JULY 2016
FEDERAL CLOUD COMPUTING SUMMIT REPORT[*]

October 5, 2016

Justin F. Brunelle, Demetrius Davis, Nicole Gong, Duy Huynh,
Michael Kristan, and Mano Malayanur
The MITRE Corporation[†]

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

[*] APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 16-3496. **©2016 THE MITRE CORPORATION. ALL RIGHTS RESERVED.**

[†] 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 authors.

Contents

1 Abstract

The most recent installment of the Federal Cloud Computing Summit, held on January 13th, 2016, included five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions. These collaboration sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in cloud computing. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of cloud computing techniques and best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in federal cloud computing: DevOps vs NoOps: Managing Public Clouds; Secure Cloud Access: From APIs to Mobile & IoT Devices; Workload Management for Cost Savings; Cloud Category Management; and HealthTrac Sponsored Session: Using Cloud in Healthcare.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government, academia, and industry while identifying intersecting points among challenge areas. The sessions identified actionable recommendations for the government, academia, and industry which are summarized below:

> As cloud computing adoption becomes increasingly prevalent, more granular challenges are arising (e.g., with respect to specific adoption of DevOps practices).
>
> As cloud environments become more secure, the security of access points is of increasing concern especially when considering Internet of Things devices. However, mobile computing offers models of implementing security in these scenarios.
>
> Interoperability is emerging as a primary concern whether considering security, vendor lock-in, or hybrid cloud environments. Specifically, data sharing and multi-party access were cited as primary challenges.

2 Introduction

During the most recent Federal Cloud Computing Summit, held on January 13th, 2016, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in cloud computing. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of cloud computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs) [12]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology. MITRE works in partnership with 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 graduates ready to join the work force and advance the state of cloud computing research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 Collaboration Session Overview

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

- DevOps vs NoOps: Managing Public Clouds
- Secure Cloud Access: From APIs to Mobile & IoT Devices
- Workload Management for Cost Savings

- Cloud Category Management
- HealthTrac Sponsored Session: Using Cloud in Healthcare

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 DevOps vs NoOps: Managing Public Clouds

The *DevOps vs NoOps: Managing Public Clouds* session focused on defining what DevOps and NoOps meant in the context of the federal government and how an agency can effectively use principles of DevOps to drive mission success. Just as agile started to make its way into the government in the previous decade,a DevOps culture can emerge into the government so long as all stakeholders are willing to embrace that some of the ways of doing business are different.

Reflecting the range of concerns associated with the session topic, a relatively large set of concerns was posited for discussion, including:

- The need for collaboration and feedback from all engaged stakeholders.
- Quantifying the benefits of DevOps through measurable metrics.
- Building DevOps into contracting language for outsourcing and acquisition.

Cloud is widely accepted as an enabler of DevOps. However, the discussion focused more on business processes instead of specific technologies. DevOps was also considered to be a means to an end; at the end of the day, if the mission did not succeed, it does not matter how the execution went about. The example given by the government lead was a mobile application that was designed to increase community recreational awareness and involvement from youth. He made the statement "if the mission was to get more kids to go outdoors and visit the park, it doesn't matter if you came in under budget or had faster software releases if no additional kids came to the park."

3.1.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *DevOps vs NoOps: Managing Public Clouds*:

- Security and accreditation are ongoing challenges. In order to increase velocity (i.e., the rate of adoption), the government needs to engage with security personnel up-front and build compliance and verification into the software delivery pipeline.
- Some organizations and agencies have multiple stakeholders that have different schedules/cycles. Granularity needs to be standardized and that Integrated Planning Teams (IPTs) are necessary as at some point there is one common superior stakeholder.
- Sometimes organizations or individuals are not comfortable with frequent learning and sharing activities. Establishing daily stand up status meetings and cross-organizational artifact repositories will aid in knowledge sharing.

3.1.2 Discussion Summary

The following items were among the most actively discussed in this context:

- Municipal governments are small enough where there is no distinction between development and operations teams. This makes implementation of DevOps easier to accomplish.
- GSA's 18F group [6] is an example of driving innovation and transforming via consultations with various government organizations.
- If a stakeholder adopts open source code and the end user fixes a bug, the user starts to become an owner and stakeholder of this service.
- Metrics that can measure DevOps success include
  - Cost
  - Time (Time to develop, deploy, market, repair)
  - Quality
  - Defects, bugs, or vulnerabilities

There are a couple of things to consider when trying to bring around transformational change and the principles surrounding DevOps are one of those game changers with several important characteristics. First, the government stakeholders and owners do not want to disrupt the mission of the end users. Second, the government needs to work around the current business processes that exist such as those that center around acquisition and compliance. While many end users and stakeholders cannot change laws overnight, they need to adhere to these policies while informing decision makers about the need for change. As noted in the IEEE publication, DevOps for Federal Acquisition [1], the government needs to comply with different funding sources, making sure that requirements are well-defined but yet flexible enough to adapt to rapid deployments, and furthermore make sure that the government can maintain a level of security accreditation even though the pace of change is greatly increased. When surveying job postings or attending local meet-ups, one can find that there is a lot of buzz around terms such as Cloud and DevOps. There is a strong demand signal for individuals who have experience in both software development and running large IT production systems. The session participants mentioned seeing a lot of talented, smart people who are looking for an opportunity to transform a product or system using these new technologies. This is evidence of an opportunity for government to capitalize on this hot area and perhaps start with a few smaller tasks to pilot. The risk of not evolving is that the government will not be able to keep up with the rapid rate of innovation with technology. Every few months, some new game-changer breaks out and commercial companies are quick to adopt. If software requirements and delivery cycles still takes months or longer, adopters will not be able to incorporate these new innovations for quite some time. The session participants also see that in many cases one organization is still responsible for development but then they defer ownership and management to the operations team. Those organizations can still exist but they need to have the freedom to operate as one cohesive team and that is something that the government adopters can encourage through success stories and recommendations for policy changes.

3.1.3 Recommendations

The participants in the *DevOps vs NoOps: Managing Public Clouds* collaboration session identified the following important findings and recommendations:

- Build collaboration into contracting language up front. Avoid feature-driven contracts and mandate training (knowledge transfer) and collaboration for each contractor.
- When budgeting for DevOps projects, avoid silos such as only involving the operations teams for hardware specification and procurement.
- Shift the requirements process from being functional-driven to user-driven.

DevOps is not about avoiding failure, but instead is about embracing failure, failing fast, and always communicating. The challenge area discussion group understands that it is unlikely the mission critical or life supporting/threatening systems will be early adopters. New start projects will likely have quicker success compared to retrofitting existing projects. As contracts are renewed, they are great opportunities to insert language that would foster a greater collaborative DevOps culture within any IT program.

3.2 Secure Cloud Access: From APIs to Mobile & IoT Devices

The *Secure Cloud Access: From APIs to Mobile & IoT Devices* session had several goals centered around identifying security challenges with accessing cloud services – a complementary concept to securing data within a cloud – and the challenges, best practices, and recommendations for securing the devices that connect to our cloud services. With one of the recommendations from the January 2016 Cloud Summit [4] emphasizing the need to secure cloud-facing end-points, this session was designed to address the security of cloud service consuming devices.

Reflecting the range of concerns associated with the session topic, a relatively large set of concerns was posited for discussion, including:

- Identify best practices, challenges, and security concerns unique to protecting cloud access points
- Identify preferred methods for consuming cloud services from mobile devices
- Recommend preparations for securing Internet of Things (IoT) devices that connect to cloud systems

The session participants discussed several challenges, recommendations, and projected future developments around these overarching challenges and their more specific sub-challenges in this session.

3.2.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *Secure Cloud Access: From APIs to Mobile & IoT Devices*:

- Partner access (e.g., via Virtual Private Network (VPN)) can be challenging from mobile and thin clients
- IoT is especially susceptible to man-in-the-middle attacks

- Government security needs are different than traditional consumers' security needs; a vendor's goal is to satisfy customers' needs

3.2.2 Discussion Summary

The participants in the *Secure Cloud Access: From APIs to Mobile & IoT Devices* session included a very deep technical discussion of cloud security challenges.

The following items were among the most actively discussed in this context:

- Existing models of using mobile devices can be re-used for IoT
- Security standards and acquisition challenges exist and are evolving
- Vendor business models do not always allow for or address government goals and needs

Primarily, this session discussed mobile computing models that can be reused for IoT services or for cloud Application Programming Interfaces (API) designs. As always, standardization and acquisition were mentioned as a challenge, but in this session these perennial challenges were applied to machine-to-machine operations and communications with specific attention to how this differs from human-in-the-loop operations. IoT also introduces new challenges with scale, authentication, and communication with machine-to-machine and human-to-machine trust models as well as interoperability within clouds and consumers of cloud services.

The session participants also discussed the impact of the need to scale services and the difficulties with matching the scale of device authentication, device integrity, and human involvement in the security process. This may impact the need for applications to be re-architected by application owners to match this scale, provide improved authentication and security management, or even incorporate a third part security tier. Further, vendors provide products for general users whose security needs differ from the security needs of government. The session participants recommended helping vendors understand the outcomes desired from their end devices and the protections required for the data rather than being prescriptive in their process for addressing those security concerns.

Finally, the session participants discussed the future advances in security and protections to include software defined environments, networks, and improvements to Trusted Internet Connections (TICs) that will help improve security going forward.

3.2.3 Recommendations

The participants in the *Secure Cloud Access: From APIs to Mobile & IoT Devices* collaboration session identified the following important findings and recommendations:

- Define specific desired outcomes from vendors rather than dictating procedure
- Consider refactoring applications when necessary
- TIC overlays will help achieve cloud endpoint security
- Cloud owners should adopt risk management rather than risk avoidance

The challenge area discussion group made recommendations for helping adopt improved security challenges for protecting data at the point of access to complement the security practices being developed within cloud environments.

3.3 Workload Management for Cost Savings

The *Workload Management for Cost Savings* session discussed challenges with managing a workload in the cloud with specific attention to the impact workload has on cost of operating within a cloud environment.

Reflecting the range of concerns associated with the session topic, a relatively large set of concerns was posited for discussion, including:

- Identify whether cost mitigation is most effectively managed through customer controlled usage or through Cloud Service Provider (CSP) adherence to contracts
- Identify the importance of load balance to mitigate cost
- Identify aspects of preparing for offloading on cost

The session participants discussed recommendations for managing their workload in relation to these challenges.

3.3.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs that might be met by applying existing or developing new *Workload Management for Cost Savings*:

- Current cost estimation models work in only homogeneous cloud environments
- Interoperability between clouds is a main cost concern, particularly for vendor lock-in
- Addressing security challenges is a major cost driver

3.3.2 Discussion Summary

This session discussed enabling decision making around workload migration and supporting workloads in a hybrid cloud environment. When discussing workload migration decision making, a distinction between lift and shift and associated migration costs as compared to operation enhancement is important. Clear definition of goals and establishing best practices using small test cases and success stories is important for migrating larger systems and services. With respect to hybrid environments, automation can be challenging when moving workloads between private and public portions of the cloud. Further, moving data and balancing capacity and Return on Investment (ROI) are challenges in a hybrid environment.

The following items were among the most actively discussed in this context:

- Pay-by-the-drink models of billing
- Cloud migration plans (e.g., *lift-and-shift* vs end of life)
- Optimizing existing applications (e.g., after the *lift-and-shift*)

However, these recommendations and topics were not necessarily clear-cut. For example, monetary impact is not the sole factor in migration; mission-critical workloads (e.g., for healthcare) were exempt from these calculations. Even considering this notion, validating and defending a cloud migration is a remaining challenge for cloud adopters.

Defining costs for migrating to a variety of environments is also challenge; for example, migrating from all-legacy to all-private, hybrid, and all-public clouds vary when being estimated. However, pay-by-the-drink models of billing helped overcome some of the estimation and management challenges. Even considering each method of estimating cost migrations can vary. Some experts cite that migrating to a cloud may offer no cost savings regardless of management policies for the workload, while other government agencies cited significant cost savings by migrating and managing their workload.

To identify an agency's management practices, the attendees recommended an initial, small, *lift-and-shift* migration to refine their process and identify potential cost savings within the first year. This will help forecast cost savings beyond the first year. Using applications with minimal Personally Identifiable Information (PII) and other security challenges is preferred;

the participants cited FedRAMP and other security processes as impediments to the migration process.

3.3.3 Recommendations

The participants in the *Workload Management for Cost Savings* collaboration session identified the following important findings and recommendations:

- Concentrate cost decision making around workload migration
- Create or use tools for workload management in hybrid environments
- Adopt organizational change management to improve communication, allow culture to shift, and enable cost savings

The challenge area discussion group distilled their discussions and recommendations into the above three recommendations. By enabling decision making around workload migration, cloud adopters can focus on what should be migrated to which cloud environments at a desired timeline with a recommended migration approach (i.e., the answers to what?, when?, where?, and how?). With an increasing emphasis on adopting hybrid environments, cloud adopters need methods to support workload management in a hybrid cloud. For example, automation and interoperability will be a challenge depending on the mix of environments. Portability when migrated between the two environments is also a challenge. Cloud bursting and adjusting each cloud's capacity are also challenges that would benefit from hybrid cloud management tools or general procedures. Finally, organizational change management adoption can address improved communication, a more adoptive culture, and techniques for cost savings when migrating and managing cloud environments.

3.4 Cloud Category Management

The *Cloud Category Management* session goals included identifying targets of migration and designing the most effective cloud platform. A well designed end-to-end integrated category management plan will allow organizations to maximize the cloud's capabilities, drive growth, profitability, and optimize value. Specifically, the session aimed to identify best practices and recommendations for identifying the proper environment and selecting the appropriate services for initial migration into the cloud.

Reflecting the range of concerns associated with the session topic, a relatively large set of concerns was posited for discussion, including:

- Recommend methods of identifying migration targets
- Identify best practices, environments, or services (e.g, IaaS) to target for first migrations
- Identify impact of cloud design on migration planning

The attendees in this session has a diversified background in cloud migration areas; the following roles are identified:

- Cloud administrators
- Policy supporters – data center operation initiative
- Business developers
- Engineers
- Security architects
- Cloud migration architect
- Application migration practitioners

3.4.1 Challenges

The collaboration session discussions identified the challenges that are targets of government cloud adopters and the associated needs that might be met by applying existing or developing new *Cloud Category Management.* The below list identifies challenges that organizations encountered, opportunities for research and applied solutions, and opportunities to make cloud migration more effective.

Make preparatory efforts to success in an initial migration: This provides an opportunity to perform vendor assessment: Which vendors will get it right first? Which will guarantee delivery? What if the cloud fails? Where are the standards? What level of transparency do you need? There is an opportunity for an initial pilot.

Migrate to cloud first, and revise data center impact after the migration: This creates an opportunity to apply Gartner best practice [9]: How will you create a compelling cloud vision? What strategies will better align business and IT? How should you measure business value? Is cloud technology selection really the easiest part? Further, Gartner's 5 Rs of migration [5] should be considered (i.e., rehost, refactor, revise, rebuild, replace).

Vendor transitions This creates an opportunity to establish an exit strategy.

Collapse of the data center: The "collapse of the data center" has created an opportunity for migrating to a cloud environment.

Fear of change: As with prior cloud summits [2, 3, 4], a cultural aversion to adopting cloud creates an opportunity for cloud adopters to also adopt new DevOps and agile practices not just in their data management, but as an overall culture and mindset. Further, this is an opportunity to establish training for policy makers and practitioners.

New application locations: By migrating applications to a cloud environment, they can be refactored to perform more efficient and effectively.

Fixed cost vs "pay by the drink" models: Paying for what you use allows for dynamic scalability. One of the most distinguishing features of cloud based application platforms is the ability to dynamically adjust the computing resources available to an application, and pay for those resources accordingly. The key is that organization may need to make adjustments to its procedures and policies to ensure that the utilization of cloud computing resources is monitored and controlled. Otherwise, the cost could be great.

Contracting vehicles: Opportunity to use NIST SLAs 19086 [10] as guidance to improve agreements.

Low hanging fruit: Easy migration targets can help refine the cloud migration practice by providing an opportunity to fail early and at a policy level rather than technical.

Small applications: Opportunity for application consolidation and provides initial migration targets.

Opportunities for failing and pilot: Failing early allows an organization an opportunity to revisit migration strategies and refine their migration practices.

PII Using PII in the cloud creates an opportunity to examine the data protection. How will you protect your data in the cloud? What is the right level of recovery and manageability in your organization? What security controls should you inject? Who will have access? Should you use data tokenization? How will you migrate your data?

3.4.2 Discussion Summary

This session discussed drivers for application migration to cloud, such as cost, economies of scale, measured provisioning, federal mandates, and increased productivity. Identifying the where of a migration plan is essential; the Gartner Methodology for migration is particularly helpful (tolerate, invest, eliminate, migrate) (Figure 1[1]). Two questions factor into the migration decisions such as how to identify what needs to move as well as how is the migration going to be effective. Identifying target technologies, timelines, challenges, vendors, and

[1] Image from `http://www.raamstijn.nl/eenblogjeom/images/stories/time%20gartner.jpg`.

training should help inform the ROI of different cloud categories. Further, categories should be standardized as models for goals such as meeting mandates, application migration, and sensitive data (e.g., PII).

The discussion started with first identifying the business drives for migration, the team explored the factors that would guide a cloud migration strategy, for example:

Determine the business drives for migration:

- Why? When?
- Effective productivities
- Technology refresh
- Mandates vs policies
- Enhance productivity and security
- Life cycle management
- Streamline operations and consistent
- Business continuity, disaster recovery and coop
- Automation

Cloud Selection IaaS, PaaS, SaaS The team identified following things to consider:

- Which migration target?
- Are you services ready for migration?
- On-premises vs Off-premises
- How much do you need (e.g., storage, compute power)?
- Cost: How much do you need vs how much is available?
- Fixed vs Variable cost models
- Is co-location is an option?
- What type support or licensing do you need?

In order to answer the questions listed above, an organization needs to understand the existing data center investment, for example:

- Identify costs associated with deploying on-premises servers
- Pilot using existing servers, license, hardware resource consumption
- Consider integrating a cloud services roadmap into the hardware lifecycle policy

Understand Application Requirements for a Cloud Migration

- Application inventory
- The performance consideration
- The application portability consideration include an application's external dependencies that rule out (or greatly complicate) a cloud migration and older applications that run on legacy operating systems may render a move to the cloud as infeasible
- While a cloud service provider can usually scale its offerings to meet even the most demanding workloads, this scalability comes at a price
- The ability for a workload to be virtualized is a key concern
- Evaluate costs

Understand Cloud Infrastructure Considerations

- For an on-premises network option, if the plan is to keep resources on-premises (even temporarily), the cloud network must function as an extension of the on-premises Active Directory forest. This means that cloud-based domain controllers, Domain Name Service (DNS) servers and other servers all have to be deployed. More importantly, the organization will have to figure out how to establish a secure communications path between the cloud-based virtual network and the on-premises network.
- While anticipating the risks and benefits of cloud migration, it is important to keep in mind that cloud migrations are not an "all-or-nothing" proposition. Organizations do not have to go "all in" with cloud migrations. In most cases, it will make sense to move certain services to the cloud while continuing to operate others on-premises.
- Choosing the right cloud environment (e.g., public, private, hybrid clouds) is key to the decision making process.

The session participants identified a series of steps to aid with cloud migration:

Step 1: Migration Candidates Discovery Analysis Perform a technology assessment to assess what components will be impacted by the migration:

- Servers
- Data
- Application
- Service needed
- Legacy application characteristics
- Security considerations
- Overall inventory, including business owner, data ownership
- Cost Benefit Analysis (CBA)
- Resources

Step 2: Technology Analysis: What do I have and where should I put it? Evaluating the current services targetted for migration and the most suitable cloud architecture target is the next step in the migration process.

- Requirement and constraints analysis
- Modernization requirements
- Development and operations skills constraints
- Application mobility
- Transform data
- Outage to move
- Data security
- New features to add
- Down time
- Infrastructure refresh

Step 3: Planning the migration Once the migration and cloud targets are defined, the migration process can be planned.

- Timeline and interdependency deconfliction
- Cost of migration
- Upfront analysis
- Training
- Piloting the strategy
- Ensuring continuity in the cloud
- Evaluate success and actual vs predicted cost

Step 4: DevOps Management Feedback loop

- Manage the infrastructure
- Manage the users
- Monitor the return on investment
- Continue update and upgrade
- Continue to refine SLAs as needed
- Continue monitoring post migration components

3.4.3 Recommendations

The participants in the *Cloud Category Management* collaboration session identified the following important findings and recommendations:

- Continually evaluate cloud migration successes and refine the migration process
- Develop and follow a cloud migration framework
- Technology is not the only impacted cloud migration target; consider DevOps and operations management changes when considering cloud migrations

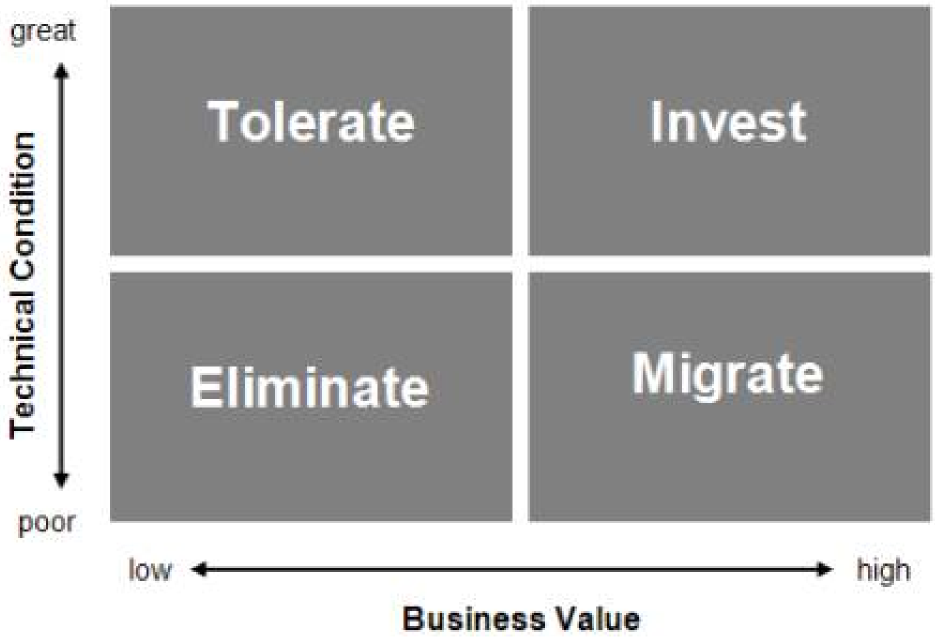

Figure 1: Gartner's time model provides guidance on migrating applications to the cloud.

The session participants also recommended referring to Gartner's Time Model (Figure 1) when evaluating services for migration.

The challenge area discussion group made very specific recommendations regarding cloud migration considerations and the steps to begin a cloud migration assessment. The most important recommendation from this session was the need to continually monitor and refine the migration process to achieve the highest return on investment.

3.5 HealthTrac Sponsored Session: Using Cloud in Healthcare

This collaboration session will help identify relevant standards for cloud computing as it applies for healthcare. It also discusses the perennial challenges of cloud as applied to healthcare, specifics of healthcare data as used in a cloud environment, and potential impacts of integrating cloud services on networks for healthcare providers.

The *HealthTrac Sponsored Session: Using Cloud in Healthcare* session had several goals:

- Identify relevant standards for cloud computing as it applies for healthcare
- Discuss the perennial challenges of cloud as applied to healthcare
- Discuss specifics of healthcare data as used in a cloud environment

- Discuss potential impacts of integrating cloud services on networks for healthcare providers

When considering a move to use cloud computing, healthcare organizations must understand the challenges with protecting health information while trusting the data in the cloud. Due to strict restrictions with data security by health regulations, healthcare organizations have to consider if it makes sense to migrate over to the cloud environment. A number of healthcare organizations have migrated some of their operations and data to the cloud.

3.5.1 Challenges

The collaboration session discussions identified the following challenges that might be solved and needs might be met by applying existing or developing new *HealthTrac Sponsored Session: Using Cloud in Healthcare*:

- What are the benefits and challenges in the healthcare domain when considering cloud deployment models (private, public, and hybrid)?
- How can the privacy and security concerns be mitigated to encourage greater use of the cloud for clinical applications?
- Is FedRAMP sufficient in assuring protection of patient information, and what more can be done?
- What are the impacts of potential performance issues, such as latency, on healthcare practitioners?

3.5.2 Discussion Summary

The interactive collaborative session proved to be successful with representatives from different government agencies and industry. This session focused on exploring healthcare specific challenges and uses of cloud computing. While the majority of the session identified permutations of the perennial challenges of adopting cloud in the government (i.e., culture, acquisition, standards, migration, etc.), several healthcare-specific outcomes were identified. For example, FedRAMP does not address PII and privacy which can impact healthcare records. Another aspect of healthcare cloud adoption is informed versus uninformed patient consent for records or healthcare data to be stored in a cloud, or even a third-party environment.

It started with the discussion of what benefits and challenges are in the healthcare domain when considering cloud deployment model. This was the first item on the agenda and it drew on for the majority of the session before addressing the other three challenges.

The following items were among the most actively discussed:

- The government's concerns were how to handle to the data and how can it be secure
- Performance was another consideration because healthcare organizations have to perform their work in remote areas with low bandwidth and internment service
- Data storage was another issue because depending on the size of samples or results, data storage can be in the petabytes
- Data standardization with making searchable data type was another concern; with healthcare organizations working with images along with textual form, how would they make data searchable

The second item discussed was how privacy and security concerns can be mitigated to encourage greater use of the cloud for clinical applications. Government agencies are concerned with who would own the data. Data access was another concern, since insurance agencies are now swapping this information between the banking industry, pharmaceutical, and clearing houses.

The third challenge was whether FedRAMP is sufficient in assuring protection of patient information, and what more can be done, if anything. The issue that was discussed is FedRAMP does not address privacy. However, numerous groups and privacy folks have developed a privacy overlay that covers this topic for FedRAMP. The topic of cloud adoption across federal enterprises with bringing big data analytics services and clinical standards to automate checking of performance outcomes is ready to be implemented in healthcare organizations. Government agencies are starting to have trust in other agencies security adopting cloud technologies before FedRAMP allows it to be used. Agencies want to avoid on wasting 6-8 months to wait for adoption, so they entrust other agencies who have already started using new technology. There was also importance on signing the risk acceptance letter and how many are not implementing risk mitigation strategies with cloud.

The last challenge was to determine the potential performance issues, such as latency, on a healthcare practitioner. This was brought up in the other challenge discussions. Government agencies with healthcare providers in remote areas will have very limited connection, low bandwidth, and high latency. Data size is also a concern due to precision medicine programs to clinical trials. Based on the analysis, the data could be small or large. Medical devices will also need to interface with the cloud to provide patient context, so that will be an issue that will have to be addressed.

3.5.3 Recommendations

The participants in the *HealthTrac Sponsored Session: Using Cloud in Healthcare* collaboration session identified the following important findings and recommendations:

- Cloud computing has been challenging relative to security issues, addressing identity management, promoting the business case of cost efficiency (software, hardware, acquisitions)
- Choosing which deployment model is based on necessary computing capacity needs; plan out in advance which deployment model is best suited for unanticipated-growth for Service Level Agreements (SLAs), dynamic provisioning, etc.; who owns the data can greatly affect deployment model
- Business case analysis is for use cases; define the requirements thoroughly, to address response times and geographical location needs
- Federal acquisition regulations make the cost model complicated; if there could be a streamlined process that would make the acquisition less complicated, cloud adoption could be more achievable
- Be aware of vendor lock-in problems, contracts are difficult with cost structure and requirements needed to support; plan for this in advance to avoid these issues
- Innovation and collaborating across public/private/industry on implementing products that work cross-boundaries
- Strategy for theater is to have a medical cloud that would support the medical records stored in the cloud to be accessible on various devices to be used by the medical team before receiving patients; this will help with giving teams background information on incoming patients to understand the demand management and provide the best healthcare possible
- When migrating to the cloud, standardizing the APIs will smooth the transition
- Laws are already in place to protect patient privacy, so that helps with privacy concerns in the cloud, however other countries outside the US will have various implementations regarding data and this needs to be addressed depending on datacenter location

- True reciprocity between agency need to be improved with inter-agency trust with one-another's Authority to Operate (ATO)
- Organizations do need to swap ATOs due to differences in environments, but should be done in a timely manner to reduce ROI before missing a technology cycle and being obsolete
- IT managers should put out a risk acceptance letter before going forward and understanding value
- Imaging data has storage and throughput considerations to be usable for the end user; tost data are in textural form, but images are difficult to search and summarize
- Development is challenging because there needs to be a new DevOps and cloud environments have to similar enough for the development environment and that has to be accounted for

4 Summit Recommendations

As with past Federal Cloud Summit discussions, the collaboration sessions discussions had a common set of themes. Adopting cloud continues to be a challenging and intimidating task for government agencies. However, cloud adoption throughout the government is becoming more widely accepted, leading to more fine-grained challenges and user-driven policies. As with other technologies, DevOps is increasing in awareness and importance when adopting cloud technologies. Specifically, the perennial challenges of acquisition are extending into defining DevOps. However, DevOps provides an opportunity to establish quantitative metrics (outside of cost of migration) that can be used to evaluate successes in the cloud. Security remains a primary challenge with cloud migration, but other solutions (e.g., advances in the TICs, securing the endpoints) are emerging to mitigate this challenge.

Another trend that mirrors those of the Mobile [8], Big Data [7], and other emerging technology domains is that industry leads the way with cloud, but the primary users are no longer government customers. This leads to a focus on non-government needs and can lead to gaps – often in the security domain – for government adoption.

Cost-driven migration remains a primary justification for beginning a cloud migration. However, cloud adopters are increasingly acknowledging the importance of both quantitative and qualitative metrics, and are adopting quantitative metrics outside of cost as primary drivers. Patterns are also emerging to help reduce costs where appropriate, such as *lift-and-shift* as a method for initially migrating. Further, migration roadmaps are beginning to emerge to help cloud adopters transition to the cloud in a cost effective and impactful way.

Healthcare is a recent domain in which cloud computing concepts are being utilized. Because cloud computing in the healthcare domain is relatively new, practitioners are beginning to grapple with the perennial cloud challenges such as cost, acquisition, and privacy. However, PII and other challenges introduce new wrinkles to the perennial challenges.

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; academics can be particularly effective at closing some of the gaps between government and industry (e.g., by researching and providing techniques for improving security). 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 formed to allow cross-government collaboration and discussion to ensure best practices are shared. Some working groups (e.g., the ATARC innovation Labs [11]) are being implemented across the government to discuss more niche concerns. 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.

5 CONCLUSIONS

The July 2016 Federal Cloud Computing Summit highlighted several challenges facing the Federal Government's adoption of cloud computing.

- Government cloud adopters should avoid silos wherever possible, whether in budgeting, DevOps, or sharing lessons learned

- SLAs should move beyond uptime and other usage metrics to include the quality and availability of the operations staff and other aspects of DevOps

- To improve government-industry relations, policy makers should define specific desired outcomes from vendors rather than dictating procedure
- Cloud owners should adopt risk management rather than risk avoidance
- Cloud adopters have a responsibility to take ownership of security by incorporating it into their end user devices as well as the applications used in the clouds to help close some of the capability gaps in security

While the July 2016 Federal Cloud Computing Summit highlighted areas of continued challenges and barriers to adoption, the Summit also cited notable advances in mitigating these perennial challenges. While security, service level agreements, and migration remain primary challenges, recommendations and roadmaps for mitigating these challenges are emerging.

Based on the recommendations made in the Collaboration Sessions, 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. Including academics in the research process can help provide solutions to challenges that are not currently financially appealing to commercial vendors. These activities will further mitigate the perennial cloud adoption challenges cited by the participating cloud practitioners.

ACKNOWLEDGMENTS

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit.

The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site[2].

[2] http://www.fedsummits.com/cloud/

References

[1] R. Cagle, T. Rice, and M. Kristan. DevOps for Federal Acquisition . In *IEEE Software Technology Conference*, 2015.

[2] K. Caraway, D. Faatz, N. Ross, J. F. Brunelle, and T. Suder. July 2014 federal cloud computing summit summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2014.

[3] K. Caraway, N. Gong, M. Kristan, N. Ross, J. F. Brunelle, and T. Suder. January 2015 federal cloud computing summit summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2015.

[4] K. Caraway, N. Gong, J. Packer, J. Vann, J. F. Brunelle, T. Harvey, and T. Suder. July 2015 atarc federal cloud computing summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2015.

[5] Gartner. Gartner identifies five ways to migrate applications to the cloud. http://www.gartner.com/newsroom/id/1684114, 2011.

[6] GSA. 18f. https://18f.gsa.gov, 2016.

[7] C. Harvey, L. Moretto, B. Natale, H. Vafaie, I. Vayndiner, N. Hamisevicz, T. Harvey, and T. Suder. December 2015 federal big data summit report. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[8] T. Harvey, T. Suder, M. Peck, G. Seth, M. Russell, P. Benito, and M. Collins. August 2015 federal mobile computing summit collaboration session summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[9] L. Leong. Best practices for planning a cloud infrastructure-as-a-service strategy, 2015.

[10] P. Mell and T. Grance. Information technology – cloud computing – service level agreement (sla) framework. Technical Report ISO/IEC 19086, National Institute of Standards and Technology, 2016.

[11] G. Mundell, K. Jones, and V. Subbiah. Atarc cloud innovation lab. http://www.atarc.org/innovation-labs/cloud/, 2016.

[12] The MITRE Corporation. FFRDCs – A Primer. http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf, 2015.