Issues and Standards in Cloud Security

Harit Mehta, harit.mehta (at) go.wustl.edu (A paper written under the guidance of Prof. Raj Jain) Download 

Abstract

Cloud computing has been one of the most important innovations in recent years providing cheap, virtual services that a few years ago demanded expensive, local hardware. Most business organizations are currently using cloud to handle multitudes of business operations. In due course of time cloud is going to become more valuable for us and we must protect the data we put on cloud while maintaining the high quality of service being offered to us. Fears over cloud security persist with hackers obtaining user information available online for notorious purposes. In the current scenario we tend to place a lot of data in the cloud, but what do we really know about its security? This paper discusses in detail various issues that arise in cloud security with respect to both customers and service providers. Various standards that define the aspects of cloud security related to safety of the data in the cloud and securely placing the data on the cloud are discussed. It further talks about a standard yet to be released and how it would impact once it is in the market.

Keywords : Cloud, Computing, Cloud Service Provider, Cloud Service Customer, Cloud Standards, Cloud Security, Security Threats, Information Technology Infrastructure Library (ITIL), Open Virtualization Format (OVF), ITU-T X.1601, PCI DSS, ISO/IEC 27017.

Table of contents

1. Introduction

Cloud computing has seen quite rapid and significant growth in the last few years. The term "Cloud computing" came into existence to define the change that occurs when applications and services are moved into the Internet "cloud". Cloud computing is a huge shift from the client server model to a model that provides faster and location independent service [Dialogic].

Many companies as of now have started delivering services from the cloud. Notable examples are:

- **Google** has a private cloud. It is used for delivering many different services to its users. These include email access, document applications, text translations, maps, and much more.
- **Microsoft** has "Sharepoint". It allows for content and business intelligence tools to be moved into the cloud. Microsoft currently also makes its office applications available in a cloud.
- **Salesforce.com** runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.

Some important features of cloud computing include *agility, device independence, location independence, reduced cost, reliability, scalability, resource sharing and security* [Michael10]. The primary function of a cloud however, is to provide service. These services fall into the following categories:

- **Infrastructure-as-a-Service (IaaS) :** It is possible for the users to now *buy infrastructure on the cloud*. The software product a user purchases is now something that the user owns in the cloud. You are now running a virtual server on a virtual disk instead of running a virtual server locally on your equipment. An example is Amazon Web Services [Michael10].
- **Platform-as-a-Service (PaaS) :** The service provider in this model provides a platform for use. The services provided therein include *all phases of the Software Development Life Cycle (SDLC)*. The model makes it feasible to use application program interfaces (APIs), website portals, or gateway software.

An example of such a model is PaaS in Google Apps [Michael10].

- **Software-as-a-Service (SaaS) :** This model provides *services to the end user*. It has the finished software, which is available for use by the end user. SaaS is designed to provide the application and the platform. The software service provided to the user is on a lease for a particular time period. The service can be provided to the end user through some type of front end or web portal. Salesforce.com is one of the examples that offer this type of service [Michael10].

Thus, in today's world cloud computing is gaining huge importance and is expected to have a huge impact on how things are designed and used in the Internet.

An important aspect of moving everything into the cloud is to keep everything safe and secure. It is important that everything we put on the cloud does not fall into malicious hands. In this paper we delve into the details of security aspects of cloud computing and the paper is divided into the following sections. Section 2 talks about the major threats and vulnerabilities the cloud faces. Section 3 of our paper discusses in detail the various Governance measures required to stem these issues. Section 4 talks about various industrial standards that have already been published covering security issues in cloud. In this section we also touch upon a new standard that will be published in 2015 for general use. Finally we present our conclusions from the discussion and the way ahead.

2. Major threats and vulnerabilities

In this section we first introduce the basic security considerations for the cloud security. Next we discuss the threats that are specific to cloud service providers (CSP) and cloud service customers (CSC).

2.1 Security considerations

There are several security issues and threats in the cloud and they can be categorized based on the security area that is under attack. Below, we discuss some of these in detail.

Privacy : Privacy is one of the more pressing issues, to the cloud and to the network security in general. It is one important aspect that must be of absolute assurance to the CSC. Privacy ensures that data, personal information and identity of a CSC must not be revealed to unauthorized users. How is the data stored within the cloud? Is it encrypted so that even the administrator can not see it without the decryption key? The encryption and decryption keys are usually present with the client and hence the CSP should not be able to look at data in the clear. Are there multiple copies of the keys? Are there multiple copies of the data that is stored? CSC has to take into account all these factors when choosing a CSP. Privacy has another threat - the insider threat. An CSP insider could easily access personal data of CSCs, if the encryption keys were available to the CSP, the stored data was not encrypted or if the data was stored in multiple locations. From the perspective of a CSP, the CSCs may be able to sue them if their privacy rights are violated. Here, private information is personally identifiable information, credit card details, religion, sexual orientation, health records etc. [Hocenski10, Shahed09, Wiki].

Confidentiality : Confidentiality is the second most important aspect of security. It is essential that CSPs maintain all data of a CSC confidential from other users, as it moves between the communication channels. There must be end-to-end encryption (secure encrypted channels), client and server authentication and no data leakage. A cross-VM side-channel attack could compromise the confidentiality of a system.

Integrity : Integrity means that no data should be modified when it is transferred from source to destination. Ensuring the integrity of the data (transfer, storage, and retrieval) really means that just the data is changed only in response to authorized transactions.

Data Protection : A cloud has vast storage space. It stores huge amount of data and information. It is therefore necessary for the CSPs to ensure that data privacy is maintained. Data isolation amongst users is important. Each CSC must have a separate address space and memory regions so that they do not access data or addresses that they should not be accessing. This isolation is usually ensured by assigning each CSC with a dedicated virtual machine [Hocenski10, Shahed09, Wiki].

Identity Management : An identity management system controls access to data and information. Organizations tend to have their own identity management system. Cloud systems could integrate the CSC's identity management system with what they have. Identity management is important in authentication, authorization and access control. CSCs assume that the service providers provide the "principle of least privilege" to their data. The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary [Hocenski10, Wiki].

Availability : Availability is an important part of any system. Availability is lost when there is a denial of service attack launched on a service. All services provided by the cloud must be available at all times. CSCs must have regular and predictable access to their data and applications [Shahed09, Wiki].

Application Security : With PaaS, CSCs can design their own applications on the platform in the cloud. These applications must be tested and verified by the CSP, before being made available for other users. In the absence of this, an attacker can create a malicious application, self-sign the application and put it up on the cloud for naive users to use them. Application security also involves an application firewall for monitoring inbound and outbound traffic to the cloud.

Compatibility : Storage services provided by one vendor may not be compatible with those provided by another vendor. It is important for CSPs to design platforms in such a way that the applications or software built over them is portable to be run on and be stored on other cloud infrastructures [Hocenski10, Shahed09, Wiki].

Data Retention : Ideally, there should be no data retention by the CSP after a legitimate request for destroying data comes from the CSC. However, if there are no multiple copies of data, then an attacker that has hijacked a session or gained privileged access, could request for the data to be destroyed and all data will be lost [Hocenski10, Wiki].

Data Security : Enterprises that use cloud services must be sure that their data is protected wherever it goes. Enterprise can also press for encrypting its data and allow only authorized people to access the data. For example, an enterprise may decide that its data should not be available outside its organization and may allow only specific officials access the data.

2.2 Threats for service providers

Based on the services that a CSP provides and the cloud environment, a CSP may face the following threats.

Wrongful use of administrative credentials : A CSP needs to give a cloud's administrative access to a CSC to some extent so that a CSC can manage its data on the cloud. This may enable an attacker to gain unauthorized access to cloud if an attacker can manage to pose as a valid CSC. This may allow an attacker to tamper with the cloud [X1601].

Inside threat : A CSP needs to be careful in providing administrative access to its employees. Carelessness of one such employee can lead to compromising of the CSP's administrative credentials and may allow an attacker to gain complete control of the cloud [X1601].

2.3 Threats for service customers

In this section we consider the threats that are faced by a CSC. Based on the CSC and type of service being used, the threats listed below may be responsible for violating a CSC's privacy or safety [X1601].

Data exposure : The data of various customers is stored in single cloud. Due to this sharing of storage resources if the data of a CSC is not sufficiently protected using proper cryptographic management then it may lead to exposure of a CSC's data to other CSCs who might not be authorized to access this data [X1601].

Access insecurity : Due to the distributed and shared nature of a cloud, accessing cloud services may also pose threats to the CSCs. The distributed nature of cloud service allows remote access of the service. If the remote connection is not secure then it may leave an open gate for an attacker to sniff for the CSC's credentials [X1601].

Above we have described the most important threats and issues that arise in the field of cloud computing and how they may cause problems to a CSP or a CSC. Apart from these, threats can also arise due to indirect denial of service, attacks such as cross-VM side-channel attack and malware infection [Shacham09].

In order to avoid the above issues and reduce them to a minimum we need certain safety measure and guidelines, which are described in the section below.

3. Governance, Regulation and Compliance Concerns

There exists a "trust but verify" relationship between CSPs and CSCs [IBM09]. Even if the workload has been moved to the cloud, the onus of compliance and protection has to be borne by the CSCs. In the following section, we enlist a few concerns related to security governance, regulation and compliance (GRC). Different models of cloud computing leads to variation in the amount of responsibility taken by the CSP and by the CSC. SaaS makes the CSP take maximum responsibility of security management. PaaS allows CSCs to assume more responsibility of the software applications and the middleware. Thus, security management is largely a job of the subscriber. IaaS makes the subscriber solely responsible for security of almost all the entities except physical security of the hardware, the infrastructure itself.

3.1 Visibility and Compliance

The clouds, as of today, are by definition "black box". Visibility is very important for CSCs to ensure compliance. It is also required for third-party audits and procedures like Electronic Discovery (eDiscovery).

The laws, regulations and standards have to be met. Who is responsible for ensuring this: the CSP or the CSC? More often than not, the resources span multiple jurisdictions, which make the issue of compliance complicated.

3.2 Storage, Retention and Destruction

The exact location of the CSC's data in the cloud is not known to the CSC. The storage can be distributed over a wide geographical range. This raises confidentiality concerns as the regulating Privacy Laws are different in different regions and some of these might me unacceptable or harmful to CSCs.

The period for which the data should exist in the cloud is decided by CSC. If a CSP does not ensures the destruction of data beyond the retention period, it may result in exposure of private and confidential data.

There is no way of ensuring that the CSP deletes all copies of CSC data when the CSC intends to do so. The only thing the CSC can do is trust the CSP.

3.3 Audit, Monitoring and Data Portability

The process of logging and auditing is largely dependent on the CSP. Especially in a SaaS or PaaS model, a majority of the system level logging and auditing is under the control of the CSP.

When a CSC chooses to move its workload from one CSP to another, it may have to go through a tedious process of ensuring compatibility and compliance again so as to match with the infrastructure, services and terms and conditions of the new CSP.

3.4 Privacy Breaches and Law Violation

Even after putting all the security measures in place, a breach of privacy is still possible. The CSC needs to know about such a breach when it occurs. It has to rely on the CSP to alert the CSC in time.

When data privacy issues are governed by foreign laws, violation of a law by CSP or CSC may cause major risk due to exposure of private data.

3.5 Government or Organizational Regulations

Some governments or enterprises may need to enforce strict limits on the spatial and temporal existence of data. For example, a government might want to keep the data of its citizens within the country and for an exact duration.

In this section we discussed what regulations and reforms are necessary on both the CSC end and CSP end to maintain confidentiality of information being put on the cloud. The next section talks about certain standards, which discuss best practices, standards, challenges and try to address the above issues in the best possible manner.

4. Cloud Security Standards

The various security threats to the cloud made it imperative to issue standards on how work is done on the cloud. The five standards described below discuss in detail the breadth of issues they cover with regard to cloud security. They provide a comprehensive structure on how security in the cloud is maintained with respect to both the user and the service provider. The fifth standard presented in this paper is to be released in 2015 and touches other finer aspects of cloud security.

4.1 Information Technology Infrastructure Library (ITIL)

It is a set of best practices and guidelines that define an integrated, process-based approach for managing information technology services. ITIL helps make sure that proper security measures are taken at all important levels, namely strategic, tactical, and operational level.

Many IT organizations employ security management framework- Information Technology Infrastructure Library (ITIL) [Marquis12]. This industry standard management framework provides guidance for planning and implementing a governance program with sustaining management processes that protect information assets and thus provide security. ITIL gives a comprehensive explanation pertaining to major IT practices with detailed checklists, tasks, and procedures that can be modified and adopted to any IT organization. One important aspect of ITIL, pertaining to cloud computing, is continuously changing organizations and information systems [Fry]. Hence, it provides a framework with continuous improvement that is necessary to align and realign IT services to changing business needs. Cloud computing services have dynamic characteristics. Hence, the security practices must be continually revised to keep it updated and efficient. Cloud security management is a continuously evolving process. Figure 1 shows the ITIL life cycle in an IT organization as described above.

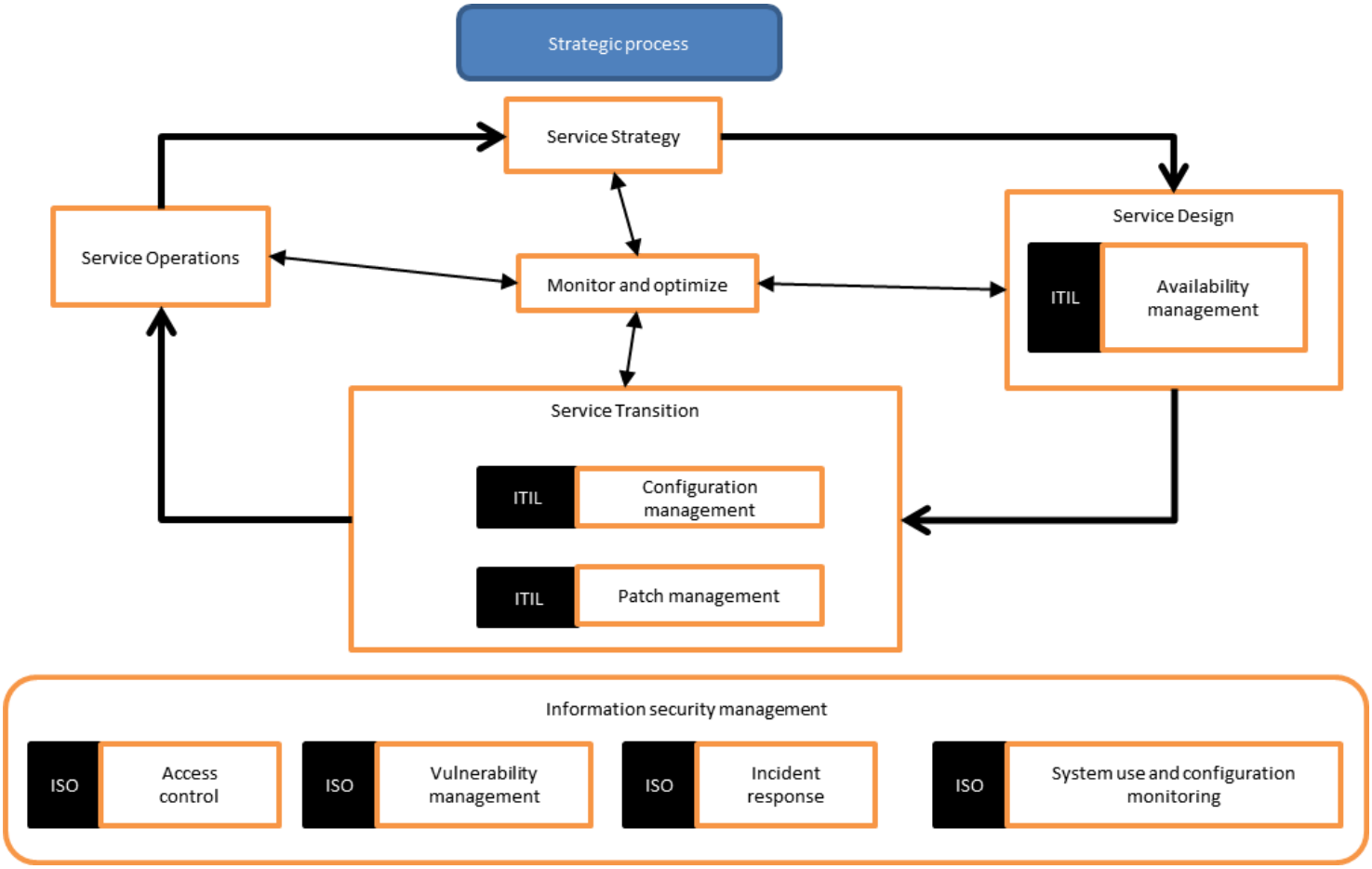

Figure 1: ITIL life cycle in an organization

Ref - [Shahed09]

ITIL Security Management framework in the cloud has two major goals: [Shahed09]:

Realization of security requirements:"Security requirements are usually defined in the SLA as well as in other external requirements, which are specified in underpinning contracts, legislation, and internally or externally imposed policies".

Realization of a basic level of security:"This is necessary to guarantee the security and continuity of the organization and to reach simplified service-level management for information security management".

Information security practices are divided into four different levels. [Shahed09]:

1. **Policies:**The major objective an organization is trying to achieve.
2. **Processes:**What steps to follow to achieve those objectives?
3. **Procedures:**Distribution of activities amongst people and setting up deadlines.
4. **Work instructions:**Specifying guidelines to perform certain activities.

The major challenge for organizations that fail to adopt ITIL efficiently is that they might have to re-define or re-implement the entire set of ITIL processes that they have. Thus, for implementing ITIL a detailed analysis of existing processes along with gaps in relation to the ITIL framework and level of process integration would be needed.

4.2 Open Virtualization Format (OVF)

Open Virtualization Format (OVF) is a standard pertaining to portability concern described in section 3.3. OVF provides the ability for an efficient, flexible and secure distribution of enterprise software over the cloud. OVF thus provides customers: vendor and platform independence as it facilitates mobility of virtual machines [OVF2]. Across the cloud OVF plays a major role in providing cross-platform portability. It also helps provide simplified deployment over multiple platforms. OVF 2.0 was released in January 2013 [OVF2].

An OVF format virtual machine can be deployed easily by customers. They can do so on the platform of their choice. It helps enhance customer experience as it provides customers with portability, platform independence, verification, signing, versioning, and licensing terms [OVF2].

The key features and benefits of the format are:

- Portable VM packaging
- Optimization for secure distribution
- Simplified Installation and Deployment
- Supports both VM and multi-VM configurations
- Vendor and platform independent
- Extensible
- Localizable

Advantages of using OVF:OVF 2.0 brings a lot on the table for the packaging of virtual machines, making the standard applicable to a broader range of cloud use cases that are emerging as the industry enters the cloud era. OVF 2.0 has a huge impact mainly attributed to its ability to include support for network configuration. In parallel it also provides the ability to encrypt package to ensure its safe delivery.

For DMTF's cloud standard development, OVF plays an important role. It provides expertise specifically for Cloud Infrastructure Management Interface (CIMI) specification. Advancements in the OVF specification are handled by DMTF's System Virtualization, Partitioning, and Clustering Working Group (SVPC WG). The working group performs a few critical tasks. It helps create standards for management of virtualized environments, managing life cycle of a virtual computer system, discovering inventory virtual computer systems and monitoring virtual systems for health and performance. Thus the SVPC WG has major contributions to DMTF's overall Cloud Management Initiative [OVF2].

4.3 ITU-T X.1601

The ITU standard presents a sketch of issues pertaining to cloud computing and proposes a framework for cloud security. It talks in detail about various security challenges and ways to reduce these security risks in cloud computing. It also discusses a framework that provides an insight into what security capabilities are required for making the cloud secure and facing security challenges. ITU-T X.1601 starts by listing down major security threats that the cloud can encounter. As we have already discussed major security threats for cloud computing in section 2, in this section we will discuss the cloud security challenges and the security capabilities that this standard deals with and those help in mitigating the relevant threats [X1601].

The standard discusses the security challenges based on the nature of the role that an individual or an organization plays in the cloud computing paradigm. The standard divides the roles of an individual or an organization into following three categories [X1601]:

1. **Cloud Service Provider (CSP):** An individual or an organization responsible for making cloud services available.
2. **Cloud Service Customer (CSC):** An individual or an organization that uses cloud services.
3. **Cloud Service Partner (CSN):** A partner that helps support the CSPs or the CSCs.

Security Challenges

Cloud security challenges are defined as those faced due to the operating environment and nature of the cloud service. This also includes the threats that affect more than one participant of the cloud service. The challenges are classified based on whether the participant is CSP or CSC [X1601].

1. Security challenges for Cloud Service Customers: This clause describes the challenges that affect the CSCs directly.
    - Ambiguity in responsibility: A CSC uses services based on different service categories as well as different deployment models. If the responsibilities are

not clearly defined in any of these cases then it may result in inconsistency or may leave an open gate for attacks. The ambiguity as to whether a CSP or a CSC should adhere to a given responsibility varies with change in jurisdictions and can be vague at international level.
    - Loss of trust: Because of the abstraction of the security implementation details between a CSC and a CSP, it is difficult for a CSC to get details of the security mechanisms that the CSP has implemented to keep the cloud data secure. This makes it a risk for the CSC to trust the CSP with its data and keeps the CSC at a high security threat in using the cloud services.
    - Loss of governance: When the CSC uses cloud services, it has to move its data onto the cloud and has to provide certain privileges to the CSP for handling the data in the cloud. This may result in misconfiguration or an attack due to the abstraction of the CSP's cloud practices and due to the privileges that need to be given to the CSP.
    - Loss of privacy: CSC's privacy may be violated due to leakage of private information while the CSP is processing CSC's private data or using the private information for a purpose that the CSP and CSC haven't agreed upon.
    - Cloud service provider lock-in: This issue arises if a CSP doesn't abide by the standard functions or frameworks of cloud computing and hence makes it difficult for a CSC using its services to migrate to any other CSP. The use of non-standard functions and cloud framework makes the CSP non-inter-operable with other CSPs and also leaves CSC open to security attacks.
    - Misappropriation of intellectual property: A CSC may face this challenge due to the possibility that a CSC's data on the cloud might leak to third parties that are using the same CSP for their cloud services. This leakage may violate the CSC's copyrights and may result in the disclosure of CSC's private data.
    - Loss of software integrity: A CSC encounters this challenge due to the fact that its software is running in the cloud once it is given to the CSP. It is possible that this software might be tampered with or might be affected while the software is running in the CSP and is not in CSC's control, resulting in CSC's loss over its software.
2. Security challenges for cloud service providers: This clause describes the challenges that affect the CSPs.
    - Ambiguity in responsibility: The ambiguity in responsibility may result when a CSP is working over various jurisdictions. This is because each contract may be in different frameworks. The challenges arise in addressing issues such as data ownership and access control.
    - Shared environment: The idea of cloud services is sharing of resources on a very large scale. This feature makes the CSPs vulnerable to many security issues. For instance, a cloud service provided by a CSP will be shared by many CSCs. This may result in a CSC having an unauthorized access to other's virtual resources in the cloud and may violate the privacy of the other cloud users.
    - Inconsistency and conflict of protection mechanisms: An attacker might be able to exploit the decentralized architecture of the cloud because of the discordant security systems among various distributed systems. This might result in the violation of a CSC's confidentiality and integrity.
    - Jurisdictional conflict: If a CSP's services are spread across various data centers and across various countries, then different jurisdictions will be applicable to the cloud data. This may result in jurisdictional conflict.
    - Evolutionary risks: Evolutionary risks arise when some system choices' implementation is delegated to the execution phase of the system rather than the design phase. This may result in some vulnerabilities in the system after or during the execution phase even if the system passed the security checks during its design phase.
    - Bad migration and integration: For migrating a system to a CSP, a large amount of data has to be moved to the cloud. If the configuration of this data and the configuration of the cloud is not matched properly then there may be open gates for an attacker and would make the cloud vulnerable.
    - Software dependencies: When a CSP's system consists of components provided by various CSNs, it won't be able to make changes immediately upon detection of a vulnerability because this change may affect multiple components and as the components are from different CSNs some of them might not be compatible to this changes.

Security capabilities

The standard suggests the following cloud computing security capabilities to mitigate the security threats discussed in section 2 and the security challenges discussed above [X1601].

1. Trust model: Due to the distributed and large scale resource sharing nature of cloud computing there must be a general trust model. This model will enable proper authentication and authorization among different entities and components of the system.
2. Physical security: This capability requires that access to the CSP premise should be granted only to authorized personnel and only to those locations that are necessary for the job function.
3. Interface security: This capability refers to securing the interfaces that are responsible for providing cloud services to various CSCs. Some of the currently used mechanisms are mutual authentication, digital signatures, encryption and integrity checksum.
4. Network security: Network security in cloud computing includes both physical as well as virtual network security through isolation and confidentiality between all involved parties. It provides security domain partition, border access control, intrusion detection and prevention [X1601].
5. Data isolation, protection and privacy protection:
    - Data isolation: It refers to preventing access and visibility of one party's data to another party in the shared environment. A participant is not allowed to access data of another party unless authorized to do so. Data isolation may be provided physical or virtually.
    - Data protection: Data protection ensures that data of a participant is sufficiently protected and no one except authorized people are allowed to temper with it. Access control list, integrity verification and encryption are some of the mechanisms used for providing data protection.
    - Privacy protection: It refers to protecting private data of the user and all the processing that is done on this private data. This process includes collection, handling, storing and deletion of private data.
6. Security coordination: Due to different computing services in a cloud environment there are different security controls provided by each cloud service. This capability is responsible for coordinating all the different security controls among different cloud services.
7. Interoperability, portability and reversibility: Interoperability refers to enabling various cloud components to synchronize their jobs in the cloud. Portability provides a CSC the freedom of migrating from one CSP to another CSP and reversibility refers to the ability of a CSC to remove its data from cloud back to its non-cloud storage.

The standard also talks about various other capabilities such as Identity and Access Management (IAM), authentication, authorization and transaction audit, computing virtualization security, operational security, incident management, disaster recovery, service security assessment and audit and supply chain security.

4.4 PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) was released by PCI security standards council. PCI's main objective is to provide security guidelines for credit card usage and address CSP's and CSC's. Cloud security is a shared responsibility between the CSP and its clients. "For example, if payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the client's usage of that environment".

Though the responsibility for managing security is shared between client and provider the client still has an important role to play. The client holds the responsibility of ensuring their cardholder data is secure under PCI DSS requirements. The division of responsibilities between the client and the CSP for managing PCI DSS controls is influenced by multiple factors, which are [PCI13]:

- The client uses the cloud service for what purpose.
- What scope of PCI DSS requirements is the client outsourcing to the CSP.
- The CSP validates which service and system components within its own operations.
- The service option that the client has selected to engage the CSP (IaaS, PaaS or SaaS).
- The scope of any additional services the CSP is providing to pro-actively manage the client's compliance (for example, additional managed security services).

The client must have a clear understanding of the scope of responsibility that the CSP is accepting for each PCI DSS requirement.

Security as a Service, or SecaaS, forms an integral part of the security of the cloud. SecaaS solutions may not be directly involved in storing, processing, or transmitting[PCI13]. Let us consider an example of a SecaaS-based anti-malware solution. This anti-malware, using a cloud delivery model updates the anti-malware signature at client's system. SecaaS plays the role in such a manner that it offers a PCI DSS control to the client's environment. In the process the SecaaS functionality is not necessarily reviewed to verify that it meets the applicable requirements.

Scoping Considerations: Organizations looking to store, process, or transmit payment card data in a cloud environment should clearly understand the impact that the cloud will have on their PCI DSS scope [PCI13]. "For example, in a private-cloud deployment, an organization could either implement adequate segmentation to isolate in-scope systems from other systems and services, or they could consider their private cloud to be wholly in scope for PCI DSS. In a public cloud, the client organization and CSP will need to work closely together to define and verify scope boundaries, as both parties will have systems and services in scope."

Special recommendations simplifying PCI DSS scope in a cloud include:

1. Not to store, process or transmit payment card data in the cloud.
2. Implement a dedicated physical infrastructure that is used only for the in-scope cloud environment.
3. Minimize reliance on third-party CSPs for protecting payment card data. The more security controls the CSP is responsible for, the greater the scope of the CDE will potentially be, thereby increasing the complexity involved in defining and maintaining CDE boundaries.

One important factor while implementing security control is that special technical know how is important for the cloud environment.[PCI13]. An important consideration therefore is that before migrating payment card operation system to a cloud, the client evaluates clients needs. It makes use of its organization team in doing so before deciding how much of the requirements set by the client are feasible and acts accordingly.

4.5 ISO/IEC 27017 Code of practice for information security controls

This standard is yet to be launched in the market. It aims to provide further guidance in the information security domain of cloud computing. It is aimed at supplementing the guidance in ISO/IEC 27002 and various other ISO27k standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards [ISO27017].

The scope and purpose is listed below:

- It aims to provide an advancement to ISO/IEC 27002 in terms of adding value to its practices of control implementation
- Additionally the standard will provide further security advice for both: clients and service providers. It will do that by offering advice for both side-by-side in each section.

For example, the draft of section 6.1.1 on information security roles and responsibilities says, in part:-

"Cloud Service Customer: The cloud service customer should review the proposed demarcation of information security responsibilities and confirm it can accept its responsibilities" [ISO27001].

"Cloud Service provider: The cloud service provider should define and document the demarcation of responsibilities of cloud service customer, cloud service supplier and its suppliers" [ISO27001].

Status of the standard: Publication is extremely unlikely before 2015.

The standards above describe in detail the considerations to make cloud computing safer for the end user and provide an experience where there is no loss of data or identity. The issues in cloud security that arise after the first four standards were issued are touched upon in the fifth standard, which is yet to be released. When published, a more comprehensive detailed document for the fifth standard will help us gain deeper insight to what value that standard adds for us in terms of cloud security.

5. Conclusion

Cloud computing is the next big step forward in the field of networking. The features of cloud computing such as speed, portability, performance improvement and utilization of shared resources have allowed the use of cloud computing to spread rapidly. The features that make cloud-computing stand apart from other non-cloud techniques also make it susceptible to many attacks and it has to deal with many security issues.

In this paper we first discussed in detail security threats and issues that are critical for a cloud. We then shed light on governance and compliance concerns related to cloud security. We extended the discussion to five important standards to enhance cloud security. We started our discussion with ITIL, which describes best practices and guidelines that define an integrated, process-based approach for managing information technology services. We then talked about Open Virtualization Format 2.0, which provides guidelines for distributing a software over the cloud. The ITU-T X.1601 standard gives a detailed insight into different services provided by the cloud, the main threats that a cloud environment faces, the challenges in providing or using cloud services, the security capabilities that help in mitigating these threats and challenges. The next standard PCI DSS focuses on authenticating the CSP and CSC for secure data handling on both sides. We further lay emphasis on ISO/IEC 27017, a standard that is currently being drafted that brings out other finer aspects of cloud security.

6. References

1. [Michael10] Michael Gregg, "10 Security Concerns for Cloud Computing", 2010, http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf
2. [Hocenski10] Z. Hocenski K. Popovic, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, 24-28 May 2010, Pages 344 - 349, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5533317&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5533317
3. [Shahed09] Shahed Latif, Subra Kumaraswamy, Tim Mather, "Cloud Security and Privacy", O'Reilly Media, Inc., Sept. 28, 2009, ISBN: 9780596802769 (Safari books), https://www.safaribooksonline.com/library/view/cloud-security-and/9780596806453/
4. [Wiki] Wikipedia. Cloud computing security, http://en.wikipedia.org/wiki/Cloud_computing_security
5. [Shacham09] H. Shacham; S. Savage; T. Ristenpart; E. Tromer. "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds", 2009, http://www.tau.ac.il/~tromer/papers/cloudsec.pdf
6. [IBM09] IBM, IBM point of view: Security and cloud computing, White Paper by IBM, 2009, http://www.ibm.com/ibm/files/K741953W02854Z25/18Security_and_Cloud_Computing_382KB.pdf
7. [Marquis12] Hank Marquis, "How ITIL helps cloud computing", 2012 http://www.globalknowledge.ae/content/files/documents/Decision_Brief_Cloud_and_ITIL.pdf
8. [Fry] Malcolm Fry, "Cloud computing and self-service; Are they the way ahead?", http://hdioc.org/storage/Cloud%20Computing%20and%20Self-Service.pdf
9. [OVF2] OVF 2.0, OVF 2.0 FAQ, http://dmtf.org/about/faq/ovf_faq
10. [X1601] ITU, X.1601 : Security framework for cloud computing, http://www.itu.int/rec/T-REC-X.1601-201401-I/en
11. [ISO27017] ISO, ISO/IEC 27017 Cloud security, http://www.iso27001security.com/html/27017.html
12. [ISO27001] ISO, ISO/IEC 27001 Certification Standard, http://www.iso27001security.com/html/27001.html
13. [PCI13] Cloud Special Interest Group; PCI Security Standards Council, "PCI Data Security Standard (PCI DSS) Version 2.0", February 2013, https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
14. [Dialogic] Dialogic White Paper, Introduction to Cloud Computing, http://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf

7. Acronyms

- CSP - Cloud Service Provider
- CSC - Cloud Service Customer
- CSN - Cloud Service Partner
- Iaas - Infrastructure-as-a-Service
- PaaS - Platform-as-a-Service
- SaaS - Software-as-a-Service
- ITIL - Information Technology Infrastructure Library
- SLA - Service-level agreement
- OVF - Open Virtualization Format
- VM - Virtual Machine
- DMTF - Distributed Management Task Force
- CIMI - Cloud Infrastructure Management Interface
- SVPC WG - System Virtualization, Partitioning, and Clustering Working Group
- ITU - International Telecommunication Union
- IAM - Identity and Access Management
- CDE - Cardholder Data Environment
- ISO - International Organization for Standardization
- IEC - International Electrotechnical Commission
- SecaaS - Security as a Service
- CD - Committee Draft
- PCI DSS - Payment Card Industry Data Security Standard

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page