Feature

Sivarama Subramanian, CISM, is lead, security testing for Center of Excellence (CoE) at Cognizant Technology Solutions, where he leads the security testing research, enabling new service rollouts and aligning new security trends to customer needs. Subramanian is a silver member of the ISACA Chennai (India) Chapter and can be reached at *sivaramasubramanian.kailasam@cognizant.com.*

Devaraj Munuswamy, CEH, is a security testing manager and security researcher at Cognizant Technology Solutions, where he is currently managing a security testing program for a publishing media company. He is an active member of Null (an open security community) in Chennai and Bangalore (India). Munuswamy can be reached at *Devaraj.munuswamy@cognizant.com.*

Security Mysteries in the Cloud

In the current world of IT, "cloud" is a buzzword heard everywhere. Many organizations are moving to cloud computing because of its scalability, on-demand service offerings over the Internet, virtualization and cost efficiency. In the future, with the rise of the hybrid cloud, organizations are likely to desire that cloud providers guarantee that private and public cloud services are secure. Forrester Research predicted in the beginning of 2014 that large vendors, such as HP, Cisco, VMware and IBM, will purchase start-ups dedicated to encrypting a company's data before such data go to the cloud.[1]

Many studies have revealed various security challenges and mysteries faced in cloud computing.[2] These studies examined the security issues related to applications, platforms and infrastructures that are offered as a service by cloud providers and their corresponding mitigation plans to overcome these issues.

ABOUT THE CLOUD

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices handle application processing. Cloud computing is defined as a set of hardware, network, storage, services and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure and storage over the Internet (either as separate components or a complete platform) based on user demand. Cloud computing helps organizations quickly go to market and reduce capital spending due to the cloud's capability to provision and release resources on demand (elasticity).

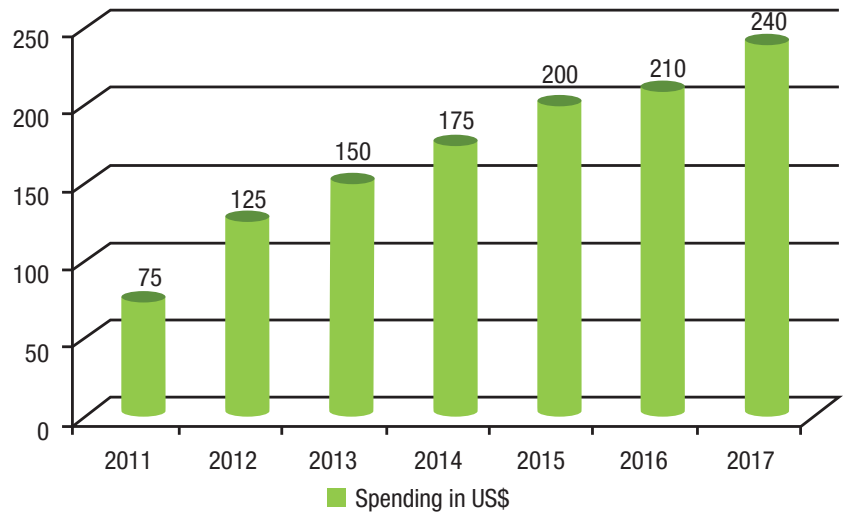
Figure 1 depicts the statistics of expenditure on cloud computing.[3] This graph depicts the investment on cloud increasing gradually.

TYPES OF CLOUD SERVICES

Cloud computing services are broadly classified into three categories (**figure 2**):

- **Software as a Service (SaaS)**—These are applications that are offered as a service to end users over the Internet. This type of service is the most common service offered in the cloud. The applications are owned by third-party providers and are offered to end users in a pay-as-you-go model. The users of this type of service are network architects.

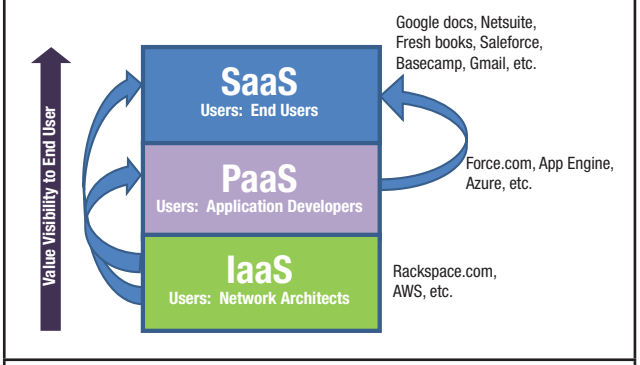
Figure 1—Global Spending Forecast for Cloud Through 2017



Source: IHS Technology. Reprinted with permission.

- **Platform as a Service (PaaS)**—This type of service provides whatever is required for building and delivering a web-based application without the cost of investing in software, provisioning and hosting. In this type of service, customers have their own build and version of the application over the provided platform. The key beneficiaries of this type of service are application developers.
- **Infrastructure as a Service (IaaS)**—This type of service provides organizations with computing resources, including servers, networking, storage and data center space, on a pay-per-use basis. The key beneficiaries of this type of service are network architects.

Figure 2—Cloud Service Types and Beneficiaries



Source: Subramanian and Munuswamy. Reprinted with permission.

PaaS and SaaS sit on top of the IaaS model, which is indicated by the blue arrow in the diagram, and for PaaS, it is SaaS that sits on top of it.

CLOUD ARCHITECTURE

There are two commonly used cloud architectures:

- **Multitenant**—In a multitenant architecture (also known as single instance), the same physical server/platform is utilized to provide services for multiple users/organizations, usually separated by a partition to prevent the data from being accessed by unauthorized users. As all services are hosted on the same server, there must be a standard SaaS architecture that includes the same configuration capabilities for the hardware, network and operating system for all customers, also known as tenants.

Enjoying this article?

- Read *Security Considerations for Cloud Computing.*
  www.isaca.org/cloud-security
- Learn more about, discuss and collaborate on cloud computing in the Knowledge Center.
  www.isaca.org/topic-cloud-computing

- **Single-tenant**—Single-tenant architecture (also called multi-instance) is a separate instance of a software application and supporting infrastructure used by each customer or tenant. Single-tenant architecture is mainly used by companies that need a customized approach, either because of their geography (or that of their client-base) or their need for a higher level of security. With single-tenant, each company has a distinct database and system that are either placed on an individual server or segregated using extensive security controls to create a virtual server network.

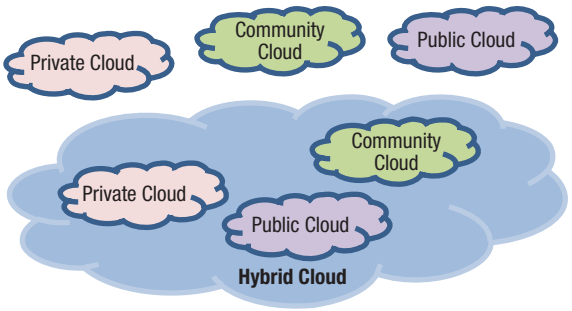
The deployment models for cloud are broadly classified into four types:

1. **Public cloud**—Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organizations or individuals. With public cloud services, users do not need to purchase hardware, software or supporting infrastructure, which is owned and managed by providers.
2. **Private cloud**—A private cloud is owned and operated by a single company that controls the way virtualized resources and automated services are customized and used by various lines of businesses and constituent groups. Private clouds exist to take advantage of many of the cloud's efficiencies while providing more control of resources and steering clear of multitenancy.
3. **Hybrid cloud**—A hybrid cloud uses a private cloud foundation combined with the strategic use of public cloud services. The reality is a private cloud cannot exist in isolation from the rest of a company's IT resources and the public cloud. Most companies with private clouds will evolve to manage workloads across data centers, private clouds and public clouds, thereby creating hybrid clouds.

4. **Community cloud**—A community cloud is a multitenant infrastructure that is shared by many organizations within a specific group, irrespective of whether the cloud is managed by a third party or by any organization in the group. The advantage of a community cloud is to offer a public cloud to an organization within the group. The community cloud can be either on-premise or off-premise and can be governed by the participating organizations or by a third-party managed service provider (MSP).

Figure 3 shows the interaction and areas of overlap among the different types of cloud deployment.

Figure 3—Cloud Deployment Models



Source: Subramanian and Munuswamy. Reprinted with permission.

CLOUD SECURITY CHALLENGES AND MITIGATIONS

Security is the most important aspect to be considered when moving to cloud computing. There are various security challenges and mysteries in each of the different types of services offered by the cloud.

IaaS Challenges

The possible security challenges and mysteries in IaaS are as follows.

IaaS Cloud Vendor Selection

The first and foremost security challenge in an IaaS cloud environment is selecting the appropriate cloud service provider (CSP) that has built-in security features on its cloud. If the CSP does not have proper security features implemented in the cloud environment, the applications deployed in the cloud environment, along with the data, may be compromised.

To overcome this challenge, the following can be done to ensure that security aspects are addressed:

- Verification and validation of physical security and built-in security features on the infrastructure resources (e.g., firewalls, load balancers, network segmentation), role-based access controls and application programming interfaces (APIs) are maintained securely.
- Verification and validation of compliance of the CSP against standards such as ISO 27000, Payment Card Industry Data Security Standard (PCI DSS), SSAE 16 and the US National Institute of Standards and Technology (NIST).[4]

Identity and Access Control Management

The Verizon 2013 Data Breach Investigations Report study showed that 76 percent of security breaches involve some kind of weak or stolen credentials, and another 13 percent involve privilege misuse or abuse.[5] Identity and access controls are even more important in the cloud as, unlike in corporate networks, users may not need a physical network connection to access resources in the cloud. Improper implementation of identity and access control management could lead to attacks or user privilege escalations.

The following actions can be taken to overcome the challenges related to identifying and accessing controls:

- Implement multifactor authentication in the cloud.
- Integrate corporate user directory with the cloud for effective and timely termination of user accounts.
- Implement proper role-based access controls (RBAC).

Verizon Universal Identity Services is an option for strong authentication, access control, multifactor authentication and integration with corporate directories.

Log Monitoring and Management

A large number of data breaches are still not discovered, because most organizations and vendors do not have effective log monitoring in place, which puts the IaaS services at risk.

The following mitigations can be implemented to address the challenges related to logs:

- Integrate the log data from the cloud with a corporate log data management strategy.
- Monitor logs for operating systems, applications and security devices in the cloud, and check if the IaaS cloud vendor provides firewall logs for correlation.

Data Encryption

Unprotected sensitive data are the next big challenge in the cloud. To mitigate this challenge, the following methods need to be adopted:

- **Full-disk encryption**—Full-disk encryption or policy-based partial encryption of data should be enforced.
- **Database encryption**—Database-level encryption controls should be implemented.
- **Network encryption**—This includes network-level encryption controls including, but not limited to, Secure Sockets Layer (SSL), Internet Protocol Security (IPsec) and encryption gateways.
- **Data backup**—The cloud vendor should provide encryption for backup data as well.

PaaS Challenges

The possible security challenges and mysteries in PaaS are as follows.

Data Location

PaaS offers a platform that is not a single host. Rather, the platform can be thought of as a group of clustered hosts. This means that, physically, the location of data cannot be isolated to a specific sector on a specific cloud. The lack of a single location for data adds to the security challenge, because a single location is easier to secure than multiple locations. Secondly, since data reside in different locations, data are never fully deleted; instead, the pointers to the data are deleted. Thus, distributed data remain like any other data, which adds to the security challenge.

Mitigations to avoid or overcome these challenges are:

- An agreement should be made with the CSP that all the data storage resources be properly security patched.
- Proper backup of data needs to be implemented, as do measures to ensure that data, once deleted in one location, are fully deleted.

Access Privileges

One of the popular features in PaaS is built-in debug. Debug mode grants access to data and storage locations, allowing developers to step through code/data and modify values in order to test various outcomes. Debug offers the equivalent of privileged access and is a highly desired tool for developers and hackers. Oftentimes, programmers want to work within the privileged environment and simply request full access rather than going through the process of determining which specific privileges are actually needed.

By moving development into the PaaS environment, organizations transfer this access problem to the CSP to resolve. Obviously, this does not guarantee the safest or best resolution of the problem, but it moves responsibility to another entity.

Mitigations to overcome this challenge include:

- Highly privileged access should not be moved to the PaaS environment.
- Organizations should establish or opt for a hybrid cloud so that the privileged environment is under the control of the organization instead of the CSP.

Distributed System

The PaaS file system is often made up of highly distributed nodes that may be independent, but the CSP owns the cluster, so it is likely that standardized configuration paths are in place. However, there are challenges associated with this type of system. For example, one popular implementation of distributed system uses the Hadoop distributed file system (HDFS), which uses default ports 50070, 50075 and 50090.[6] These ports are Transmission Control Protocol (TCP) ports, but they represent attack vectors in which various inputs can be tried in an attempt to cause failures or denial-of-service (DoS) attacks.

To mitigate this challenge, it is important to recognize that potential attack vectors are not real vulnerabilities; they represent areas that require additional analysis before committing to the PaaS architecture. Evaluation of the traffic flow and the security mechanisms in place are minimal requirements. The CSP should be able to provide the necessary security, but the responsibility for verifying this belongs to the end user or organizations that utilize PaaS services.

SaaS Challenges

Apart from the multitude of advantages that SaaS provides to organizations, there are still a few challenges that an organization may encounter when dealing with SaaS. The following are some of the most common security challenges that business may face when using SaaS services.

Lack of Control Over Application Security Aspects

It is common practice for an organization to utilize a SaaS over the Internet.[7] Ideally, CSPs should address all security-related issues with the help of extensive penetration testing. However, there is no guarantee that the CSP has addressed all security vulnerabilities in the platform.

The ways to mitigate this challenge are:

- Organizations/end user of SaaS services should have an agreement with the CSP that applications provided as a service should be properly penetration-tested before production release.
- If not penetration-tested by the CSP, the client should be allowed to conduct penetration testing for the applications that they are using.

Identity Protection

In the case of providing a single sign-on login to access multiple applications over the Internet (e.g., email, contacts, calendar, documents), it is easier to hijack the credentials via session hijacking (e.g., side jacking, cross-site scripting).

To mitigate this challenge, the CSP should implement strong identity management for the application as a service to end users—providing various authentication mechanisms, including, for example, two-way authentication and secret question authentication.

SECURITY TESTING TOOLS IN THE CLOUD

The assurance of security can be best provided by performing periodic and continuous penetration testing for cloud security solutions. There are various penetration testing tools that are used for the applications hosted in the cloud.

Core Cloud Inspect is a tool that is used to test Amazon Web Services (AWS)-hosted machines and applications to check for vulnerabilities and provide proper recommendations for the identified ones.

NeXpose Community Edition is a free collection of vulnerability management tools that offers scan templates and the ability to scan networks, operating systems, desktops and databases.

SECURITY STANDARDS IN THE CLOUD

As cloud computing is now used widely, adherence to standards based on these service offerings for various domains has also become important. Some of the standards associated with the cloud are:

- US Federal Information Security Management Act (FISMA)
- US Health Insurance Portability Accountability Act (HIPAA)
- US Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- American Institute of Certified Public Accountants' (AICPA) Auditing Standards Board's Statements on Auditing Standards (SAS)
- Open Web Application Security Project (OWASP)

A CASE STUDY

For example, a global beauty products company with an extensive portfolio of beauty brands sold in more than 100 countries. The organization uses SaaS for the company's employee management and payroll teams, and they were able to easily manage human resources (HR) and payroll processes off-site. Wages were paid without any disruption to the company's employees.

Security Challenges

Due to the nature of its business and the sensitivity of data, the company wanted to safeguard its sensitive data from any cloud-specific attack and opted for a security assessment of its application to defend against such attacks. The security assessment gives the posture of security for its data and platform.

Tools Used

The commercial tool used for this assessment provides the below solution:

1. Validate your cloud deployments with real-world security intelligence.
2. Quickly and easily verify your cloud security and gain actionable information to remediate exposures.
3. Keep up with evolving threats with repeatable, updated cloud security testing.

Approach

The steps followed by the organization in order to validate cloud security included:

- Provide an automated, tool-based approach, along with manual evaluation of security vulnerabilities outlined in the OWASP Cloud Top 10 Security Risks.
- Identify the root cause of the security vulnerabilities.
- Provide recommendations and help the cloud service provider (CSP) remediate the issues identified.
- Present an executive security assessment summary report that gives an overview of the solution's security.

Benefits of the Security Assessment

The security assessment:

1. Provided the current security posture of the SaaS platform.
2. Identified basic to real-time threats, e.g., multitenancy and physical security, user privacy and secondary usage of data, accountability and data ownership.
3. Provided recommendations for high-severity vulnerabilities, including:
   - That the provider encrypt the data-at-rest and the data-in-transit to avoid hard-sniffing of sensitive information
   - The use of strong encryption algorithms and adoption of encrypted storage
   - Verification that the provider destroys deleted data in such a way that they cannot be re-created later
   - The use of multiple layers of authentication

Figure 4 depicts 15 vulnerabilities that were identified as a part of this assessment, based on OWASP Cloud Top 10 Security Risks.

Figure 4—Vulnerabilities Identified During Security Assessment

Vulnerabilities Identified	Number of Vulnerabilities
Accountability and data Ownership	5
Service and data integration	3
Multitenancy and physical security	5
Nonproduction environment exposure	2
Total no. of vulnerabilities	**15**

Source: Subramanian and Munuswamy. Reprinted with permission.

CONCLUSION

Security and privacy of the cloud remain two of the top concerns for IT decision makers. With a thoughtful strategy, security mysteries can be addressed and resolved by proactively conducting periodic security assessments using both automated and manual approaches.

Organizations can mitigate the security challenges captured in this article based on their requirement to consume cloud services such as SaaS, PaaS and IaaS.

ENDNOTES

[1] Jansen, J; "Top 10 Predictions on the Future of the Cloud in 2014," *Business Today,* 2 January 2014, *www.businesstoday.org/articles/2014/01/top-10-predictions-on-the-future-of-the-cloud-in-2014*

[2] Hashizume, Keiko; David G. Rosado; Eduardo Fernandez-Medina; Eduardo B. Fernandez; "An Analysis of Security Issues for Cloud Computing," *Journal of Internet Services and Applications*, 27 February 2013, *www.jisajournal.com/content/4/1/5*

[3] El Segundo; "Cloud-related Spending by Businesses to Triple From 2011 to 2017," 14 February 2014, *http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017*

[4] National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2, USA, July 2013, *www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*

[5] Verizon,"Verizon Data Breach Report 2013," 2013, *https://ics-cert.us-cert.gov/sites/default/files/documents/data-breach-investigations-report-2013_en_xg.pdf*

[6] Sample, Char; "An Examination of PaaS Security Challenges," *TechTarget*, September 2012, *http://searchcloudsecurity.techtarget.com/*

[7] Menken, Ivanka; "Common SaaS Problems That Occur After Implementation," *TechTarget*, August 2009, *http://searchitchannel.techtarget.com/feature/Common-SaaS-problems-that-occur-after-implementation*