IJIS Institute

CLOUD COMPUTING:
A Business Case

IJIS Institute

Emerging Technologies

Advisory Committee

April 2016

Principal Contributors
Iveta Topalova, Microsoft, ETAC Vice-chair*
Anil Sharma, IBM

ACKNOWLEDGEMENTS

The IJIS Institute would like to thank the following contributors and their sponsoring companies for supporting the creation of this document:

Principal Contributors

- Iveta Topalova, Microsoft – Committee Vice-Chair, IJIS Institute Emerging Technologies Advisory Committee
  * *The information in this paper reflects Iveta's personal thoughts and ideas and does not necessarily represent the position of Microsoft.*
- Anil Sharma, IBM - IJIS Institute Emerging Technologies Advisory Committee

Committee Members

The IJIS Institute Emerging Technologies Advisory Committee is comprised of the following members:

- *Chair:* Matthew D'Alessandro, Microsoft Corporation
- *Vice Chair:* Iveta Topalova, Microsoft Corporation
- Mike Reade, IBM
- Crystal McDuffie, Association of Public Safety Communications Officials
- Michael Alexandrou, Georgia AOC
- Leland Algatt, Intergraph
- Mike Cormaci, Watch Systems
- Josh Davda, Optimum Technology
- Ted deSaussure, Information Builders, Inc.
- Sean Gunderson, Law Enforcement Intelligence Group
- Susan Smith Hammen, Bair Analytics
- Jim Harris, National Center for State Courts
- Larry Helms, Cody Systems
- Bill Lake, Datamaxx
- Lt Glen Mills, Burlington MA Police Department
- Anil Sharma, IBM
- Josh Smith, Spillman
- Mike Spirito, Cody Systems
- Teresa Wu, 3M Identity Management/Cogent
- Deputy Chief Lawrence Zacarese, Stony Brook University

CONTENTS

Table of Figures

INTRODUCTION

The Obama administration has made cloud computing a high priority, calling it a, "fundamental re-examination of investments in the technology infrastructure." Vivek Kundra, the past U.S. Chief Information Officer, identified cloud computing as, "the next generation of IT," in government and initiated the *Cloud First* policy encouraging government departments to shift to cloud computing where possible. Kundra stressed that standards for security, interoperability, and data portability are critical to drive forward the massive transition to cloud computing underway across government. His successor, Steven VanRoekel, committed to take this work even further through a plan he called *Future First.* VanRoekel noted that, "much as our *Cloud First* policy changed the landscape of IT spending, *Future First* is beginning to jump start the government's adoption of new technologies and approaches." Even with a clear and maturing national priority, the government and, in particular, justice and public safety agencies, sometimes struggle with understanding the business drivers and benefits for adoption of the Cloud.

From a more pragmatic perspective, most state and local agencies are grappling with IT and operational budget cuts and have to figure out ways to make more with less. Lower budgets mean reductions in workforce, as well as reduced spending on hardware and software. However IT departments such as those in justice and public safety still have to support existing IT infrastructure, ongoing initiatives, and develop new and improved secure services for their citizens and staff. The Cloud can provide answers to these types of challenges.

Organizations are adopting Cloud computing based on real business drivers:

- Many agencies are involved in building new citizen-centric applications. These apps require IT departments to develop solutions that offer enough processing power and storage to host the new application capabilities. The Cloud offers a highly-flexible, lower-cost, option and a more rapid path to achieve goals such as those of our court and judiciary systems.

- Some municipalities are looking for solutions that would provide the ability to scale up and down as required by significant changes in service needs such as the significant changes in population during the certain periods of the year. Since they do not have the budget to procure additional hardware to support the needed processing power and IT resources to support the installation and maintenance, they deploy their applications in the Cloud to leverage its elasticity for this scenario. Moving their applications to the Cloud could also result in reduced total cost of ownership due to savings on new servers, licenses, and manpower while giving them the needed infrastructure, based on a pay-for-what-you-use model.

- Another challenge involves agency IT departments struggling with time consuming application development processes. Multiple environments running on separate servers for the building, testing, debugging, and quality-assurance (QA) processes with different team members responsible for each environment. By moving the application development into the Cloud, they can change the way their software is developed. The developer can create the environment, build the application, deploy, and scale the

application programmatically, thus making the application development process much more efficient and allowing for faster time-to-beneficial use.

- Finally, a continuing and increasing trend is for municipalities, both small and large, to migrate a significant portion of their workforce to the Cloud. This means that instead of hosting various back office applications on their servers – such as email, word processing, spreadsheets, and other applications – they achieve significant savings on infrastructure, and, at the same time, provide the ability for their users to access information from anywhere. In addition, this approach helps facilitate enhanced collaboration capabilities.

WHAT IS CLOUD COMPUTING?

Cloud computing emerged not long ago as an industry buzzword and has quickly matured into a valuable tool with an ever-growing footprint that can help quickly transform justice and public safety agencies. In the IT world, is has become a more general term (and certainly a marketing hot button) for anything that involves delivering hosted services over the Internet. The challenge is that, like the nature of clouds themselves, the shape and meaning of cloud computing seems nebulous, and everyone has a different definition: virtualization, grid computing, utility computing, distributed computing…

…are these terms all the same? Are they similar? Are they Interchangeable?

UNDERSTANDING THE CLOUD

To simplify the terminology variety and hype, the name Cloud computing was inspired by the cloud symbol that is often used to represent networks, or the Internet, in flowcharts and diagrams. Some IT professionals and Cloud providers define Cloud computing very specifically as an updated version of utility computing: basically virtual servers available over the Internet. The concept of the co-location of physical IT assets in remote data centers (especially for storage, back-up, failover, and disaster recovery) is not new. Still, others are pushing the boundaries much further, suggesting that anything you consume outside your own firewall is *in the Cloud*.

Cloud computing can be examined in a more practical context. Perhaps, when you consider the business issues that IT shops struggle with routinely: then Cloud is a way to quickly (sometimes in an unexpected way and with urgent need) increase capacity, or add capabilities, without budgeting for new infrastructure, hiring new IT staff, re-training current IT staff, or purchasing and licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real-time over the Internet, extends an organization's existing capabilities.

The following is an overview of the facets of Cloud computing:

Cloud Service Models

The most popular Cloud services can be broadly divided into three categories, or service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service

(SaaS). There are other variations such as Networking-as-a-Service (NaaS), Communications-as-a-Service (CaaS), Monitoring-as-a-Service (MaaS), as well as a concept known as 'x' or anything as a service (XaaS) that initially became a catch-all for the wide varieties of models emerging to provide services and capabilities. Today the 'x' model is becoming ever more granular with process, testing, and integration just a few of the ever growing varieties available as needs are defined.

Infrastructure-as-a-Service (IaaS) provides virtual server instances with unique IP addresses and blocks of data storage, on-demand. Consumers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and data storage. In the enterprise, cloud computing allows an organization to pay for only as much capacity as is needed, and bring more online quickly, as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are bought and consumed, it's sometimes referred to as utility computing.

Platform-as-a-service (PaaS) in the Cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals, or gateway software installed on the customer's computer.

The **Software-as-a-service (SaaS)** Cloud model is perhaps the best known, where the service provider supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal or web application. In other words, these are applications that are hosted in the Cloud. Services can be anything from web-based email to law enforcement records management, court case management, and database processing. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere. From the agencies perspective, it means no upfront investment in servers or software licensing; on the provider side, with just one app to maintain, costs are low compared to conventional hosting.

Cloud Characteristics

A cloud service has three distinct characteristics that distinguish it from traditional hosting models.

1) It is sold on demand, typically by the minute or the hour;
2) It is elastic – meaning that a consumer can have as much, or as little, of a service as they want at any given time; and
3) The service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access).

Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have therefore greatly accelerated the interest in and adoption of Cloud computing solutions and alternatives.

Cloud Offerings

Another important consideration among cloud services is in the nature of the Cloud itself. A Cloud can be private or public. A public Cloud sells services to anyone on the Internet. A private Cloud is a proprietary network or a data center that supplies hosted services to a specific and limited number of people or organizations. When a service provider uses public Cloud resources to create their private Cloud, the result is called a virtual private Cloud, or a hybrid Cloud. In government, especially in combined state and local government services, a growing concept is that of the community Cloud. Here the Cloud infrastructure is jointly owned or subsidized by many organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, privacy policies, and compliance considerations). In some instances, this might be a joint-powers managed private facility, or a nonprofit formed thru agreements made between multiple agencies to save money by way of the economies of scale (e.g., 22 agencies share the cost of hosting a single RMS application, rather than individually standing up 22 separate deployments of varying software offerings). Nlets (the International Justice and Public Safety Network) is an example of a community Cloud within the national law enforcement community. A good resource examining the specific unique requirements of the courts in the Cloud can be found in IJIS Courts Committee's InfoBrief – *Cloud Computing for the Courts.*

Whether private or public, or a hybrid combination, the goal of Cloud computing is to provide easy, scalable access to computing resources and IT services. Typically this can be achieved at costs lower than full ownership and management, while removing the barrier-to-entry issues for many by lowering or eliminating the upfront project costs.

Figure 1, reproduced from a Cloud Standards Customer Council (CSCC) white paper, shows typical variables to be considered when choosing Cloud deployment models. The term *Dedicated* in the figure refers to a hybrid cloud using dedicated resources which provide a standardized configuration for IaaS and enables an even faster deployment timeline.

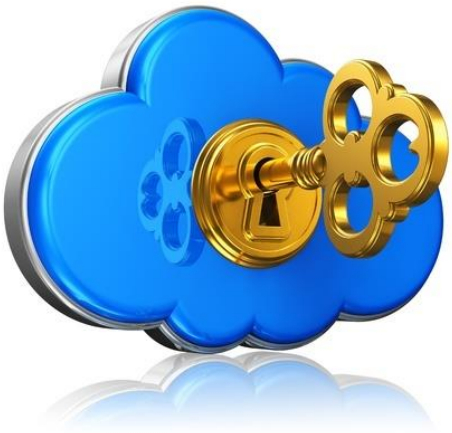
		Primary Criteria					
		Elasticity	**CPU and Computation**	**Data Volume**	**Data Bandwidth**	**Data Proximity**	**Governance and Jurisdiction**
Secondary Criteria	**Workload Responsiveness**	Public	Public and Hybrid	Public and hybrid	Public and Hybrid	Hybrid and Dedicated	Private and Hybrid
	CPU and Computation	Public and Dedicated	Hybrid	Hybrid	Public and Hybrid	Hybrid and Dedicated	Private and Hybrid
	Data Volume	Public and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid	Hybrid and Dedicated	Private and Dedicated
	Data Bandwidth	Public and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Private and Dedicated
	Data Proximity	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid and Dedicated	Hybrid and Private	Private and Dedicated
	Governance and Jurisdiction	Private and Hybrid	Private and Hybrid	Private and Dedicated	Private and Dedicated	Private and Dedicated	Private & Dedicated

FIGURE 1: CSCC OPTIMIZED PROVISIONING WORKSHEET

Security in the Cloud

Security has been the single most important challenge of the Cloud model especially in the justice and public safety area. It is critical when evaluating transition to a Cloud model to consider both the security challenges and the security advantages. Tim Grance, program manager of cyber and network security at the National Institute of Standards and Technology (NIST), said "Just because a cloud is public it doesn't mean that your data is public." Similarly, a private cloud is only as secure as the technology, protocols and staff that manage it.

Some of the key security risks of Cloud computing are moving personally identifiable and sensitive data to the Cloud, trusting the outsourced security model, data ownership issues, indirect administrator accountability, concern about proprietary implementations which cannot be examined, concerns that large Clouds are an attraction to hackers, risks based on the possibility of massive outages, and concerns about loss of physical control. These disadvantages are offset by some key advantages of Cloud security such as greater investment in security infrastructure, the fact that Cloud homogeneity makes security auditing and testing simpler, the automated security management enabled by many Cloud implementations, the simplification of compliance analysis, the fact that data is held by an unbiased party, the fact that Cloud providers have dedicated security teams and the native redundancy and disaster recovery capabilities available in a Cloud environment. Each of these advantages and disadvantages needs to be considered, prioritized and included in a transition plan and will in many cases be agency or organization specific.



As a result, selecting a migration path is a key strategy for reducing the security risk of Cloud computing. While public Clouds offer higher opportunity for savings, at the same time they usually present the highest security risk. On the opposite side of the spectrum are private Clouds offering reduced cost-efficiencies but may provide better control over security. Many officials believe that a community Cloud model, which supports a select group of organizations and meets the requirements of this community, may be uniquely suited to the government setting and in particular to justice and public safety organizations, where many agencies have common objectives and concerns, such as mission goals and security requirements. That approach is fully supported by a number of Cloud providers which have developed community Cloud and more specifically government Cloud offerings. Independently of the selected Cloud platform, one of the key security mitigation approaches is the existence of strict and enforceable Service Level Agreements (SLA) with the Cloud provider which meet the specific security concerns for each deployment. Additionally, while government Cloud offerings do support a number of targeted security controls such as those defined by the Federal Information Security Management Act (FISMA), there has been a significant gap in the area of justice and public safety domain-specific security requirements and controls critical for successful implementation of Cloud computing. Although these requirements and controls will be different for the different domains or lines of business such as courts, law enforcement, corrections, etc. a common robust security standard

trend is gaining traction. The Criminal Justice Information Systems (CJIS) Security Policy, while directly applicable and required of many public safety agencies, is being seen more and more as simply a sound, comprehensive policy with an industry standard foundation that can be used for many types of data across multiple lines of business. This *blanket* security policy model is increasingly being adopted by agencies across the public safety spectrum with minor modifications based on specific agency policy rules.

When support for the CJIS Security Policy is required or preferred, there are a few key questions which should be considered as part of Cloud Services Provider evaluation:

- Does the cloud provider support national standards for protecting criminal justice information?
- Does the Cloud Service Provider have a national program working with state Chief Security Officers (CSO) to demonstrate security in accordance with national standards?
- Does the Cloud Service Provider have a fully isolated network and hardware instance of their Cloud?
- Have the employees working in the data center passed the FBI background check?
- Is the Cloud Service Provider willing to submit to audit to demonstrate that they are providing full compliance with national CJIS Standards?

The trend of accepting the CJIS Security Policy as a best practice may continue across multiple lines of business with accompanying minor changes to meet either line of business or agency specific requirements. These changes have been fostered by a partnership between justice and public safety organizations as well as industry via organizations like IJIS to help define these requirements and the respective controls and to pilot implementations to prove the approach.

Another critically important mitigation approach for the security risks associated with Cloud computing is the recognition of the fact that every application leveraged by a justice and public safety agency has different security requirements. For example the security requirements for email applications are typically significantly less critical compared to the requirements for case or record management systems. It is important for agencies to create a comprehensive inventory of requirements for the different applications they plan to migrate to the cloud and take a stepwise or incremental approach migrating the applications which carry the least risk first.

Portability in the Cloud

Portability is another key requirement for successful adoption of cloud computing in government organizations. Cloud providers are actively working on solving the portability challenge. For example the Open Virtualization Format (OVF) is an industry standard format for portable virtual machines. It allows virtual machines packaged in this format to be installed on any virtualization platform that supports the standard. The

companies behind the collaboration on this specification include Dell, HP, IBM, Microsoft, VMware, and XenSource. With time, the requirement for portability brought forward by cloud computing will lead to portability never considered or available in the past.

Interoperability in the Cloud

Interoperability is another important and dynamic consideration. Today, cloud providers are leveraging existing industry standards at the same time as standards bodies are actively working on defining new interoperability standards specifically designed for cloud computing. The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) has been on the forefront of this development. It is also important to note that standards and specifications developed specifically for justice and public safety – such as the National Information Exchange Model (NIEM), the Global Reference Architecture (GRA) and the Global Federated Identity and Privilege Management (GFIPM) specification, all of which IJIS has been a key player in – are enablers of Cloud computing interoperability. Additionally, these specifications could be elaborated in order to meet the specific requirements of Cloud computing which could result in further adoption of these standards and specifications.

CONCLUSION

Cloud computing continues to gain traction with increasing adoption rates in justice and public safety. It offers a significant opportunity for justice and public safety organizations to realize cost efficiencies while at the same time improving quality of service. While there are still risks associated with the adoption of Cloud computing, a partnership between justice and public safety organizations and industry providers to define the specific requirements, controls and the respective service level agreement clauses can accelerate the adoption and result in significant benefits to the community.

Possibly most significantly, it is important to realize that the Cloud is not a one-size-fits-all solution and its applicability, benefits, and challenges are highly dependent on existing and future strategic planning. However with thoughtful consideration, the Cloud can be a key component helping organizations to achieve their goals more quickly and provide the potential to continually increase capabilities and lower costs over time enabling agencies to better serve their agencies and constituents.

FOR FURTHER INFORMATION

Tech Target – Public sector CIO's cloud adoption trend:
http://searchcio.techtarget.com/news/1507544/Public-sector-CIOs-answer-Vivek-Kundras-cloud-computing-call-to-arms?asrc=EM_USC_11258627&track=NL-981&ad=758599

Cloud Standards Customer Council 2015, Customer Cloud Architecture for Big Data and Analytics, Version 1.1:
http://www.cloud-council.org/deliverables/CSCC-Customer-Cloud-Architecture-for-Big-Data-and-Analytics.pdf

Information Week article on Federal Cloud Initiative:

http://www.informationweek.com/news/government/cloud-saas/231901731

The National Institute of Standards Cloud Computing Program:
http://www.nist.gov/itl/cloud/

Distributed Management Task Force – Open virtualization format:
http://www.dmtf.org/standards/ovf

IJIS Courts Committee InfoBrief – *Cloud Computing for the Courts*:
http://c.ymcdn.com/sites/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/ijis_info_brief_cloud_computing_courts_20150402.pdf

ABOUT THE IJIS INSTITUTE

The IJIS Institute unites the private and public sectors to improve mission-critical information sharing and safeguarding for those who protect and serve our communities. The IJIS Institute provides training, technical assistance, national scope issue management, and program management services to help government fully realize the power of information sharing.

Founded in 2001 as a 501(c)(3) nonprofit corporation with national headquarters on The George Washington University Virginia Science and Technology Campus in Ashburn, Virginia, the IJIS Institute has grown to nearly 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the Emerging Technology Advisory Committee for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in the commitment to improving justice, public safety, and homeland security information sharing.

For more information on the IJIS Institute:

- Visit the website at: http://www.ijis.org/,
- Follow the IJIS Institute on Twitter: @ijisinstitute,
- Read the IJIS Factor Blog, and
- Join us on LinkedIn at: Justice and Public Safety Information Sharing.

About the IJIS Institute Emerging Technologies Advisory Committee

The IJIS Institute's Emerging Technologies Advisory Committee addresses new and emerging technologies in the justice and public safety domains. The Emerging Technologies Advisory Committee develops advisory materials and conducts briefings for industry and government on these key emerging technologies in support of national programs with a goal of increasing adoption. The Committee is corporation agnostic and strives to provide an industry view of these emerging technologies to assist the practitioner community in making more informed decisions.