Data Security in Cloud

R. Boopathi,
Student, department of Information technology
Kumaraguru College of technology
Coimbatore, India.

B. Gopinathan,
Student, department of Information technology
Kumaraguru College of technology
Coimbatore, India.

***Abstract* - Cloud based computing services is among the fastest growing sections of the IT industry due to features such as attractive cost savings for buyers, accessibility & reliability options for users and scalable sales for providers, especially as recession-hit institutions are increasingly cost conscious.An overview of current and upcoming cloud computing threats and cyber security risks such as hacks, cracks and carelessness.And then concludes with a review of building cloud security awareness and minimizing the risks associated with cloud computing.**

I.INTRODUCTION

A. *Cloud Computing*

Cloud based computing services is among the fastest growing sections of the IT industry due to features such as attractive cost savings for buyers, accessibility & reliability options for users and scalable sales for providers, especially as recession-hit institutions are increasingly cost conscious.

B.*Types*

There are four types of cloud computing. They are

- *Public cloud*

It is, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

- *Private cloud.*

The private cloud is a data center that supplies services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud.

- *Community cloud*

The community cloud may be established where several organizations have similar requirements and
seek to share infrastructure. This option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov. Cloud".

- *Hybrid cloud*

The term "Hybrid Cloud" has been used to mean either two separate clouds joined together (public, private) to provide a single common service. Two clouds that have been joined together are more correctly called a "combined cloud".

C. Service model architecture

- *Infrastructure-as-a-Service (IAAS)*

Like Amazon Web Services provides servers with unique IP addresses and blocks of storage.Customers use the provider's application program to start, stop, access and configure their virtual servers and storage.

- *Platform-as-a-service (PAAS)*

It is as a set of software and product development tools hosted on the provider's infrastructure.Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud.

- *Software-as-a-service (SAAS)*

The vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. Because the service provider hosts both the application and the data, the end user is free to use the service from anywhere.

II. CURRENT THREADS IN CLOUD COMPUTING SECUIRTY

2.1. Data breaches

It describing how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other client’s data as well.

You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data. However, if you opt to keep offline backups of your data to reduce data loss, you increase your exposure to data breaches.

2.2. Prospect of seeing your valuable data disappear into the ether without a trace

A malicious hacker might delete a target's data out of spite but then, you could lose your data to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting your data to ward off theft can backfire if you lose your encryption key.Data loss isn't only problematic in terms of impacting relationships with customers, the report notes. You could also get into hot water with the feds if you're legally required to store particular data to remain in compliance with certain laws, such as HIPAA.

2.3. Account or service traffic hijacking

If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. "Your account or services instances may become a new base for the attacker".The key to defending against this threat is to protect credentials from being stolen.

2.4. *Insecure interfaces and APIs*

IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services.From there, organizations and third parties are known to build on these interfaces, injecting add-on services."This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency," the report notes.

Advice here is for organizations to understand the security implications associated with the usage, management, orchestration, and monitoring of cloud services. Weak interfaces and APIs can expose an organization to such security issues pertaining to confidentiality, integrity, availability, and accountability.

2.5. Denial of service

DoS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed.

While an attacker may not succeed in knocking out a service entirely, he or she "may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself,".

2.6. Malicious insiders

Which can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes? In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From IaaS to PaaS to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data.

In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryption is implement, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack".

2.7. Cloud abuse

Such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.

2.8. Insufficient due diligence

Organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud. CSA's basic advice is for organizations to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud.

2.9. Shared technology vulnerabilities

Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models," according to the report.

If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to a potential of compromise and breach. CSA recommends a defensive, in-depth strategy, including compute, storage, network, application, and user security enforcement, as well as monitoring.

III. TO REDUCE RISK AND PROTECT DATA.

3.1. *Know who's accessing what.*

People within your organization who are privileged users, – such as database administrators and employees with access to highly valuable intellectual property – should receive a higher level of scrutiny, receive training on securely handling data, and stronger access control.

3.2. *Limit data access based on user context.*

Change the level of access to data in the cloud depending on where the user is and what device they are using. For example, a doctor at the hospital during regular working hours may have full access to patient records. When she's using her mobile phone from the neighborhood coffee shop, she has to go through additional sign-on steps and has more limited access to the data.

3.3. *Take a risk-based approach to securing assets used in the cloud*

Identify databases with highly sensitive or valuable data and provide extra protection, encryption and monitoring around them.

3.4. Extend security to the device.

Ensure that corporate data is isolated from personal data on the mobile device. Install a patch management agent on the device so that it is always running the latest level of software. Scan mobile applications to check for vulnerabilities.

3.5. Add intelligence to network protection.

The network still needs to be protected – never more so than in the cloud. Network protection devices need to have the ability to provide extra control with analytics and insight into which users are accessing what content and applications.

3.6. Build in the ability to see through the cloud.

Security devices, such as those validating user IDs and passwords, capture security data to create the audit trail needed for regulatory compliance and forensic investigation. The trick is to find meaningful signals about a potential attack or security risk in the sea of data points.

Adding a layer of advanced analytics – a security intelligence layer – brings all of this security data together to provide real-time visibility into the both the data centre and the cloud infrastructure.In the same way that clouds in the sky have an ever-evolving perimeter, so does cloud computing. Security is an important factor in cloud deployments and by building in the security capabilities described in these six steps, organizations can better manage and protect people, data and their devices in the cloud.

IV. CONCLUSION

Computing clouds are changing the whole IT , service industry, and global economy. Clearly, cloud computing demands ubiquity, efficiency, security, and trustworthiness.Cloud computing has become a common practice in business, government, education, and entertainment leveraging 50 millions of servers globally installed at thousands of datacenters today.

Effective trust management, guaranteed security, user privacy, data integrity, mobility support, and copyright protection are crucial to the universal acceptance of cloud as a ubiquitous service.

V. REFERENCES

[1] Cloud Computing: Concepts, Technology & Architecture by Thomas Erl.
[2] Cloud Computing Explained by John Rhoton.
[3] Security Engineering for Cloud Computing: Approaches and ToolsDavid G. Rosado, D. Mellado, Eduardo Fernandez-Medina and Mario G. Piattini.
[4] http://www.infoworld.com/article/2613560/cloud-security/9-top-threats-to-cloud-computing-security.html
[5]http://www.theguardian.com/media-network/media-network-blog/2013/sep/05/cloud-computing-security-protect-data