



INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY CHALLENGES WITH CLOUD COMPUTING

Prof. Ambika V Mittapally

* Computer Science and Engineering , Government Polytechnic Solapur , INDIA

ABSTRACT

Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users.

Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.

KEYWORDS: cloud computing, security challenges -Saas , Paas , Iaas,Services

INTRODUCTION

Cloud computing security or, more simply, **cloud security** is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.



Fig. 1: Cloud Computing

RELATED WORK

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. 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:

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.

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. 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.

Organizations and enterprises are increasingly considering Cloud Computing to save money and to increase efficiency. However, while the benefits of Cloud Computing are clear, most organizations continue to be concerned about the associated security implications. Due to the shared nature of the Cloud where one organization's applications may be sharing the same metal and databases as another firm, Chief Security Officers (CSOs) must recognize they do not have full control of these resources and consequently must question the inherent security of the Cloud.

All Cloud Models Are Not the Same

Although the term Cloud Computing is widely used, it is important to note that all Cloud Models are not the same. Cloud Models can be segmented into **Software as a Service (SaaS)**, **Platform as a service (PaaS)** and **Integration as a Service (IaaS)**.



Fig. 2: Cloud Model- SaaS, PaaS, IaaS.

SaaS: this particular model is focused on managing access to applications. For example, policy controls may dictate that a sales person can only download particular information from sales CRM applications. For example, they are only permitted to download certain leads, within certain geographies or during local office working hours.

PaaS: the primary focus of this model is on protecting data. This is especially important in the case of storage as a service. An important element to consider within PaaS is the ability to plan against the possibility of an outage from a Cloud provider. The security operation needs to consider providing for the ability to load balance across providers to ensure fail over of services in the event of an outage.

IaaS: within this model the focus is on managing virtual machines. The CSOs priority is to overlay a governance framework to enable the organization to put controls in place regarding how virtual machines are created and spun down thus avoiding uncontrolled access and potential costly wastage.

SECURITY CHALLENGES WITH CLOUD COMPUTING

The following check-list of Cloud Security Challenges provides a guide for Chief Security Officers who are considering using any or all of the Cloud models.

For CHIEF SECURITY OFFICERS focused on SaaS

Challenge #1: Don't replicate your organization in the Cloud

Large organizations using Cloud services face a dilemma. If they potentially have thousands of employees using Cloud services, must they create thousands of mirrored users on the Cloud platform? The ability to circumvent this requirement by providing single sign-on between on-premises systems and Cloud negates this requirement. Users with multiple passwords are also a potential security threat and a drain on IT Help Desk resources. The risks and costs associated with multiple passwords are particularly relevant for any large organization making its first foray into Cloud Computing and leveraging applications or SaaS. For example, if an organization has 10,000 employees,

it is very costly to have the IT department assign new passwords to access Cloud Services for each individual user. For example, single sign-on users are less likely to lose passwords reducing the assistance required by IT helpdesks. Single sign-on is also helpful for the provisioning and de-provisioning of passwords. If a new user joins or leaves the organization there is only a single password to activate or deactivate vs. having multiple passwords to deal with. In a nutshell, the danger of not having a single sign-on for the Cloud is increased exposure to security risks and the potential for increased IT Help Desk costs, as well the danger of dangling accounts after users leave the organizations, which are open to rogue usage.

For CHIEF SECURITY OFFICERS focused on PaaS

Challenge #2: Keep an Audit Trail

Usage of Cloud Services is on a paid-for basis, which means that the finance department will want to keep a record of how the service is being used. The Cloud Service Providers themselves provide this information, but in the case of a dispute it is important to have an independent audit trail. Audit trails provide valuable information about how an organization's employees are interacting with specific Cloud services, legitimately or otherwise! The end-user organization could consider a Cloud Service Broker (CSB) solution as a means to create an independent audit trail of its cloud service consumption. Once armed with his/her own records of cloud service activity the CSO can confidently address any concerns over billing or to verify employee activity. A CSB should provide reporting tools to allow organizations to actively monitor how services are being used.

For CHIEF SECURITY OFFICERS focused on IaaS

Challenge #3: Governance: Protect yourself from rogue cloud usage and redundant Cloud providers

The classic use case for Governance in Cloud Computing is when an organization wants to prevent rogue employees from mis-using a service. For example, the organization may want to ensure that a user working in sales can only access specific leads and does not have access to other restricted areas. Another example is that an organization may wish to control how many virtual machines can be spun up by employees, and, indeed, that those same machines are spun down later when they are no longer needed. So-called "rogue" Cloud usage must also be detected, so that an employee setting up their own accounts for using a Cloud service is detected and brought under an appropriate governance umbrella. Whilst Cloud Service providers offer varying degrees of cloud service monitoring, an organization should consider implementing its own Cloud service governance framework. The need for this independent control is of particular benefit when an organization is using multiple SaaS providers, i.e. HR services, ERP and CRM systems. However, in such a scenario the CSO and Chief Technology Officer (CTO) also need to be aware that different Cloud Providers have different methods of accessing information. They also have different security models on top of that. Some use REST, some use SOAP and so on. For security, some use certificates, some use API keys. The problem that needs to be solved is that these cloud service providers all present themselves very differently. So, in order to use multiple Cloud Providers, organizations have to overcome the fact they are all different at a technical level. Again, that points to the solution provided by a Cloud Broker, which brokers the different connections and essentially smoothes over the differences between them. This means organizations can use various services together.

For CSOs focused on SaaS, PaaS and IaaS




Challenge #4: Protect your API Keys

Many Cloud services are accessed using simple REST Web Services interfaces. These are commonly called "APIs", since they are similar in concept to the more heavyweight C++ or Java APIs used by programmers, though they are much easier to leverage from a Web page or from a mobile phone, hence their increasing ubiquity. "API Keys" are used to access these services. These are similar in some ways to passwords. They allow organizations to access the Cloud Provider. Consider the example of Google Apps. If an organization wishes to enable single sign-on to their Google Apps (so that their users can access their email without having to log in a second time) then this access is via API Keys. If these keys were to be stolen, then an attacker would have access to the email of every person in that organization. The casual use and sharing of API keys is an accident waiting to happen. Protection of API Keys can be performed by encrypting them when they are stored on the file system, or by storing them within a Hardware Security Module (HSM).

RESULTS AND DISCUSSION

Here the graphs represents the different services provided by SaaS, PaaS, and IaaS

Table 1: Cloud computing service models geared for different purpose

	SaaS	PaaS	IaaS
Who uses it?	Bussiness user	Developer and deployer	System Manager
Services available	website testing, Wiki,office automation,Blog, Virtual Desktopp	Service and application Test,development ,Integration and deployment.	Message Queue, CPU, Network storage,virtual machine,Operating system,memory,keyboard,hard disk.
Why uses it?	To complete business task	To create applications and services of users	Create platform for service ,application test, development, Integration and deployment.
Example			

CONCLUSION

Cloud Computing deals with our Daily life. It becomes most popular for every user can enjoy highly demanded services provided by cloud. A user can share cloud services anywhere, anytime with any device . This paper outlined a survey in cloud computing security challenges in its services, focusing on the long list services provided by leading companies. The researchers still have more work to do; we hope this paper will be considered as a starting point identifying opportunities for future research.

REFERENCES

1. B. Furht, "Cloud Computing Fundamentals," Handbook of Cloud Computing, pp. 3-19, Springer, 2010.
2. Hamzeh Khazaei, Student Member, IEEE, Jelena Mistic, Senior Member, IEEE, and Vojislav B. Mistic, Senior Member, IEEE "Performance nalysis of Cloud Computing Centers Using M/G/m/m + r Queuing Systems", Vol. 23, NO. 5, May 2012
3. Paul Marshall, Kate Keahey and Tim Freeman , " mproving Utilization of nfastructure Clouds" IEEE/ACM Cloud Computing May 2011
4. Karim BB S and jamil " SS N , " Approximation in an M.G/1 queuing system with breakdowns and repairs", Laboratory of Modelization and Optimization of Systems University of Bejaia, 06000(Algeria)
5. P. Hokstad, " pproximations for the M/G/m Queues," Operations Research, vol. 26, pp. 510-523, 1978.
6. Sivadon Chaisiri, Student Member, IEEE, Bu-Sung Lee, Member, IEEE, and Dusit Niyato, Member, IEEE "Optimization of Resource Provisioning Cost in Cloud Computing" Vol. 5, No. 2, pril-June 2012
7. Alexandru Iosup, Member, IEEE, Simon Ostermann, M. Nezhil Yigitbasi, Member, IEEE,Radu Prodan, Member, IEEE, Thomas Fahringer, Member, IEEE, and Dick H.J. Epema, Member, IEEE "Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing "
8. J.M. Smith, "M/G/c/K Blocking Probability Models and System Performance," Performance Evaluation, vol. 52, pp. 237-267, May 2003.
9. Sinung Suakanto, Suhono H Supangkat, Suhardi and Roberd Saragih, PERFORM NCE MEASUREMENT OF CLOUD COMPUTING SERV CES" JCCS ,Vol.2, No.2, April 2012
10. J. D. Poston and W. D. Horne, "Discontiguous OFDM considerations for dynamic spectrum access in idel TV channels," in Proc. IEEE DySPAN, 2005.