Security Threats in Cloud Computing Environments[1]

Kangchan Lee

Electronics and Telecommunications Research Institute
chan@etr.re.kr

Abstract

Cloud computing is a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources. The security for Cloud Computing is emerging area for study and this paper provide security topic in terms of cloud computing based on analysis of Cloud Security treats and Technical Components of Cloud Computing.

Keywords: *Cloud Computing, Security treats, Cloud service user, Cloud service provider*

1. Introduction

Cloud computing is a model for enabling service user's ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables cloud services.

The security architecture and functions highly depend on the reference architecture, and this paper shows the reference architecture and the main security issues concerning this architecture.

2. Technical Components of Cloud Computing

As shown in the Figure 1, key functions of a cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a set of functions:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.

Other functions like Management, Security & Privacy, etc. are considered as cross-layer functions that covers all the layers. The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who

[1] This research was supported by the ICT Standardization program of MKE(The Ministry of Knowledge Economy)

wants to use the reference architecture may select and implement only a subset of these layers.

However, from the security perspective, the principal of separation requires each layer to take charge of certain responsibilities. In event the security controls of one layer are by passed (e.g. access layer), other security functions could compensate and thus should be implemented either in other layers or as cross-layer functions.

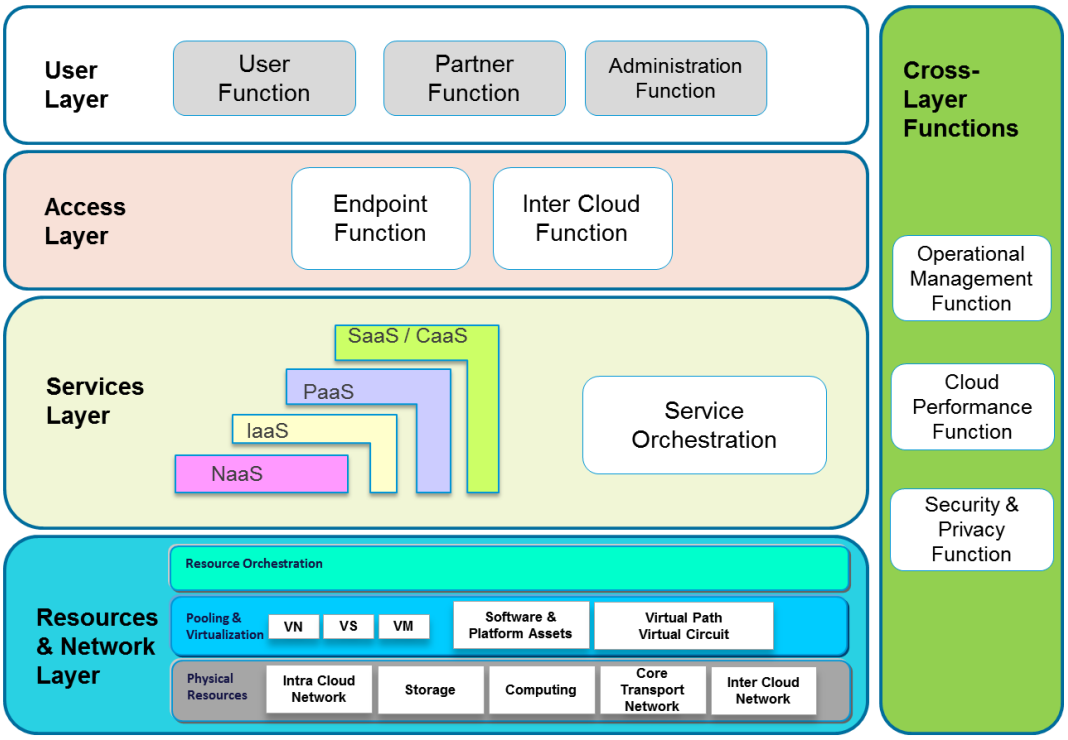

Figure 1. The Cloud Computing Components

3. Threats for Cloud Service Users

3.1 Responsibility Ambiguity

Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

3.2 Loss of Governance

For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.

3.3 Loss of Trust

It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

3.4 Service Provider Lock-in

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.

3.5 Unsecure Cloud Service User Access

As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

3.6 Lack of Information/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

3.7 Data loss and leakage

The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data center reliability; and disaster recovery can be recognized as major behaviors in this threat category.

4. Threats for Cloud Service Providers

4.1 Responsibility Ambiguity

Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user).

4.2 Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

4.3 Evolutional Risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

4.4 Business Discontinuity

The “as a service” feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

4.5 Supplier Lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked-in could be a lack of freedom regarding how to replace a supplier.

4.6 License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a “clouded” license management scheme which allows to pay only for used licenses may cause software use conflicts.

4.7 Bylaw Conflict

Depending on the bylaw of hosting country, data may be protected by different applicable jurisdiction. For instance, the USA Patriot Act may authorize such seizures. EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of protection guarantees. An international cloud service provider may commit bylaws of its local datacenters which is a legal threat to be taken into account.

4.8 Bad Integration

Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

4.9 Unsecure Administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

4.10 Shared Environment

Cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

4.11 Hypervisor Isolation Failure

The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms isolating attack” could be launched on a hypervisor to gain illegal access to other virtual machines’ memory.

4.12 Service Unavailability

Availability is not specific to cloud environment. However, because of the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers much more possibilities for an attacker. A typical Denial of Service attack on one service may clog the whole cloud system.

4.13 Data Unreliability

Data protection includes access to data for the confidentiality as well as its integrity. Cloud service users have concerns about how providers handle with their data, and whether their data is disclosed or illegally altered. Even if the cloud service user trust is not in the central of cloud security, it is a major marketing differentiator for a cloud service provider to advance the migration of IT system to cloud environment.

4.14 Abuse Right of Cloud Service Provider

For a cloud service user, migrating a part of its own IT to a cloud infrastructure implies to partially give control to the provider. This becomes a serious threat to cloud service user's data, notably regarding role and privileges assignment to providers. Coupled with lack of transparency regarding cloud provider practices may conduce mis-configuration or malicious insider attack. Such security breaches will lower the provider’s reputation, resulting in lower cloud service user confidence.

5. Conclusion

In any cloud service (infrastructure, software or platform) the end service provider or enterprise will control the access to the services. If these services are being hosted on the cloud, then the cloud provider (which may be different from the service provider or enterprise) also needs to protect their network from unauthorized accesses. However, since the cloud provider and the service provider or enterprise is legally different entities, they may in certain cases need to isolate their respective user information.

In this paper, we provide Cloud Security treats in terms of Cloud Service user and provider. Based on these Cloud Security treats, the following items are main topic for Cloud Security standardization:

- Security Architecture/Model and Framework
- Security Management and Audit Technology
- Business Continuity Planning (BCP) and Disaster Recovery
- Storage Security
- Data and Privacy Protection
- Account/Identity Management
- Network Monitoring and Incident Response
- Network Security Management
- Interoperability and Portability Security
- Virtualization Security
- Obligatory Predicates

References

[1] Recommendation ITU-T X.1500, "Overview of cybersecurity".
[2] Recommendation ITU-T E.409, "Incident organization and security incident handling: Guidelines for telecommunication organizations".
[3] FG Deliverable (Introduction to the cloud ecosystem: definitions, taxonomies, use cases, high level requirements and capabilities).
[4] Introduction to Global Inter-Cloud Technology Forum (GICTF) and its Roadmaps (Cloud-i-0026).
[5] OASIS Identity in the Cloud Technical Committee, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud.
[6] Architecture for Managing Clouds White Paper (DSP-IS0102), http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf.
[7] Special Publication 800-53, Recommended Security Controls for Federal Information Systems, **(2006)** December.
[8] Special Publication 800-125, "Guide to Security for Full Virtualization Technologies".
[9] Draft Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing", http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.
[10] Draft Special Publication 800-145, "Definition of Cloud Computing", http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf, **(2011)** January.
[11] Draft Special Publication 800-146, "Cloud Computing Synopsis and Recommendation", http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf, **(2011)** January.
[12] Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP.
[13] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, **(2009)** December.
[14] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, https://cloudsecurityalliance.org/research/security-guidance/, **(2011)** November.
[15] Top Threats to Cloud Computing V1.0, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[16] SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models, http://www.csoonline.com/article/print/660065.
[17] The Open Web Application Security Project, "10 Risks with Cloud IT Foundation Tier", https://www.owasp.org/index.php/Cloud-10_Risks_with_Cloud_IT_Foundation_Tier, **(2009)**.
[18] Cloud Computing and Security, A Natural Match, http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf, **(2010)**.
[19] P. A. Karger, "Multi-Level Security Requirements for Hypervisors", ISBN: 0-7695-2461-3, 21st Annual Computer Security Applications Conference, **(2005)** December 5-9, pp. – 275.
[20] RSA Office of the CTO, "A Proposed Security Architecture for Next-Generation Data Center", **(2010)** January 29.
[21] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments", Whitepaper, **(2008)**.
[22] T. Garfinkel, M. Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", In Proc. Network and Distributed Systems Security Symposium, **(2003)**, pp. 191-206.
[23] O. Gerstel and G. Sasaki, "Quality of Protection (QoP): A Quantitative Unifying Paradigm to Protection Service Grades", Proceedings of SPIE , vol. 4599 (1), SPIE – **(2001)** August 9.
[24] O. Gerstel and G. Sasaki, "A General Framework for Service Availability for Bandwidth-Efficient Connection-Oriented Networks", IEEE/ACM Transactions on Networking, vol. 18, Issue 3, **(2010)** June, pp. 985-995.
[25] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Proceedings on First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009, Lecture Notes in Computer Science, vol. 5931, **(2009)**, pp. 69-79.
[26] D. Xu, Y. Li, M. Chiang and A. R. Calderbank, "Elastic Service Availability: Utility Framework and Optimal Provisioning", IEEE Journal on Selected Areas in Communications, vol. 26, no. 6, **(2008)** August.

Author

Dr. Kangchan Lee has been working for ETRI since 2001. He started in Protocol Engineering Center to develop the technology and standards for Next Generation Web. Until now, he has been participated several standardization projects which are related to Web technologies, such as Ubiquitous Web Services, Mobile Web, etc, and his major research interests are Next Generation Web, Cloud Computing, Future Networks, distributed system integration, database integration technology, digital library, information retrieval and database, and structured document, etc. He has also been actively involved in international and domestic standardization activities. Regarding of international standardization activity, he has been working for a deputy manager of W3C Korea Office since 2002. Since 2005, he is working with ITU-T to develop the Web-based convergence service standard in NGN environment with several editorships in Study Group 13 of ITU-T. Also he is now the Rapporteur of NGWeb (Next Generation Web) EG (Expert Group) at ASTAP for 5 years since 2003.