Security Architectures for Cloud Computing

● Masayuki Okuhara ● Tetsuo Shiozaki ● Takuya Suzuki

Moving computing into the "Cloud" makes computer processing much more convenient for users but also presents them with new security problems about safety and reliability. To solve these problems, service providers must establish and provide security architectures for Cloud computing. This paper describes domestic and international trends in security requirements for Cloud computing, along with security architectures proposed by Fujitsu such as access protocol, authentication and identity (ID) management, and security visualization.

1. Introduction

Cloud computing is a new processing scheme in which computer processing is performed in the Internet "Cloud." This means that users need not concern themselves with the processing details. Although Cloud computing enables flexible and agile computing impossible with existing systems, it brings new security problems that make users anxious about safety and reliability. This paper describes the security problems surrounding Cloud computing and presents existing approaches to solving them. It also describes the security architectures of a service platform proposed by Fujitsu for dealing with those problems.

2. Security problems in Cloud computing

Users feel a sense of security and reliability when they understand exactly how a process is functioning and running. Although Cloud computing offers great user convenience by freeing users from the need to understand processing details, it forces them to trust the Cloud services provider, which worries many users. In today's market, awareness about Cloud computing problems is heavily weighted toward security and reliability problems. For example, a survey conducted by Fujitsu on problems in Cloud computing from the customer viewpoint (**Figure 1**) revealed that security, stable operation, and a support system, that is, safety and reliability, ranked highest among user concerns. Given that in Cloud computing the information technology (IT) system is invisible to the user, it is understandable that customers strongly want their information to be fully protected and services to be provided stably. The following concerns, in particular, are commonly raised by customers with regard to security:

1) Within the same data center, there are some cases in which information belonging to more than one customer resides on the same computer. In such a case, will such different sets of information be appropriately isolated?
2) Should we be concerned that operations in a data center might lead to information leakage or data corruption caused, for example, by one customer's information

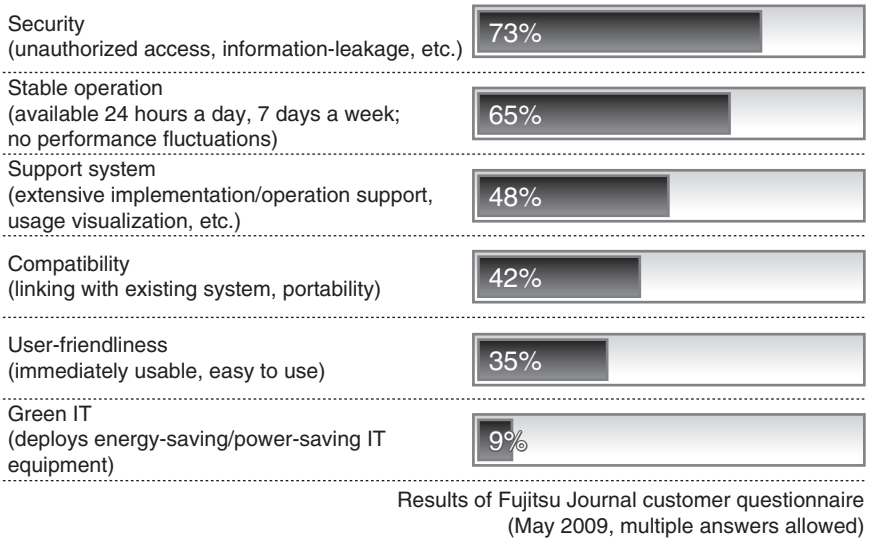

Figure 1
Concerns in using Cloud computing.

being mistaken for another's?

3) Since the system platform of a Cloud services provider is shared by a wide variety of customer environments, couldn't reliability be a problem? For example, if a malicious program such as a virus were to penetrate the service, mightn't all the environments using that service might be affected?

4) When multiple Cloud services are used at the same time to perform work involving the linking of tasks between those services, can service reliability be assured?

3. Security demanded of Cloud computing

How then should a Cloud services provider respond to the abovementioned security-related problems? This is a question that cannot be avoided if providers want their customers to use Cloud computing without worry.

The approach taken by the Cloud Security Alliance (CSA)[1] in the USA, where Cloud computing is advancing quickly, provides valuable clues to a possible answer. The CSA, which began activities in October 2008, is a non-profit organization composed of Cloud-computing-related companies. It has organized the security requirements demanded of Cloud computing and released them in the form of guidelines entitled "Security Guidance for Critical Areas of Focus in Cloud Computing." Version 2.1 (January 2010) of these guidelines describes necessary security considerations for performing critical tasks on a Cloud-computing platform divided into the 13 domains listed below. This information can serve as a reference for both the side implementing Cloud computing and the side using it.

- Domain 1: Cloud computing architectural framework
- Domain 2: Governance and enterprise risk management
- Domain 3: Legal and electronic discovery
- Domain 4: Compliance and audit
- Domain 5: Information life cycle management
- Domain 6: Portability and interoperability
- Domain 7: Traditional security, business continuity, and disaster recovery
- Domain 8: Data center operations
- Domain 9: Incident response, notification, and remediation
- Domain 10: Application security
- Domain 11: Encryption and key management
- Domain 12: Identity and access management

・ Domain 13: Virtualization

In addition to the above, the European Network and Information Security Agency (ENISA)[2] released a report entitled "ENISA Cloud Computing Security Risk Assessment" in November 2009. It assesses 35 types of security risks in Cloud computing through use-case scenarios.

On the basis of these groundbreaking surveys and studies, activities for organizing Cloud computing requirements have also begun in Japan under the leadership of the Ministry of Internal Affairs and Communications (MIC) and Ministry of Economy, Trade and Industry (METI).

Among these requirements, Fujitsu considers access control, authentication and ID management, and security visualization to be particularly important themes considering the nature of Cloud computing. The following sections introduce Fujitsu's approach to Cloud computing security architectures in these areas.

4. Access control

The most outstanding feature of a Cloud-computing platform is across-the-board virtualization. The virtualization of each system level leads to flexible system construction and operation essential to Cloud computing.

In Fujitsu's Cloud services platform called the "Trusted-Service Platform," the network, operating-system, and data layers feature a logical separation of computing environments through advanced virtualization technology established, for example, by METI's secure platform project. This logical separation by virtualization achieves the same level of security as physical separation of computing environments (**Figure 2**).

To ensure sufficient reliability, especially in the virtual-server layer, which is the focus of virtualization, source-code reviews of the virtualization software are conducted within Fujitsu. Moreover, through the combination of virtualization and more robust authentication of Cloud-computing clients and the addition of key functions such as ones for visualizing access

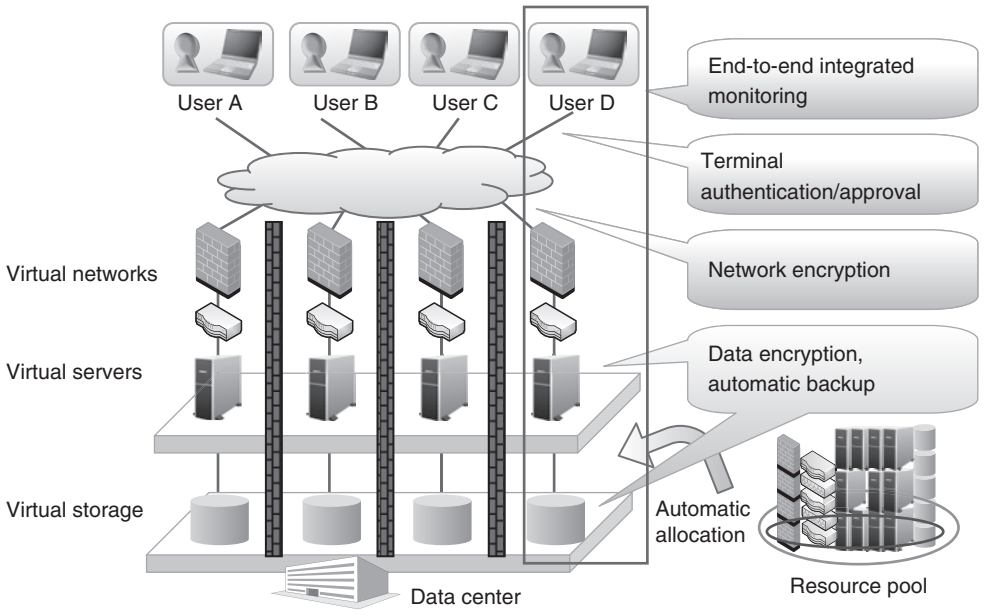

Figure 2
Separation of Cloud computing environments.

activities, it has become possible to detect and prevent access-control problems and attack schemes and to create more effective security measures.

5. Authentication and ID management

Proper authentication of users or user environments such as a client computer is basic to access control and other IT security functions. It is an essential technology for Cloud-computing environments in which connections to external environments are common and risks are high.

In Fujitsu's Cloud computing, there are plans to provide various options to fortify traditional authentication based on an identifier (ID)/password format. In one-time password authentication, for example, the user enters a temporary password displayed on a dedicated card or on a mobile phone into a field on a Web screen as authentication information. This mechanism prevents the reuse of a password even if it should leak for some reason during transmission and therefore makes authentication significantly safer. In addition, the use of device authentication technology using digital certificates or other means can provide much safer authentication than password-based authentication, which is relatively easy to crack through guessing, leakage, etc.

The management of user information when a user operates multiple systems by Cloud computing is also a major issue. So-called ghost IDs—leftover IDs of users who have lost their usage rights—and IDs that have been given inappropriate rights because of management oversights are a problem in terms of not only security but also corporate internal controls. To solve this problem, one needs a mechanism for identity management common to multiple systems. In Fujitsu's Cloud computing, there are plans to provide customers with an ID management platform based on open ID management frameworks such as the Security Assertion Markup Language (SAML)[note 1] and WS-Federation.[note 2]

6. Security visualization

A characteristic of Cloud computing is that unnecessary details are invisible. However, this is exactly why necessary things must be clearly visible to reassure customers and instill confidence in Cloud computing.

Fujitsu is taking various approaches to security visualization. For example, it developed a security dashboard in 2009 for visualizing security conditions within the Fujitsu Group. This dashboard has helped to improve security governance. Also in the same year, Fujitsu began to provide an information-security visualization service to enable customers to visualize the efficiency and cost-effectiveness of information-security measures.

In 2010, Fujitsu will begin providing a security monitoring service using the ArcSight monitoring platform adopted in the USA and elsewhere in the world. This platform gathers security-related information from a customer's various business systems on the Cloud, manages that information in a unified manner, and provides value-added reports from the viewpoints of information-security governance, internal controls, and the effects of security measures. Deploying such a general-purpose information-gathering platform can improve the efficiency of security management and, by extension, the efficiency of internal controls and corporate risk management in the Cloud-computing era.

This service can also be used to efficiently and safely outsource the managing and archiving of corporate and organizational logs that require

note 1) XML-based protocol drawn up by the OASIS standards body for exchanging authentication information and attribute data such as IDs and passwords.

note 2) Technical specifications released in April 2002 by Microsoft, IBM, and VeriSign for linking IDs, accounts, attributes, authentications, approvals, etc.

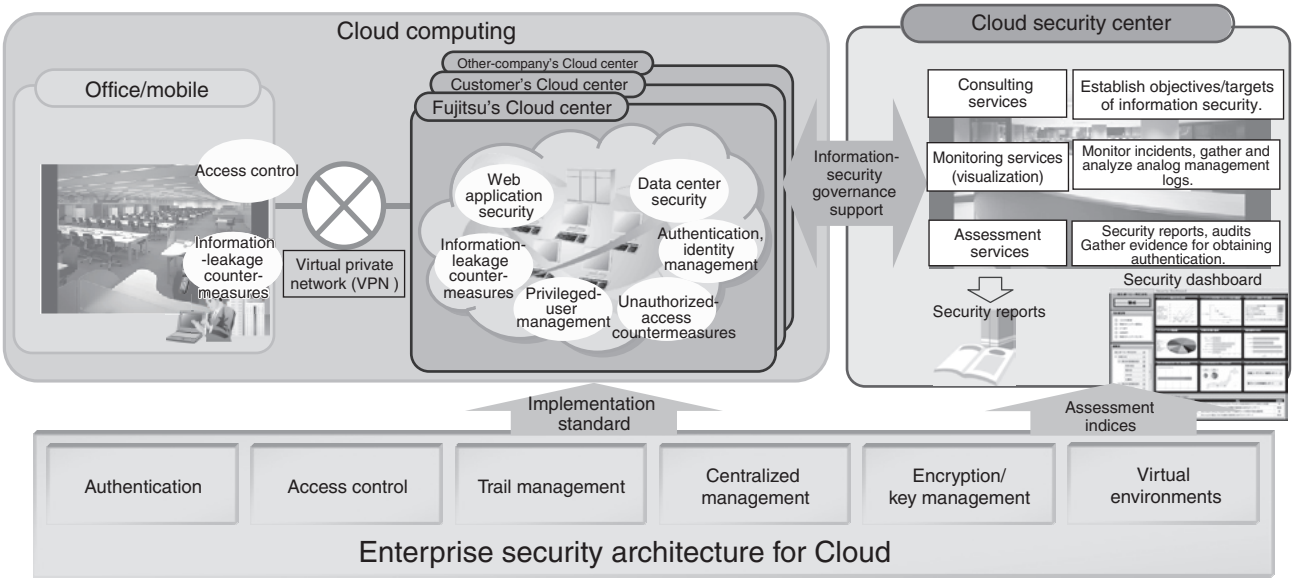

Figure 3
Monitoring concept of Cloud computing.

a considerable amount of storage. In this way, the service can reduce management costs and provide thorough maintenance of log data.

The work of recording and monitoring security-related activities in the Fujitsu Cloud is performed by a special organization that is independent of the Fujitsu department providing Cloud services. This scheme allows Cloud computing security to be assessed independently of the service business (**Figure 3**).

7. Conclusion

In this paper, we explained how customers, despite their deep-seated concerns and uneasiness about Cloud computing, can enjoy the benefits of the Cloud without worry if Cloud services providers use appropriate architectures for implementing security measures. We also described the security problems that surround Cloud computing and outlined Fujitsu's security architectures for solving them. Fujitsu provides support for drafting security policies and creating security strategies as part of a consulting menu for businesses migrating to Cloud computing. Going forward, we hope to dispel any concerns that customers may have when considering a move to Cloud computing for various types of tasks and operations.

References

1) Cloud Security Alliance.
http://www.cloudsecurityalliance.org/
2) ENISA: Cloud Computing Security Risk Assessment.
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Masayuki Okuhara
Fujitsu Ltd.
Mr. Okuhara is a director of Fujitsu's Information Security Center and engaged in strategic planning for the IT security solutions business.

Tetsuo Shiozaki
Fujitsu Ltd.
Mr. Shiozaki is the general manager of Fujitsu's Information Security Center and engaged in strategic planning for the IT security solutions business.

Takuya Suzuki
Fujitsu Ltd.
Mr. Suzuki is engaged in strategic planning for the IT security solutions business.