Comparison of Security Frameworks for Governmental Clouds between United States and European Union

Zhilong Wang[1], Tao Zhang[1], Yu Yang[2], Haipeng Qu[1*]
[1]College of Information Science and Engineering, Ocean University of China
NO.238 Songling Road, Qingdao, Shandong, China
[2]State Key Laboratory of Networking and Switching Technology,Beijing University of Posts and Telecommunications
No.10 Xitucheng Road, Haidian District, Beijing, China
+86 (532) 66786309
[*]Corresponding author's E-mail: quhaipeng@ouc.edu.cn

ABSTRACT

Cloud computing, as an emerging computing model, can provide users with inexpensive, convenient and large scale computing. In the recent years, both government and other organizations have begun to utilize cloud computing, such as the United States and European Union. However, deployment of clouds brings security challenges to consumers. Governmental cloud is a secure and trusted environment for government to deliver services to citizens. With the governmental use of cloud, there are many emerging risks and threats. It is important to focus on cloud security, governmental cloud in particular. United States proposed Security Reference Architecture and Challenging Security Requirements for US Government Cloud Computing Adoption and European Union proposed a security framework for governmental clouds. We introduce cloud computing, governmental cloud and risks related to use of cloud, then analyze the security frameworks of governmental cloud of United States and European Union. Finally, we make comparisons/comments on both frameworks from different perspectives.

CCS Concepts

• Computer systems organization → Architectures → Distributed architectures → Cloud computing • Security and privacy → Software and application security → Domain-specific security and privacy architectures.

Keywords

Governmental clouds; security framework; comparison; US; EU

1. INTRODUCTION

As an emerging technology, cloud computing can provide users with inexpensive, convenient and large scale computing. Cloud computing usage is growing steadily in the past years. The federal government has adopted cloud slowly in the recent years and more organizations and applications will move to cloud in the future. Though cloud computing provides a flexible solution for shared resources, software and information, it also brings additional security challenges to consumers using the clouds[1]. Once cloud computing is adopted in government and critical sectors, millions of users will be affected when attacks on cloud happened. It is important to focus on cloud security, governmental cloud in particular.

The organization of this paper is as follows. In section 2, we introduce features, service models and deployment models of cloud computing. In section 3, we introduce governmental clouds and survey on benefits and risks of deployment of gov clouds. In section 4, we introduce security frameworks for gov Cloud of United States and European Union. In section 5, we make comparison of security frameworks for gov Cloud between United States and European Union. Finally, we present our conclusions in section 6.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
ICCNS 2016, November 26-29, 2016, Singapore, Singapore
© 2016 ACM. ISBN 978-1-4503-4783-9/16/11...$15.00
DOI: http://dx.doi.org/10.1145/3017971.3017985

2. CLOUD COMPUTING[2]

According to National Institute of Standards and Technology (NIST)'s definition, Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model has five necessary features, four kinds of application models and three kinds of service models in cloud computing.

2.1 Features of Cloud Computing

On-demand self-service. It means that users can access to cloud service as needed without intervention of service providers.

Broad network access. Users can access to cloud service on the internet with any devices, such as mobile phones, ipads.

Resource pooling. All kinds of services, including computing resources, storage, memory, and virtual machines, are pooled and assigned to different users according to users' demand.

Rapid elasticity. Users can adjust the scale of resources used according to demands dynamically.

Measured Service. All computing resources and services can be monitored, controlled and measured .

2.2 Service Models

Cloud Software as a Service (SaaS). The third parties or service providers provide users with cloud applications which are applications running on a cloud infrastructure via internet, such as online word processors and consumer relationship management services.

Cloud Platform as a Service (PaaS). The platform provides users with tools and API (Application Programming Interface) to develop applications, manage and configure platform.

Cloud Infrastructure as a Service (IaaS). The capability provides users with computing resources including virtual machines,

hardware and operation systems that can be controlled and configure with API remotely.

2.3 Deployment Models

The four deployment models are private cloud, community cloud, public cloud and hybrid cloud.

Private cloud. The cloud infrastructure is owned and managed by only an organization.

Community cloud. The cloud infrastructure is shared by several organizations or a community which shared same missions, security requirements or policies.

Public cloud. Public cloud is owned by services providers who provide services for the public.

Hybrid cloud. Hybrid cloud is composed of more than two clouds, such as public cloud and private cloud.

3. Governmental Cloud

European Union Agency for Network and Information Security (ENISA) defines governmental cloud (Gov Cloud) as environment running services compliant with governmental and EU legislations on security, privacy and resilience, a secure and trustworthy way to run services under public body governance and a deployment model to build and deliver services to state agencies to citizens and to enterprises[3].

There are three kinds of roles in Gov Cloud, cloud consumer, cloud service provider and cloud owner.

Cloud owner is owner of Gov Cloud and defines related policies and requirement.

Cloud service provider (CSP) is the organization that provide related service to cloud owner and cloud consumers.

Cloud consumer is who consume the cloud services provided by CSP and cloud owners.

3.1 Benefits and Risks of Deployment of Gov Clouds

A key benefit of cloud computing is resilience when facing power cuts or natural disasters, especially for government users.

Security benefits of deployment of cloud[4]

The benefits of scale. Scale means that consumers can enjoy more services with less money.

Security as a market differentiator. With massive adoption of Gov cloud, cloud providers need to update their products and services to compete in the market.

More timely and effective and efficient updates and defaults. As more Gov cloud users and applications, the cloud providers will update their products more timely and efficiently to provide more secure services.

Rapid, smart scaling of resources. The cost will decrease with scaling resources, and users can more smartly use resources as needed.

Standardized interfaces for managed security services. Cloud providers will provide standardized interfaces to manage security services, with which users can better manage their resources.

3.2 Risks Related to Use of Gov Clouds[4,5]

The deployment of cloud computing in government will cause risks inevitably, there are some known and unknown risks and threats.

3.2.1 Known risks

Policy and organization related risks. The risks include monopoly, management failure, application challenge, failure of cloud service and combination of CSP.

Technology risks. Shortage of resource, isolation failure, malicious operation from CSP employees, loss of keys, attacks such as DDoS (Distributed Denial of Service) and EDoS (Economic Denial of Sustainability).

Legal risks. Data protection, change of right of jurisdiction and permission all will cause legal risks.

Risks outside of cloud. Network management, network flow redirect, attacks outsides, loss of backup data, loss of computer devices, natural disasters and so on.

3.2.2 Unknown risks

There are also some unknown risks with government use of cloud computing, such as security considerations on data access, availability and integrity when data is migrated to cloud. We may focus more on the unknown risks, because these unknown risks may cause unexpected results. And it takes time for us to look for an effective way to stop the disaster caused by unknown risks.

4. SECURITY FRAMEWORK FOR GOV CLOUDS

4.1 Security Framework for Gov Cloud of EU

In 2015, after analyzing the security policies of members of EU when deploying Gov Cloud and other countries' successful experience of Gov Cloud deployment, ENISA find some common security considerations in the deployment of Gov Cloud and propose the security Framework for Governmental Clouds[3].

The security framework for Gov Cloud use the classic Deming cycle (PDCA model), the life cycle of model includes 4 phase, plan, do, check and act. Each phase is divided into different security activities to achieve security objectives. There are detailed security steps within security activities.

The first phase, plan, including 3 activities, risk profiling, architectural model and security & privacy requirements, focuses on setting policies, a strategy for implementing controls to achieve security objectives. The do phase is composed of 2 activities, security controls and implementation development & accreditation. The check phase includes log/monitoring and audit and is to verify the efficiency and effectiveness of security activities deployed in the check phase. The act phase, including changes and exit management, involves actions deployed during act phase.

There is the overview of the logic model for security framework for Gov Cloud of EU (see Table 1).

4.2 Security Solutions of US Gov Clouds

By now, US does not propose formal security framework for Gov Cloud like EU. However, NIST published NIST Cloud Computing Security Reference Architecture, which can also be used for US Gov Cloud. The white paper Challenging Security Requirements for US Government Cloud Computing Adoption published by NIST propose basic security requirements for US Gov Cloud.

In the paper, we regard NIST Cloud Computing Security Reference Architecture and Challenging Security Requirements for US Government Cloud Computing Adoption as US security framework for Gov cloud.

Table 1. Overview of the Logic Model[3]

Lifecycle Phase	Security Activity	Security Steps
Plan	Risk Profiling	Identify services to cloudify
		Select relevant security dimensions
		Evaluate individual impact to dimensions
		Determine global risk profile
	Architectural model	Decide on the deployment service model
	Security & privacy requirements	Establish security requirements
Do	Security controls	Selection of security controls
	Implementation,development & accreditation	Formalization and implementation of the selected security controls
		Exante verification of suitability of the Cloud service to provide a sufficient level of assurance
		Start service execution
Check	Log/monitoring	Periodically check that security controls are in place and being followed
	Audit	Verification that the defined/contracted levels of security are fulfilled
Act	Changes	Implementation of remedies and improvement to the security framework
	Exit management	Contract termination, return of data to consumer and data deletion

Table 2. Overview of the Security Reference Architecture[6]

Role	Architectural components	Sub-components
Broker	Secure cloud service management	Secure provisioning and configuration
		Secure portability and interoperability
		Secure business support
	Secure cloud ecosystem orchestration	Secure service layer
	Secure service aggregation	Secure provisioning and configuration
		Secure portability and interoperability
	Secure service intermediation	Secure provisioning and configuration
	Secure Service Arbitrage	Secure provisioning and configuration
Consumer	Secure cloud consumption management	Secure configuration
		Secure portability/interoperability
		Secure business support
		Secure organizational support
	Secure cloud ecosystem orchestration	Functional layer
Provider	Secure cloud service management	Secure provisioning and configuration
		Secure portability and interoperability
		Secure business support
	Secure cloud ecosystem orchestration	Secure physical resource layer
		Secure resource abstraction and control layer
		Secure deployment & service layers
Auditor	Secure Auditing Environment	Security audit
		Privacy impact audit
		Performance audit
Carrier	Secure transport support	----

4.2.1 Cloud Computing Security Reference Architecture

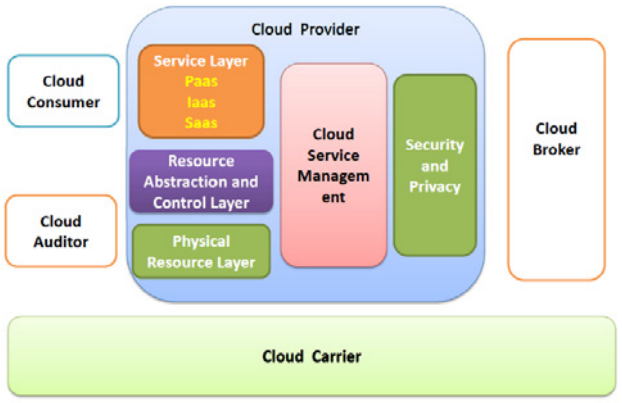

Figure 1. Formal Model – Security Reference Architecture[6]

In the security reference architecture (see Fig. 1), there are 5 kinds of users, cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier. Cloud providers protect personal information of cloud consumers, such as name, social security number, biometric records. Cloud auditor is who conducts independent assessments of cloud services, information systems operations, performance, privacy impact and security of cloud implementations. The carrier is to provide connectivity and transport of cloud service. A cloud Broker provides business and relationship services and plays the role of a Business Broker[6].

There is the overview of the security reference architecture proposed by NIST (see Table 2).

4.2.2 Security requirements proposed by NIST[7]

NIST proposed 17 security requirements in total which are divide into process-oriented security requirements and technically oriented security requirements. Examples of process-oriented security requirements are security controls for information systems based on cloud, cloud audit assurance, cloud certification and accreditation and forensics guidelines based on cloud. Technically oriented security requirements are proposed from technical prospective, examples are visibility and control for consumers, data security, access management and authorization, and incident response. Both of these requirements are important in government cloud computing adoption. These requirements can be regarded as baseline requirements when deploying Gov cloud.

There is the 17 security requirements proposed by NIST (see Table 3).

Table 3. Security Requirements Proposed by NIST[7]

Process-oriented security requirements	NIST SP 800-53 security controls for cloud-based information systems
	Cloud audit assurance and log sensitivity management
	Cloud certification and accreditation
	Needed electronic discovery guidelines
	Clarity on cloud actors security roles and responsibilities
	Trustworthiness of cloud operators
	Business continuity and disaster recovery
	Technical continuous monitoring capabilities
Technically oriented security requirements	Visibility for consumers
	Control for consumers
	Data security
	Risk of account compromise
	Identify credential and access management and authorization
	Multi-tenancy risks and concerns
	Cloud-based denial of service
	Incident response

5. COMPARISON/ANALYSIS OF SECURITY FRAMEWORK FOR GOV CLOUD BETWEEN EU AND US

ENISA proposed security framework for Gov cloud in 2015 as guidelines when EU members adopt Gov cloud. The framework includes 3 roles and uses classic PDCA model. There are different activities which are divided into ordered steps in different phases.

There are also some user cases and examples of logic secure Gov Cloud model in [3].

The PDCA model is widely used in project management and the benefits of the security framework for Gov clouds are significant. The PDCA is a cycle and problems will be solved in a cycle. With the introduction of PDCA, the security framework can be improved persistently.

NIST published NIST Cloud Computing Security Reference Architecture and Challenging Security Requirements for US

Government Cloud Computing Adoption, which are the same as security framework for US Gov cloud. There are 5 roles in the security architecture proposed by NIST. In [7], NIST lists 17 security requirements, explains the importance of these requirements and give different mitigation. When deploying Gov cloud, governments can take these requirements and mitigation into account to achieve the security goal and protect public privacy.

Table 4. Comparison of Security Framework for Gov Cloud between EU and US

	ENISA's security framework	NIST's security framework
Roles	3	5
Security activities	Yes	No
Security steps	Yes	No
Security requirements	No	Yes
Security mitigation	No	Yes
Security components	No	Yes

The security reference architecture proposed by NIST is different from ENISA's security framework for Gov cloud in roles, components and so on (see Table 4). The NIST's architecture focuses more on the components that are accumulated to achieve security goals. And the architecture is commonly used for all organizations, not only for governmental clouds. The security requirements for US government cloud computing adoption focus more on the requirements and importance of these requirements, then propose related mitigation. However, different countries may have different security needs and requirements on various applications, and the requirements may be unable to transplant. The components and sub-components, requirements and mitigation are more modules other than a framework.

NIST did not propose logic model as ENISA did. Although the security framework for Gov cloud has not been proposed formally, the requirements, mitigation and security reference architecture can be viewed as the preliminary version of security framework for Gov cloud for US.

The ENISA security framework gives a security framework with detailed security activities and security activity steps. Followed by these steps, Gov cloud users may adopt Gov cloud more securely. However, the PDCA model is born with some faults, such as with little intervention and creativity. Users who use the model need to follow these steps proposed before and it is hard to add new contents or change some steps. What's worse, the model may not be applicable in all Gov cloud users. The architecture may be good as a baseline or reference, but if we want to design our own security framework for Gov cloud, we may change the architecture as needed.

6. CONCLUSION

Cloud computing has the benefit of ease of use, portability, convenience, efficiency and cheapness. Some countries and organizations have been the first to adopt Gov clouds. However, the adoption of Gov cloud has brought some potential risks and challenges, such as data loss, data leakage, monopoly, application challenge, management failure and attacks on cloud. To be frank, the deployment of Gov cloud of US and EU is still low, security considerations may be the main reasons. The security frameworks proposed by ENISA and NIST will promote the actual Gov cloud deployment consequently. If Gov cloud users follow those steps in the security framework proposed by ENISA, the Gov cloud applications may be much securer. But the model is based on the PDCA model and it is difficult to change these steps and the model did not define the security requirements in the adoption of Gov cloud. The deployment of Gov cloud can refer to NIST Cloud Security Reference Architecture, but the security requirements of Gov cloud are different from cloud computing and there should be some changes. The frameworks can be used by existing Gov cloud as a baseline for analyzing side-by-side different deployments from MS[3]. The two frameworks can also be used for other countries to design their own best-practices of adoption of Gov clouds.

Comparing the different security architectures proposed by the EU and the US helps us to better understand how to move governmental applications and data into the cloud more securely and how to create and deploy safe and secure enterprise solutions quickly. In the future works, we would like to survey on security requirements in the adoption of Gov cloud and propose a security framework for Gov cloud adoption based on the PDCA security framework and NIST cloud security reference architecture.

7. ACKNOWLEDGMENTS

Our research is supported by CERNET Innovation Project (NGII20151203) .

8. REFERENCES

[1] Robert B. Bohn, John Messina, Fang Liu, Jin Tong, and Jian Mao. 2011. NIST Cloud Computing Reference Architecture. In Proceedings of the 2011 IEEE World Congress on Services (SERVICES '11). IEEE Computer Society, Washington, DC, USA, 594-596. DOI=http://dx.doi.org/10.1109/SERVICES.2011.105.

[2] Peter M. Mell and Timothy Grance. 2011. SP 800-145. the NIST Definition of Cloud Computing. Technical Report. NIST, Gaithersburg, MD, United States.

[3] ENISA(2015). "Security Framework for Govenmental Clouds".Available online at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds/at_download/fullReport,Feb 2015.

[4] Catteddu, D. (2010). Cloud Computing: Benefits, Risks and Recommendations for Information Security. Web Application Security. Springer Berlin Heidelberg.

[5] Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly, 27(3), 245-253.

[6] NIST. "NIST Cloud Computing Security Reference Architecture". Available online at http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

[7] Iorga, Michaela. "Challenging Security Requirements for US Government Cloud Computing Adoption." NIST (2012).