the service and provider; obtaining qualified staff to implement the cloud service; budgeting and paying for an elastic service; and the culture of use around cloud computing.

To alleviate some of the cultural, procurement and financial risks, an agile model of adopting cloud services should be implemented. In keeping with agile practices, a policy of prototyping and *starting small* allows a low-risk, fail early system to refine best practices at low cost. Additionally, it allows the service to be scaled up quickly – a core principle of cloud computing. By selecting high value target opportunities, the impact of scaling quickly is optimized.

Recommendations for mitigating procurement risks included establishing pricing models to support a cloud business model vs. the traditional "hardware buy" model in which hardware and associated services are purchased. Firm fixed pricing models do not have the flexibility required to leverage the scaling benefits (e.g., bursting) that cloud offers to the enterprise. Contract Line Item (CLIN) structures need to be reassessed so that they do not unintentionally lock out medium sized companies who offer cloud solutions. A menu of services model is better suited to cloud procurements than the current task procurement construct. There is also a need to consider open market vs. FAR regulated procurements. Finally, the "color of money" and how cloud procurements are funded at the agency level needs to be reviewed to ensure the success of small, initial cloud procurements and sustainment of broader, enterprise-wide procurements in the future.

Security related recommendations included the simplification of a lengthy and costly compliance/certification process; identify the applications that do not contain sensitive data as candidates for successful cloud adoption while waiting for IA/PII data protection policy to be established; understand the implications of non-CSPs (Cloud Service Providers) carrying the burdens and risks of securing data in the cloud.

Qualified cloud subject matter experts are often difficult to hire and are in high demand among industry and government. To mitigate the difficulty of finding experts, the existing government practitioners should be re-trained to better understand the intricacies of adopting a cloud computing service as well as the technical aspects of implementing and delivering the service. CSP-centric security policies and practices need to be developed.

In the area of policy, recommendations focused on reviewing agency-level policies and practices to ensure that they do not prevent or inhibit cloud procurements. Better understanding of data ownership and governance is also needed.

Along with the other sessions, this session identified a need to foster and enable collaboration and communication across the Government. Successful Government use of cloud computing is not limited to the federal level, and state and local governments should be included in the collaboration.

Decision makers should be made aware of the non-technical challenges, advancements, and other aspects of cloud computing. The consensus of the session is that decision makers have preconceived notions or biases with respect to cloud computing and should be made aware of new challenges as well as

advancements that mitigate existing challenges. This practice will help enable the cultural shift toward adopting and accepting cloud computing as a viable Government tool.

Top Discussion Points

- Adopt an agile model
- Encourage small failures to find the best approaches
- Encourage re-training and re-tooling of staff to support new technologies
- Evaluate cloud pricing and purchasing strategies to alleviate contract/FAR purchasing limitations on current approaches
- Include state and local governments in the collaboration of enterprise cloud implementers

Summit Recommendations

Each collaboration session produced common themes. In general, Government cloud computing struggles with security concerns and standards, acquisition processes, budgeting and procurement, and disconnected efforts. With these cross-cutting challenges in mind, the collaboration sessions made the following high-level recommendations for the Government when implementing cloud computing:

- Identify low risk targets to initially implement;
- Pilot and test early and often to fail early with low impact;
- Lessons learned need to be shared across the Government;
- State and local governments should be included in information sharing – not just Federal;
- Identification and prioritization of high-priority data;
- Focus on the management of data and the use of cloud technologies as a tool; and
- Educate the decision makers on the cloud implementation challenges.

Cloud computing – and the associated technology – is ready to be implemented by the enterprise, but the enterprise is not ready (at the policy level) to implement cloud computing most efficiently. An organizational, business, and cultural change needs to occur to enable cloud computing to be readily adopted. To facilitate this change, the Government should treat the cloud as a tool that needs to be federated and shared – rather than isolating clouds in silos or swim lanes – including at the cloud service provider level – prevents interoperability and the sharing benefits that come with cloud computing.

Migrating legacy systems to cloud environments is a cross-Government challenge that should be approached through information sharing and improved standards. A need was identified during the collaboration session out-brief for a migration suitability tool.

Data formatting, metadata sharing, and interoperability were identified as key aspects of improving cloud computing for Government use. The incorporation of federated clouds (e.g., integrating multiple cloud providers and multiple cloud services) and emerging technologies (i.e., mobile and IoT) will help provide higher-impact systems and mission components within the Government. Each of these emerging technologies enables and helps advance the state of the art of the others.

The consensus of the collaboration sessions is that cloud computing may or may not offer efficiency benefits (such as cost benefits) but instead the larger benefit of implementing cloud computing is the performance improvements (such as the additional features and capabilities that can be performed) through implementing cloud computing.

Academia can provide strong technical resources and insights into the challenge areas discussed. To alleviate the burden on the Government, academics should be included in the planning and research processes to help provide technical input. Qualified cloud practitioners are in high-demand, and universities can help provide access to researchers and work with Government to identify high value concepts that can help prepare graduates for Government cloud employment.

Working groups should also be held to allow cross-Government collaboration and discussion to ensure best practices are shared. In conjunction with the Federal Cloud Computing Summit, specialized Government-only working groups should be established to allow specific solutions and Government programs to be discussed.

Moving forward, Federal Summits and specialized working groups that help broker the conversation within Government and between Government, Academia, and Industry will continue to provide high value impacts for Government cloud practitioners.

Conclusion

The July 2014 Federal Cloud Computing Summit highlighted several challenges facing the Federal Government's adoption of cloud computing. The challenges were not compartmentalized based on the challenge areas at the Summit, but span across the discussions by Government cloud practitioners. Specifically, cultural challenges and technical understanding remain difficulties to be overcome. The adoption of agile processes, increased collaboration, and improved education and training can help mitigate the identified challenges.

From these recommendations, Government practitioners (at all levels of Government) should participate in special interest groups or working groups to increase collaboration; continue to influence standards development within the discipline; and continue to partner with academia to leverage cross-cutting research and to help train the Government workforce.

The authors' affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

Approved for Public Release; Distribution Unlimited. Case Number 14-3272