Security issues associated with the cloud[edit]

Cloud computing and storage provide users with capabilities to store and process their data in third-party data centers.[1] Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community).[2] Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).[3] The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a 2010 Cloud Security Alliance report, insider attacks are one of the top seven biggest threats in cloud computing.[4] Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.[2]

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service.[5] Virtualization alters the relationship between the OS and underlying hardware – be it computing, storage or even networking. This introduces an additional layer – virtualization – that itself must be properly configured, managed and secured.[6] Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist.[7] For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Cloud security controls[edit]

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.[8] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[8]

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[8] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

Dimensions of cloud security[edit]

It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. Cloud security concerns can be grouped in various ways; Gartner named seven[9] while the Cloud Security Alliance identified twelve areas of concern.[10] Cloud access security brokers (CASBs) are software that sits between cloud users and cloud applications to provide visibility into cloud application usage, data protection and governance to monitor all activity and enforce security policies.[11]

Security and privacy[edit]

Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system,[1] or provide an identity management system of their own.[12] CloudID,[1] for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.[1]

Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Cloud Vulnerability and Penetration Testing[edit]

Scanning the cloud from outside and inside using free or commercial products is crucial because without a hardened environment your service is considered a soft target. Virtual servers should be hardened just like a physical server against data leakage, malware, and exploited vulnerabilities. "Data loss or leakage represents 24.6% and cloud related malware 3.4% of threats causing cloud outages”[13]

Scanning and penetration testing from inside or outside the cloud must be authorized by the cloud provider. Since the cloud is a shared environment with other customers or tenants, following penetration testing rules of engagement step-by-step is a mandatory requirement. Violation of acceptable use policies can lead to termination of the service.[*citation needed*]

Data security[edit]

A number of security threats are associated with cloud data services: not only traditional security threats, such as network eavesdropping, illegal invasion, and denial of service attacks, but also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud services. The following security requirements limit the threats.[14]

Confidentiality[edit]

Data confidentiality is the property that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information of the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and data sharing, without the leakage of the data contents to CSPs or other adversaries.

Access controllability[edit]

Access controllability means that a data owner can perform the selective restriction of access to their data outsourced to the cloud. Legal users can be authorized by the owner to access the data, while others can not access it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

Integrity[edit]

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

Encryption[edit]

Some advanced encryption algorithms which have been applied into cloud computing increase the protection of privacy. In a practice called crypto-shredding, the keys can simply be deleted when there is no more use of the data.

Attribute-based encryption (ABE)[edit]

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

Ciphertext-policy ABE (CP-ABE)[edit]

In the CP-ABE, the encryptor controls access strategy. The main research work of CP-ABE is focused on the design of the access structure.[15]

Key-policy ABE (KP-ABE)[edit]

In the KP-ABE, attribute sets are used to describe the encrypted texts and the private keys are associated to specified policy that users will have.[16][17][18]

Fully homomorphic encryption (FHE)[edit]

Fully homomorphic encryption allows computations on encrypted data, and also allows computing sum and product for the encrypted data without decryption.[19]

Searchable encryption (SE)[edit]

Searchable encryption is a cryptographic system which offer secure search functions over encrypted data.[20][21] SE schemes can be classified into two categories: SE based on secret-key (or symmetric-key) cryptography, and SE based on public-key cryptography. In order to improve search efficiency, symmetric-key SE generally builds keyword indexes to answer user queries. This has the obvious disadvantage of providing multimodal access routes for unauthorized data retrieval, bypassing the encryption algorithm by subjecting the framework to alternative parameters within the shared cloud environment.[22]

Compliance[edit]

Numerous laws and regulations pertain to the storage and use of data. In the US these include privacy or data protection laws, Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Federal Information Security Management Act of 2002 (FISMA), and Children's Online Privacy Protection Act of 1998, among others. Similar standards exist in other jurisdictions, eg Singapore's Multi-Tier Cloud Security Standard.

Similar laws may apply in different legal jurisdictions and may differ quite markedly from those enforced in the US. Cloud service users may often need to be aware of the legal and regulatory differences between the jurisdictions. For example, data stored by a cloud service provider may be located in, say, Singapore and mirrored in the US.[23]

Many of these regulations mandate particular controls (such as strong access controls and audit trails) and require regular reporting. Cloud customers must ensure that their cloud providers adequately fulfill such requirements as appropriate, enabling them to comply with their obligations since, to a large extent, they remain accountable.

Business continuity and data recovery

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered.[24] These plans may be shared with and reviewed by their customers, ideally dovetailing with the customers' own continuity arrangements. Joint continuity exercises may be appropriate, simulating a major Internet or electricity supply failure for instance.

Log and audit trail

In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., eDiscovery).

Unique compliance requirements

In addition to the requirements to which customers are subject, the data centers used by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.[25]

The European Union’s GDPR regulation has introduced new compliance requirements for customer data.

Legal and contractual issues[edit]

Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), intellectual property, and end-of-service (when data and applications are ultimately returned to the customer). In addition, there are considerations for acquiring data from the cloud that may be involved in litigation.[26] These issues are discussed in service-level agreements (SLA).

Public records[edit]

Legal issues may also include records-keeping requirements in the public sector, where many agencies are required by law to retain and make available electronic records in a specific fashion. This may be determined by legislation, or law may require agencies to conform to the rules and practices set by a records-keeping agency. Public agencies using cloud computing and storage must take these concerns into account.