2013 13th International Conference on Computational Science and Its Applications

Data Management Challenges in Cloud Computing

Hai V. Tran, Ph.D.
Center for Science, Technology, and Engineering
The U.S. Government Accountability Office
Washington, DC 20548, USA
tranh@gao.gov

***Abstract* — Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Web-based technologies, has the potential to provide information technology services more quickly and at a lower cost but also introduces new challenges to the management of data. This is especially important to the oversight responsibilities of government organizations where public data are concerned. The U.S. Government Accountability Office (GAO) periodically performs audits of U.S. federal agencies' information technology (IT) acquisitions and practices. This paper presents some survey results on efforts of federal agencies to address data management issues while transitioning to cloud computing environments.**

Keywords:* *Cloud computing, data management,, accountability, auditing, information security, critical infrastructure protection, IT services, policy analysis framework, strategic planning.

I. Introduction

Cloud computing delivers IT services by taking advantage of several broad evolutionary trends in IT, including the use of virtualization. According to the U.S. National Institute of Standards and Technology (NIST), cloud computing is a means "for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST also states that an application should possess five essential characteristics to be considered cloud computing: on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service. In other words, cloud computing can be referred to as outsourcing IT services to an external provider(s).

Cloud computing offers three service models: infrastructure as a service, where a vendor offers various infrastructure components; platform as a service, where a vendor offers a ready-to-use platform on which customers can build applications; and software as a service, which provides a self-contained operating environment used to deliver a complete application such as Web-based e-mail. Figure 1 illustrates the potential service models.

Cloud computing actually is the evolution of information technologies. Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. The speed and accessibility that create benefits of the computer age, if not properly controlled, could allow for unauthorized individuals and organizations to inexpensively eavesdrop or interfere with these operations from remote locations, for mischievous or malicious purposes including fraud or sabotage.

In the United States, use of cloud computing can also create numerous information security risks for federal agencies. The U.S. GAO, as an investigative arm of the U.S. Congress, periodically audits federal agencies with respect to their information system operational and practices. As a result, we carried out a survey of the 24 departments and agencies on their concerns in adopting cloud computing as their IT environment. Twenty two of 24 major federal agencies reported that they are either concerned or very concerned about potential information security risks associated with cloud computing. Several of these risks relate to being dependent on a vendor's security assurances and practices. Specifically, several agencies stated concerns about the possibility that ineffective or noncompliant service provider security controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information; the potential loss of governance and physical control over agency data and information when an agency cedes control to the provider for the performance of certain security controls and practices; and potentially inadequate background security investigations for service provider employees could lead to an increased risk of wrongful activities by malicious insiders.

978-0-7695-5045-9 2013

DOI 10.1109/ICCSA.2013.14

Of particular concern was dependency on a vendor. All assessed agencies specifically noted concern about the possibility of loss of data if a cloud computing provider stopped offering its services to the agency. For example, the provider and the customer may not have agreed on terms to transfer or duplicate the data.

Multi-tenancy, or the sharing of computing resources by different organizations, can also increase risk [5]. Twenty-three of 24 major agencies identified multi-tenancy as a potential information security risk because, under this type of arrangement, one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information. Agencies also stated concerns related to exchanging authentication information on users and responding to security incidents. Identity management and user authentication are a concern for some government officials because customers and a provider may need to establish a means to securely exchange and rely on authentication and authorization information [6] for system users. In addition, responding to security incidents may be more difficult in a shared environment because there could be confusion over who performs the specific tasks—the customer or the provider.

Although there are potential information security risks related to cloud computing, these risks may vary based on the particular deployment model. For example, NIST stated that private clouds may have a lower threat exposure than community clouds, which may have a lower threat exposure than public clouds. Several industry representatives stated that an agency would need to examine the specific security controls of the provider the agency was evaluating when considering the use of cloud computing.

Currently, federal agencies have begun to address information security for cloud computing; however, they had not developed corresponding guidance. About half of the 24 major agencies reported using some form of public or private cloud computing for obtaining infrastructure, platform, or software services. These agencies identified measures they were taking or planned to take when using cloud computing. These actions, however, had not always been accompanied by development of related policies or procedures.

Most agencies had concerns about ensuring vendor compliance and implementation of government information security requirements. In addition, agencies expressed concerns about limitations on their ability to conduct independent audits and assessments of security controls of cloud computing service providers. Several industry representatives were in agreement that compliance and oversight issues were a concern and raised the idea of having a single government entity or other independent entity conduct security oversight and audits of cloud computing service providers on behalf of federal agencies. Agencies also stated that having a cloud service provider that had been pre-certified as being in compliance with government information security requirements through some type of government-wide approval process would make it easier for them to consider adopting cloud computing. Other agency concerns related to the division of information security responsibilities between customer and provider. As a result, we reported that the adoption of cloud computing by federal agencies may be limited until these concerns were addressed.

In addition to the Government Services Administration (GSA)'s efforts, the Chief Information Officers (CIO) Council had established a cloud computing Executive Steering Committee to promote the use of cloud computing in the federal government, with technical and administrative support provided by GSA's Cloud Computing Program Management Office, but had not finalized key processes or guidance. A subgroup of this committee had developed the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program to provide joint authorizations and continuous security monitoring services for all federal agencies, with an initial focus on cloud computing. The subgroup had worked with its members to define interagency security requirements for cloud systems and services and related information security controls. However, a deadline for completing development and implementation of a shared assessment and authorization process had not been established.

In the GAO Oct. 2011 report, we made recommendations to the Office of Management and Budget (OMB), GSA, and NIST to assist federal agencies in identifying uses for cloud computing and information security measures to use in implementing cloud computing and their responses. These agencies generally had agreed with our recommendations and took actions. Specifically, we recommended that the Director of OMB establish milestones for completing a strategy for implementing the federal cloud computing initiative; ensure the strategy addressed the information security challenges associated with cloud computing, such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, division of information security responsibilities between customer and provider, the shared assessment and authorization process, and the possibility for precertification of cloud computing service providers; and direct the CIO Council Cloud Computing Executive Steering Committee to develop a plan, including milestones, for completing a government-wide security assessment and authorization process for cloud services.

In February 2011, OMB responded by issuing the *Federal Cloud Computing Strategy*, which references the establishment of a shared assessment and authorization process for cloud computing. In addition, the strategy discusses other steps to promote cloud computing in the federal government, including ensuring security when using cloud computing, streamlining procurement processes, establishing standards, recognizing the international dimensions of cloud computing, and establishing a governance structure [1]. However, the strategy does not address other security challenges such as needed agency-specific guidance, the appropriate use of attestation standards for control assessments of cloud computing service providers, and the division of information security-related responsibilities between customer and provider. Until these challenges are addressed, agencies may have difficulty readily adopting cloud computing technologies.

We also recommended that the Administrator of GSA, as part of the procurement for infrastructure as a service cloud computing technologies, ensure that full consideration be given to the information security challenges [1, 2] of cloud computing, including a need for a shared assessment and authorization process.

In response, GSA issued a request for quote relating to its procurement for cloud services that included the need to use FedRAMP once it is operational. FedRAMP was further developed by GSA, in collaboration with the Cloud Computing Executive Committee, as a shared assessment and authorization process to provide security authorizations and continuous monitoring for systems shared among federal agencies. The CIO Council, in collaboration with GSA, issued a draft version of the shared assessment and authorization process in November 2010;8 however, the process has not yet been finalized. GSA officials stated that they intend to release additional information on FedRAMP once OMB issues a policy memorandum related to cloud computing, expected in the first quarter of fiscal year 2012.

Lastly, to assist federal agencies in implementing appropriate information security controls when using cloud computing, we recommended that the Secretary of Commerce direct the Administrator of NIST to issue cloud computing information security guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53, such as virtualization, data center operations, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers.

NIST has also taken steps to address our recommendations. In January 2011, it issued SP 800-125, *Guide to Security for Full Virtualization Technologies*. Virtualization is a key technological component of cloud computing. SP 800-125 discusses the security characteristics of virtualization technologies, provides security recommendations for virtualization components, and highlights security considerations throughout the system life cycle of virtualization solutions. In July 2011, NIST issued SP 500-291, *NIST Cloud Computing Standards Roadmap* and in September 2011, SP 500-292, *NIST Cloud Computing Reference Architecture*. Collectively these documents provide guidance to help agencies understand cloud computing standards and categories of cloud services that can be used government-wide. Among other things, these publications address cloud computing standards for interoperability and portability.

NIST also issued a draft publication on cloud computing, SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, which addresses the security concerns associated with data center operations and the division of responsibilities among providers and customers. In addition, the guide discusses the benefits and drawbacks of public cloud computing, precautions that can be taken to mitigate risks, and provides guidance on addressing security and privacy issues when outsourcing support for data and applications to a cloud provider. According to NIST officials, SP 800-144 will be finalized in the first quarter of fiscal year 2012. All of these publications are available on the NIST web site.

In summary, the adoption of cloud computing has the potential to provide benefits to federal agencies; however, it can also create numerous information security risks. Since our report, federal agencies have taken several steps to address our recommendations on cloud computing security, but more remains to be done. For example, OMB has issued a cloud computing strategy; however the strategy does not fully address key information security challenges for agencies to adopt cloud computing. The CIO Council and GSA have also developed a shared assessment and authorization process, but this process has not yet been finalized. In addition, NIST has issued several publications addressing cloud computing security guidance. Although much has been done since our report, continued efforts will be needed to ensure that cloud computing is implemented securely in the federal government.

We should also note that federal agencies are also responsible for protecting critical infrastructure of the nation while attempting to perform their duties more effectively and efficiently by restructuring their business to take advantage of the benefits of cloud computing. However, they are ultimately responsible for their success/failure of their service to the nation and the American people. As a mechanism to hold these agencies responsible, periodic auditing of the agencies operations are demanded by the U.S. Congress and the GAO conducts its audits chiefly from the requests from congressional committees. This oversight requirement demands the federal agencies to also address the issue of data ownership and custodianship, in additional to the inherent requirement of confidentiality, integrity and availability of agencies information and data.

Before addressing the specific data requirements relating to accountability and auditing, it is worthwhile to review the critical infrastructure sectors in which data must be protected.

TABLE I. CRITICAL INFRASTRUCTURE SECTORS

Agriculture	Includes supply chains for feed and crop production.
Banking and finance	Consists of commercial banks, insurance companies, mutual funds, government sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.
Chemical and hazardous materials	Produces more than 70,000 products essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Emergency services	Includes fire, rescue, emergency medical services, and law enforcement organizations.
Energy	Includes electric power and the refining, storage, and distribution of oil and natural gas.
Food	Covers the infrastructures involved in post-harvest handling of the food supply, including processing and retail sales.
Government	Ensures national security and freedom and administers key public functions.
Information tech. & telecommunications	Provides information processing systems, processes, and communications systems to meet the needs of businesses and government.
Postal and shipping	Includes the U.S. Postal Service and other carriers that deliver private and commercial letters, packages, and bulk assets.
Public health and healthcare	Consists of health departments, clinics, and hospitals.
Transportation	Includes aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit that are vital to our economy, mobility, and security.
Drinking water and water treatment systems	Includes about 170,000 public water systems that rely on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.

II. ASSESSMENT OBSERVATIONS

Federal agencies have been using IT services to conduct their work and certain practices have become institutionalized. With the adoption of new model of cloud computing, federal agencies must adapt their processes to improve their performance in a cost-effective and timely way!

A. *Information technology dependence and vulnerabilities*

All critical infrastructure owners rely on computers in a networked environment. Although all infrastructure sectors make use of similar computer and networking technologies, specific requirements in each sector depend on many factors, such as the sector's risk assessments, priorities, applicable government regulations, market forces, culture, and the state of its IT infrastructure. These factors, in combination with financial and other factors like costs and benefits, can affect an infrastructure entity's use of IT as well as its deployment of technologies.

B. *Technologies*

There are a number of technologies that can be used to better protect critical infrastructures from cyber attacks, including access control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies. In each of these categories, many technologies are currently available, while other technologies are still being researched and developed.

Since cloud computing are based on networked assets, these assets are facing all the cyber threats mentioned so far. And because there may be a concentrating of data from many customers on one cloud provider's networks, hackers are more likely drawn to these rich domains! Table 2 summarizes some of the common cyber- security technologies, categorized by the type of security control they help to implement.

TABLE II. COMMON TECHNOLOGIES

Category	Technology	Function
Access control: Boundary protection	Firewalls	Control access to/from networks or computers
	Content management	Monitors Web and messaging applications for inappropriate content, including spam, banned file types, and proprietary information.
Authentication	Biometrics	Uses human characteristics, such as fingerprints, irises, and voices to establish the identity of the user.
	Smart tokens	Establish identity of users through an integrated circuit chip in a portable device such as a smart card or time synchronized token.
Authorization	User rights and privileges	Allow or prevent access to data and systems and actions of users based on policies of an organization.

Critical infrastructure sectors use all of these types of cyber-security technologies to protect their systems. However, the level of use of technologies varies across sectors and across entities within sectors.

C. Cyber-security technology research

Despite the availability of current cyber-security technologies, there is a demonstrated need for new technologies to combat and prevent the compromising of data in a cloud computing environment. Long-term efforts are needed, such as the development of standards, research into cyber-security vulnerabilities and technological solutions for these problems, and the transition of research results into commercially available products. While several standards exist for cyber-security technology in the areas of protocol security, product-level security, and operational guidelines, there is still a need to develop standards that could help guide the use of cyber-security technologies and processes.

There are several research areas being pursued by the federal government, academia, and the private sector to develop new or better cyber-security technologies [4-6]. We have identified some of the important cyber-security research needs shown in Table 3.

TABLE III. RESEARCH in CYBER-SECURITY

Research area	Description
Composing secure systems from insecure components	Building complex heterogeneous systems that maintain security while recovering from failures.
Security for network embedded systems	Detect, understand, and respond to anomalies in large, distributed control networks that are prevalent in electricity, oil and natural gas, and water sectors.
Security metrics and evaluation	Metrics that express the costs, benefits, and impacts of security controls from multiple perspectives: economic, organizational, technical, and risk.
Socioeconomic impact of security	Legal, policy, and economic implications of cyber-security technologies and their possible uses, structure and dynamics of the cyber-security marketplace, role of standards and best practices, implications of policies intended to direct responses to cyber attacks.
Vulnerability identification and	Techniques and tools to analyze code, devices, and systems in dynamic and large-scale environments analysis.
Wireless security	Device- and protocol-level wireless security, monitoring wireless networks, and responding to distributed denial-of-service attacks in wireless networks.

This is currently an active area of research in academia, private industry and government, with a great deal of collaboration and cooperation since the government is also the customer of the private industry in many sectors.

In addition to the need for research that addresses existing threats, there is a need for long-term research that anticipates the dramatic growth in the use of computing and networks in the coming years. Some of the possible long-term research areas include tools for ensuring privacy, embedding fault-tolerance in systems, self managing and self-healing systems, and re-architecting the Internet. Prior information technology developments have shown that more than 10 years are often required to develop basic research concepts into commercially available products.

D. Framework

The use of an overall framework can assist in the selection of technologies to protect critical infrastructure against cyber attacks.

An overall framework should include:
(1) determining the business requirements for security;
(2) performing risk assessments;
(3) establishing a security policy;
(4) implementing a solution that includes people, process, and technology to mitigate identified security risks; and
(5) continuous monitoring and managing security.

Risk assessments, which are central to this framework, help organizations to determine which assets are most at risk and to identify countermeasures to mitigate those risks. Risk assessment [4] is based on a consideration of threats and vulnerabilities that could be exploited to inflict damage.

Even with such a framework, there often are competing demands for investments. For example, for some companies or infrastructures, mitigating physical risks may be more important than mitigating cyber risks. Further, adopting cloud computing technologies needs to make business sense. For some critical infrastructure owners, national security and law enforcement needs do not always outweigh the business needs of the entity. Without legal requirements for cyber-security, security officers often need to justify cyber-security investments using either strategic or financial measures. Further, critical infrastructures and their component entities are often dependent on systems and business functions that are beyond their control, such as other critical infrastructures and federal and third-party systems [6]. Several of the currently available cyber-security technologies could, if used properly, improve the cyber-security posture of critical infrastructures. It is important to bear in mind the limitations of some cyber-security technologies and to be aware that their capabilities should not be overstated. Technologies do not work in isolation. Cyber-security solutions make use of people, process, and technology. Cyber-security technology must work within an overall security process and be used by trained staff.

In many cases, numerous instances of cyber-security technology were being poorly implemented, which reduced the effectiveness of the technology to protect systems from attack. Best practices and guidelines are available from organizations such as NIST to assist infrastructure owners in selecting and implementing cyber-security technologies. To increase the use of currently available cyber-security technologies, various efforts can be undertaken. These efforts could include improving the cyber-security awareness of computer users and administrators, considering security when developing systems, and enhancing information sharing mechanisms between the federal government and critical infrastructure sectors, state and local government, and the public. For cloud computing there must be transparency and accountability provisions in any contracts between the provider and customer in whatever service model that is contracted.

E. Policy Analysis Framework

When deciding whether to continue or expand existing programs or to create new programs, it will be important for the federal government to consider the scope of the problem and the costs and benefits, the implementation issues, and the consequences of each option. Factual information is needed on the scope and scale of cyber vulnerabilities and the consequences of possible cyber attacks on critical infrastructures. The technology issues surrounding the problem and the structure of the security marketplace have to be determined. To help determine the proper approach for federal action, the government will require information from the private sector on the scope and size of the cyber-security problem and the actions that the private sector is already taking to address the problem. Further, information on critical infrastructure assets, vulnerabilities, and priorities, which could be gleaned if private sector entities follow the risk-based framework for security that we have described, is needed from the private sector.

As with any federal program, it will be important to measure the results of any federal cyber-security program [5-6]. However, the lack of well-defined security standards or benchmarks makes it difficult to measure the benefit of such a program. Further, what may be appropriate for some sectors may not be appropriate for others. While all sectors place some value on protecting the confidentiality, integrity, and availability of their computer systems and data, the relative importance of these objectives varies among the sectors. Further, because of business or other demands, the emphasis on cyber-security issues varies from entity to entity and from sector to sector.

It is also important to consider the proper role of the federal government. Sometimes, the best course of action may be to take no action at all. In some critical infrastructure sectors, private sector responses may adequately address a problem so that federal involvement is not required. A national CIP plan that defines the roles and responsibilities of federal and nonfederal CIP organizations; identifies and prioritizes critical assets, systems, and functions; and establishes standards and benchmarks for infrastructure protection could help the federal government to apply its limited resources where they are most needed.

Ultimately, the protection of critical infrastructures in this country falls on the critical infrastructure owners. However, as we have described, the federal government has several options at its disposal to manage and encourage the increased use of cyber-security technologies, research and develop new cyber-security technologies, and generally improve the cyber-security posture of critical infrastructure sectors [7]. Table 4 describes some policy options for a federal critical infrastructure protection plan.

TABLE IV. POLICY ANALYSIS FRAMEWORK

Policy option	Description
Assist infrastructures with risk assessments	Provide funding to sectors and sector entities to conduct risk assessments so that vulnerabilities, threats, and mitigation strategies can be identified.
Provide threat and vulnerability information to critical infrastructures	Increase the private sector's awareness of cyber threats and the need for cyber-security technologies by improving the federal government's capabilities to identify, analyze, and disseminate information about threats to and vulnerabilities of critical infrastructure sectors and their member entities.
Enhance information sharing by critical infrastructures	Increase the federal government's and the private sector's awareness of cyber threats and the effective implementation of technology by developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector.
Promote cyber-security awareness	Ensure that the private sector is aware of cyber-security services that are provided by the federal government and the critical infrastructure sectors.

III. CONCLUSIONS

Cloud computing has changed the way business is transacted in the information age. Indeed, with information explosion in a networked global environment, countries are increasingly wired and nations are highly interconnected, the protection of a country's critical infrastructure is a tremendous challenge for all levels of government. The task is even more important when the services affect the population of a country. As a result, oversight through auditing to reinforce accountability is an indispensible requirement in society.

The evolution of technologies have made IT services seamless and transparent to users, especially federal agencies; these services are now offered through the new paradigm called cloud computing, which holds promises for public institutions and private enterprises to improve their operations. However, since these services are provided by external entities, users of cloud computing must exercise due diligence in the evaluation and adoption of the model as well as providers. As is the case with other computing environments, data management challenges in cloud computing essentially involve accountability and auditing practices that are unique when the owners of the data assign custody to external providers. The issue of social trust lies at the foundation of cloud computing.

An effective program of data protection to meet the unique requirements for security and privacy in the context of accountability and auditing should address all aspects of the problem: people, process, and technology. Technology alone will never solve this problem of threat to an organization's data. The program should also involve both the government and the private sectors to develop realistic and implementable measures to guarantee the continuity of the provisions of services to the people, yet at the same time assure confidentiality, integrity and availability of the data that an organization might have entrusted to cloud service providers. At the same time, impact of these protective measures while operating in a cloud computing environment must be weighed on economic efficiency, social cohesion and personal privacy.

REFERENCES

[1] *Additional Guidance Needed to Address Cloud Computing Concerns*, The US Government Accountability Office, GAO-12-130T, Oct 6, 2011.

[2] "Customer Security Concerns in Cloud Computing," in International Conference on Networks. 2011.

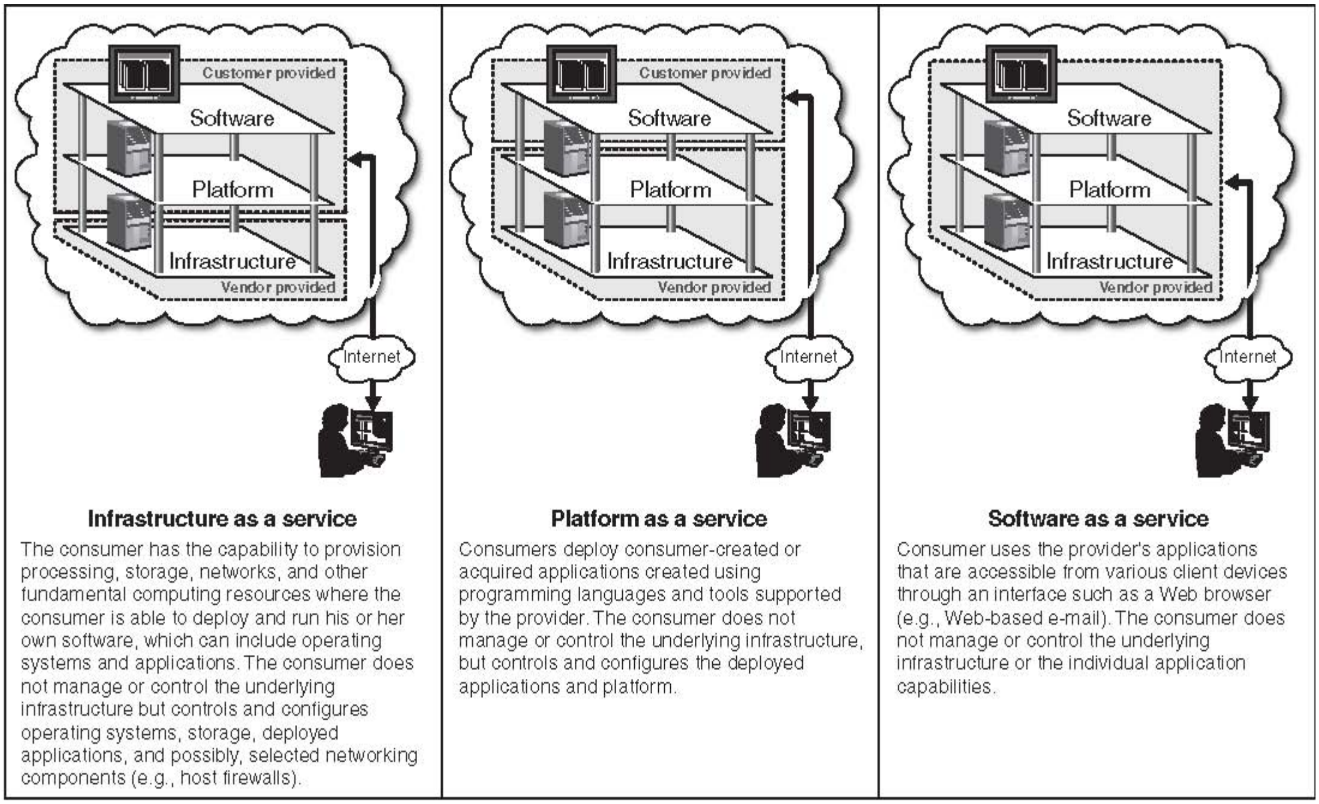
[3] "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," in Second International Conference on eHealth, Telemedicine, and Social Medicine. 2010.

[4] "SLA Perspective in Security Management for Cloud Computing," in Sixth International Conference on Networking and Services. 2010.

[5] "Multi-Tenancy Authorization System with Federated Identity to Cloud Environment Using Shibboleth," in International Conference on Networks, 2012.

[6] "Intrusion Detection for Grid and Cloud Computing," in IEEE IT Professional Magazine. 2010.

[7] "Management and Security for Grid, Cloud and Cognitive Networks," in Journal of Information Systems of the FSMA, 2011.



Infrastructure as a service

The consumer has the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run his or her own software, which can include operating systems and applications. The consumer does not manage or control the underlying infrastructure but controls and configures operating systems, storage, deployed applications, and possibly, selected networking components (e.g., host firewalls).

Platform as a service

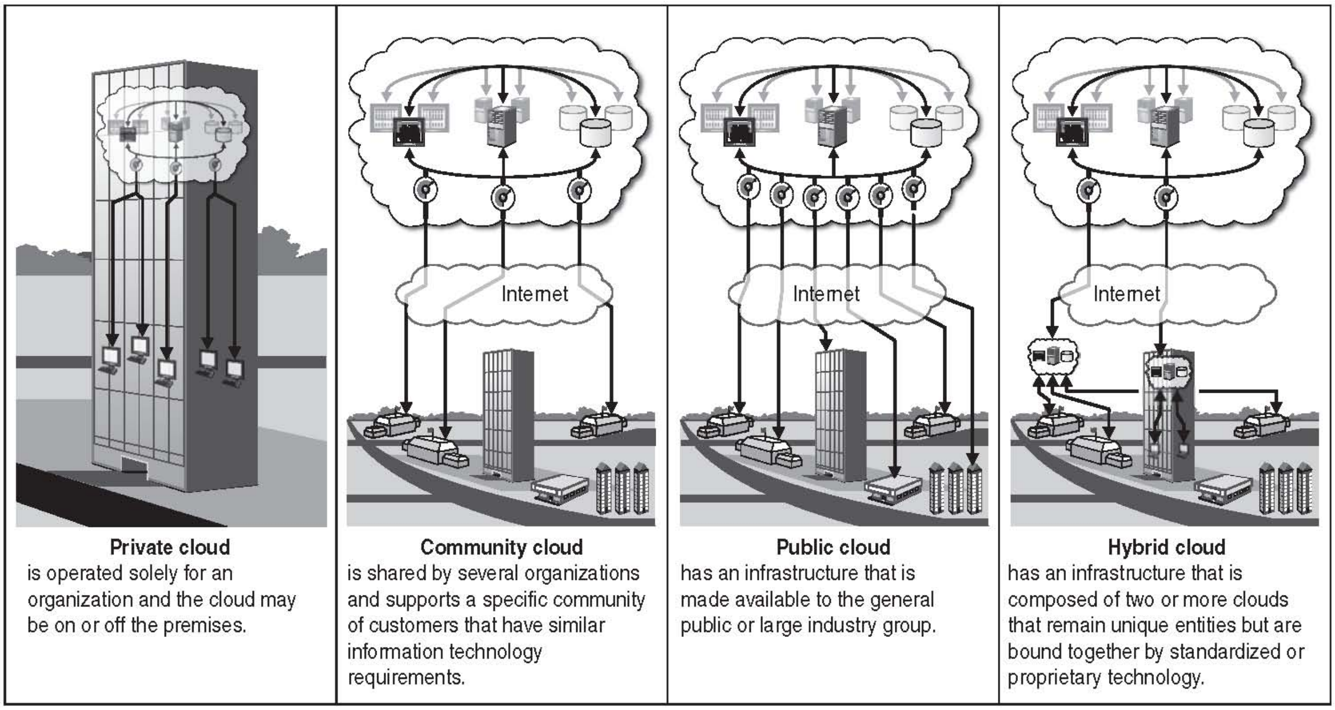
Consumers deploy consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying infrastructure, but controls and configures the deployed applications and platform.

Software as a service

Consumer uses the provider's applications that are accessible from various client devices through an interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying infrastructure or the individual application capabilities.

Source: GAO analysis of NIST data.

Figure 1. Cloud Computing Service Models



Private cloud
is operated solely for an organization and the cloud may be on or off the premises.

Community cloud
is shared by several organizations and supports a specific community of customers that have similar information technology requirements.

Public cloud
has an infrastructure that is made available to the general public or large industry group.

Hybrid cloud
has an infrastructure that is composed of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology.

Source: GAO analysis of NIST data.

Figure 2. Cloud Computing Environments