SECURITY RISKS IN CLOUD COMPUTING

Modern definitions of cloud computing state that cloud computing is an on-demand service model for IT provision that is based on virtualization and distributed computing technologies. Cloud computing technologies have certain standout features including highly abstracted resources that are nearly instantly scalable and flexible with instantaneous provisioning. Architectures typically share resources such as hardware, database, memory and software. They are run on programmatic management.

Cloud computing can definitively be categorized in 2 ways. One of them is based on the functionality of service provided. Under this sub category, cloud computing services are as follows:

1. Software as a service: Software offered by a third party provider via internet which is generally remotely maintainable and configurable.
2. Platform as a service: Allows customer to host develop new applications using APIs which can be deployed and reconfigured remotely.
3. Infrastructure as a service: Provides virtual machine support and abstracted hardware support for customers to develop their own operating systems and service APIs

Under the second sub category cloud computing services are based on the customer base they cater to:

1. Public: Any public organizations may subscribe to this service
2. Private: Services only acceptable within a private network.
3. Partner: Services offered by one provider to multiple interested parties

There are several advantages of using cloud computing. Data storage capability is only limited to how much one can afford to pay for it. Maintenance and backups are paid for by the customer and taken care of by professionals. Cloud computing security is however a multi-faceted concern. There are several easily variable factors that need to be optimally balanced to provide good security to cloud based data centric services. Data being accessible to cloud computing center employees is a major concern. Also, customers often don't take into account the question of what happens to their data once they choose to disassociate themselves from their cloud service provider. There is no guarantee of the data being deleted or overwritten if data is no longer required. It is practical to consider worst case scenarios where third parties might be able to access confidential data stored within the cloud. It may be susceptible to manipulation, interception or corruption. Level of risk always varies with the type of architecture deployed.

Cloud related risk factors in themselves have been classified in certain ways:

1. Policy and Organizational Risks: Risks related to administrative and policy decisions and compliance rules.
2. Technical Risks: Resource exhaustion. Data leakage, links breaking etc are the type of risks that need better timely technical maintenance.
3. Legal Risks: Disclosure of data that was intended to be private and confidential has serious legal consequences.

EXPLORING TECHNICAL RISKS: DATA LEAKAGE ON DOWNLOAD/UPLOAD/INTRA-CLOUD

Data leakage means loss of data either by accident due to physical and technical malfunctions or deliberately created leakage during the transfers between the customer and cloud service provider. Data leakage compromises the confidentiality as well as validity of data. Corrupted data renders the rest of the connected data useless. There are several reasons for a data leakage to occur:

1. Cloud computing architectures have continuous streams of data in transit. This makes data more vulnerable to accidental or deliberate losses.

2. Multi-platform storage may allow for data to be distributed across vast physical regions. Transfer of data between these cloud centers is also prone to the risk of leakage of data.

3. Most of this data is encrypted which makes the loss of data even more plausible.

4. Some cloud services do not have a secure VPN connection built in for their transfers which makes it easier for data leakage to occur. Publicly prevalent cloud services are most prone to the lack of a VPN.

5. Deliberate attacks on data target transmit times to intercept crucial information or render data useless.

The repercussions of this kind of an occurrence are multifold. Attacks on assets can be widespread and with varying degrees of damage to both parties involved. Some of them can be listed as:

1. Company Reputation: Slightest amounts of irregularity in the data being stored or transmitted can have a damaging on the reputation of any company that claims to keep data safe.

2. Customer Trust: Negative publicity can affect customers deeply.

3. Employee Loyalty and Experience: Any data leakage or corruption directly puts the employees of a company under scrutiny. This may discourage employees from staying with the company and make them question their loyalties.

4. Intellectual Property: One of the most sensitive categories of data stored in a cloud is IP. There are several legal, moral and financial liabilities associated with storing and protecting IP. Data leakage associated with IPs is severely harmful to both the cloud service provider and the customer.

5. Personal Data: Individual Users may store personal information such as photos, bank related documents, educational documents etc. Leakage of this type of information is compromises the identity and credentials associated with the individual, making him/her vulnerable to a variety of crimes.

6. Personal-Critical data and Sensitive Data: Per the definition from EUs data protection directive, personal information entered onto any online or cloud service is still under the supervision and protection of the individual. Violation of this right occurring through attacks on cloud center services reflects extremely poorly on the service provider and their security measures. Sensitive data is generally related to financial data

7. HR Data: Data related to operational perspective is classified as HR data. Any changes in this data directly affects the functioning of dependent systems.

8. Credentials: Credentials of the people handling data flow in and out of the cloud based system are also taken into considering while assessing assets affected by data leaks.

9. User Directory: User directory is the definitive list along with credentials of everyone who is allowed to access the cloud services. Any leaks in this directory will lead to the respective persons being completely locked out of the system.

10. Cloud Service Management Interface: Management interface that oversees all processes and functionalities supported by the cloud service. Changes made to the CSMI will directly affect services provided by the cloud.

Protecting against data leaks involves effectively protecting all vulnerabilities from anticipated technical failures and deliberate attacks on the system. Some of these vulnerabilities are stated as below:

1. AAA – Authentication, authorization and Accounting: Poor procedure for authentication and authorizing users to their accounts s one of the most common vulnerabilities that can be exploited through basic rules of hacking the user database within the cloud management system. Credentials stored on transitory machines are easy to manipulate. There should be a multilayer approach with increasing levels of complexity to ensure effective security.

2. Communication Encryption Vulnerabilities: These vulnerabilities concern how useful data intercepted in transit can be to a fraudster or hacker. MITM attacks, poor authentication etc can be the causes that this vulnerability can be exploited easily.

3. Possibility that internal network probing will occur: Cloud customers have power to perform port scans and tests on other customers within the internal network. This gives wrong-intentioned people with enough resources to get an account on the same cloud services, much easier leeway into other accounts.

4. Possibility that co-residence checks will be performed: Side channel attacks exploiting the lack of resource isolation allow attackers to determine which cloud centers are shared by which set of customers. This helps them conduct targeted attacks.

5. Impossibility of processing data in encrypted form: Data at rest can be encrypted with sufficient security applied. But processing data with encryption is still underdeveloped. Hence it is easier to exploit data mid-process and mid-transit. AT this point in time the system is at its most vulnerable. The tradeoff for encrypted processing is time which essentially translates to money.

6. Application vulnerabilities or poor patch management: Applications cannot be programmed and hosted perfectly from the word go. Throughout the process of using the application different security vulnerabilities will be exposed. These are generally corrected with patches. Poor patch management simplifies the process of exploitation of these vulnerabilities.

Considering all these risk factors, a well-implemented security system is beneficial to the customer as well as the cloud service providers. The scale of cloud implemented services makes security implementation cheap. Multiple location storage increases redundancy facilitating secure storage and hosting. Quick and timely responses play a big part in mitigating most threats at their root. Providing disk images to customers and/or analysis of attack data can help diagnose security leaks and weak points within a systems protection.