IJournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 12, December-

A review of Modular Approach for Security in Cloud Services

Sunil Dhawan
Research Scholar, NIMS University,
Jaipur, India
Email Id: sunildhawan007@gmail.com

Vikas Verma
Associate Professor, Chandigarh Business School,
CGC, Landran,Mohali, India
Email Id: vikas2005verma@yahoo.co.in

Abstract – In this paper we analyse and interpret the growing security concerns in cloud computing. Cloud computing provides many benefits like resource sharing. Cloud computing provides flexible and cost effective platform for providing IT services over the Internet. Cloud Computing also inherits security threats as the computing power is outsourced. Cloud Computing follows SPI model. We will discuss and identify the security threats and weakness in this paper. A modular security approach would be created so as to provide security solution to different level of services offered by Cloud Computing.

Keywords – Security, Cloud Computing, SPI model, threats, security solutions.

I. INTRODUCTION

For quite some time now we have witnessed an unparalleled growth in a technology which was once considered to be a niche product. Cloud Computing or services has a distinct association with internet. The term cloud here represents a platform that exists in the world of internet and that is always online. It provides us virtual hardware as well as software platforms that are much more efficient than building servers and other infrastructure for the same. Security in information technology domain is an issue that is too big to be ignored. Any product ranging from desktop application to mobile applications from server products to banking applications the security has a role to play in any of the products.

Cloud computing is is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.[1]

Cloud describes the use of a collection of services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned and scaled up or down providing for an on demand utility like model of allocations and consumption. Any network computing service to be called as cloud service has to have 5 characteristics:

1. On demand computing resource allocation and capabilities.
2. It should have multiple and broad network access.
3. The resources must be pooled together to create a vast pool of resource that can be used to serve multiple clients.
4. The service should be scalable so as to achieve elasticity.
5. The services should be monitored

Cloud Computing enables ubiquitous, convenient,on-demand network access to a shared pool of configurablecomputing resources (e.g., networks, servers, storage,applications, and services) that can be rapidly provisionedand released with minimal management effort or serviceprovider interaction.Cloud Computing appears as a computational paradigmas well as a distribution architecture and its mainobjective is to provide secure, quick, convenient datastorage and net computing service, with all computingresources visualised as services and delivered over theInternet [2].Cloud Computing combines a number of computingconcepts and technologies such as Service OrientedArchitecture (SOA), Web 2.0, virtualisation and othertechnologies with reliance on the Internet, providingcommon business applications online through webbrowsers to satisfy the computing needs of users, whiletheir software and data are stored on the servers [3]. There are many benefits to adopting CloudComputing, there are also some significant barriers to its adoption. One of themost significant barriers to adoptionis security, followed by issues regarding compliance,privacy and legal matters [4]. Because Cloud Computingrepresents a relatively new computing model, there is agreat deal of uncertainty about how security at all levels(e.g., network, host, application, and data levels) can beachieved and how applications security is moved toCloud Computing [5]. That uncertainty has consistentlyled information executives to state that security is theirnumber one concern with Cloud Computing [6]. Security concerns are quite relevant in case of Cloud Computing because pretty much everything lies in the hands of third party. Issues such as integration, external data storage, open internet access. One of the major concerns is regarding the sharing of resources for different applications. Virtualised environment also contributes to the same and the methods that are traditionally used cannot be used for cloud computing. Because of the multiple levels of integration happens while providing cloud services it presents different risks to an organisation compared to the existing it infrastructure. Integration of security into models make the system more rigid and slow. But the cost of performance must not be on the basis of security. The categorisation of security issues is based on the most common model adopted by the cloud computing providers known as SPI Model (SAAS, PAAS, IAAS). We will be considering threats and vulnerabilities as objects for findings and research. A threat is a potential attack that maylead to a misuse of information or resources, and theterm vulnerability refers to the flaws in a system thatallows an attack to be successful. We here present a list of vulnerabilities and threats and their effects on different services in cloud. Further we present some countermeasures to stop or eradicate these threats.

II. Literature Review

We have studied and carried out review of the available resources in terms of security analysis and review of cloud computing. Identification of the main vulnerabilities in this kind of system are found in the literature related to cloud computing .We have done this to identify the existing issues for cloud computing. [7-9]

A. Sources for Literature

The selection of sources is based on the study conducted by us using different thoughts and searches on internet revealed how we should go about studying a source. All of the sources are available on the web. The sources include ACM digital library, Google Scholar and Science Direct and other journals mentioning relevant data.

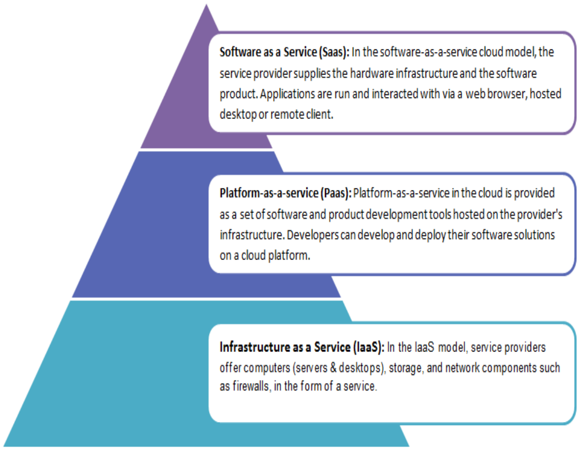
B. Evaluation of Resource

With the pool of sources defined we described the process for study selection and evaluation. The criteria for selection of resource was that it should provide information about threats, vulnerabilities and the level of risk it contains.

III. Cloud Computing-Model and Implications

Any Cloud Computing service provider provides cloud services in three tier architecture based model known as SPI. Three type of services that comes under this model are:

1. Software as a Service (SaaS). The capabilityprovided to the consumer is to use the provider'sapplications running on a cloud infrastructure. Theapplications are accessible from various clientdevices through a thin client interface such as a webbrowser (e.g., web-based email).
2. Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications with installing any platform or tools on their local machines. Pass refers to providing platform layer resources including operating system support and software development frameworks that can be used to build higher-level services.
3. Infrastructure as a Service (IaaS). The capabilityprovided to the consumer is to provision processing,storage, networks, and other fundamentalcomputing resources where the consumer is able todeploy and run arbitrary software, which caninclude operating systems and applications.



Software as a Service (Saas): In the software-as-a-service cloud model, the service provider supplies the hardware infrastructure and the software product. Applications are run and interacted with via a web browser, hosted desktop or remote client.

Platform-as-a-service (Paas): Platform-as-a-service in the cloud is provided as a set of software and product development tools hosted on the provider's infrastructure. Developers can develop and deploy their software solutions on a cloud platform.

Infrastructure as a Service (IaaS): In the IaaS model, service providers offer computers (servers & desktops), storage, and network components such as firewalls, in the form of a service.

The security has different implications at different ends of cloud services. This is due to the two dimensional equation between functionality and customer control. In case of SaaS mode of service there is huge integrated functionality but at the cost of customer control. From security's point of view the responsibility lies with the cloud provider. In case of PaaS mode of service, it hits a sweet spot between functionality and control. It provides greater extensibility with greater customer control over security. In case of IaaS or Infrastructure as a Service there is really low level of abstraction. Relationships between these cloud service models add to the security challenges. e.g. both PaaS and SaaS are hosted on top of IaaS. Thus any breach or vulnerability at IaaS will definitely impact as they become the part of the cloud hosting stack. As far as PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between the models. Thus it depends on how deep the attack is on which layer. If the target is low layer then it would consequently affect the upper layers also. The relationship can also contribute towards accumulation of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Thus the security policy would be different for different providers. Thus providing a inconsistent combination of security models. It leads to a situation where the customer might not be able to ascertain the responsible service provider in case of a security attack[10].

IV. Security Challenges in Cloud Computing

As discussed in the above section the security challenges depends what combination of security and cloud computing model you are using. The SPI model allows a hybrid solution to implement security policy. There are certain security issues that are specific to these models.

1. **Security Issues for Software as a Service (SaaS)**- SaaS provides on demand services like Email, conferencing software and ERP, CRM and SCM as business applications. Out of the three models SaaS provides least security control to its users. Thus the concerns over security is highest in this model of cloud services.

- Application security is one of the security concerns. The applications hosted on SaaS are typically delivered via Internet through a Web browser such as Google Chrome or Firefox etc. At the basic level these are web applications and attackers can use web flaws to gain access to data or sensitive information. Security challenges in this domain are same as of a web application thus posing a challenge for providing security as just using the application level security doesn't effectively protect the hosted applications.

- Data Security is a common security security concern. It has major impact in case of SaaS users as they have to rely on their providers for proper implementation of security. The data is often processed in plain text and stored in the cloud. The SaaS provider is the one responsible for the security of the data while its being processed and stored. It also involves the issue of backup and recovery. It may happen that cloud providers may hire third party backup services which again lead to sharing of data and raising security concerns. In SaaS, the processof compliance is complex because data is located in theprovider's datacenters, which may introduce regulatorycompliance issues such as data privacy, segregation, andsecurity, that must be enforced by the provider.

- Accessibility- Using internet as a platform and accessing the applications via web browser not only makes the things easier but also exposes the service to additional security risks. The current state of mobile computing has high no. of threats such as insecure networks, malware, snuffing and hacking in marketplaces.

2. **Security Issues for Platform as a Service (PaaS)-** Using Paas as platform provides us the facility to use cloud as a platform without deploying the hardware and just using only software layers. PaaS application security comprises of two software layers. Security of the PaaS platform itself and security of customer applications deployed on a PaaS platform. PaaSproviders are responsible for securing the platform softwarestack that includes the runtime engine that runsthe customer applications. Same as SaaS, PaaS alsobrings data security issues.

3. **Security Issues for Infrastructure as a Service (IaaS)**- IaaS provides a pool of resources such as servers, storage,networks, and other computing resources in the form ofvirtualized systems, which are accessed through theInternet. Users are entitled to run any softwarewith full control and management on the resources allocatedto them. With IaaS, cloud users have bettercontrol over the security compared to the other modelsas long there is no security hole in the virtual machinemonitor. They control the software running in theirvirtual machines, and they are responsible to configure securitypolicies correctly. However, the underlyingcompute, network, and storage infrastructure is controlledby cloud providers. IaaS providers must undertake a substantialeffort to secure their systems in order to minimise these threats that result from creation, communication,monitoring, modification, and mobility [11].Following are some of the areas of concern in terms of security at infrastructure level:

- Virtualisation allows us to create virtual machines and copy and share them and run a no. of different applications using same hardware however this sharing mechanism provides new opportunities to attackers.

- Shared Resources Sharing resources between VMs may decreasethe security of each VM. For example, a maliciousVM can infer some information about other VMs throughshared memory or other shared resources without need ofcompromising the hypervisor.Thus,a malicious Virtual Machine can monitor sharedresources without being noticed by its VMM, so theattacker can infer some information about other virtualmachines.

V. Analysis of Threats and Vulnerabilities

We have analysed the existing security threats and vulnerabilities of cloud computing. We identify the cloud service model affected by the security problems. Some of the threats and vulnerabilities that become relevant due to the additional level of interference caused by human resources that are listed below:

- Lack of employee screening and poor hiringpractices – some cloud providers may notperform background screening of their employees orproviders. Privileged users such as cloudadministrators usually have unlimited access to thecloud data.
- Lack of customer background checks – most cloudproviders do not check their customer's background,and almost anyone can open an account with a validcredit card and email. Apocryphal accounts can letattackers perform any malicious activity withoutbeing identified.
- Lack of security education – people continue to be aweak point in information security [12]. This is truein any type of organisation; however, in the cloud, ithas a bigger impact because there are more peoplethat interact with the cloud: cloud providers, third party providers, suppliers, organisational customersand end-users.

Following table contains the list of vulnerabilities:

Vul. No.	Vulnerabilities
1	Cloud API and Interfaces are insecure
2	Insufficient Authorization checks
3	Inaccurate modeling of resources
4	Data Handling by untrusted third parties
5	Uncontrolled migration and backup of Virtual Machines

Following table contains the list of threats:

Threat No.	Threat Name & Desc.
1	User Id based attack where the access is gained through account theft using social engineering.
2	Data leakage where the data gets into the wrong hands while being processed.
3	Data Scavenging using the old devices and recovering information through some recovery software.
4	Denial of Service Attack by eliminating access to the legitimate users.
5	VM Hopping happens when we are able to gain access by using another VM's hypervisor vulnerability.
6	Sniffing Virtual networks allow us to redirect packet traffic to different VMs

VI. Countermeasures

Some of the recommendations based on the study are provided to eradicate some of the issues:

A. Identity based access management system to ensure that minimum access is provided to the anonymous users. Cloud Security Alliance has suggested some of the best practices that one can adopt identity based secure access.

B. Use of Dynamic Credentials for mobile computing means that the value of credentials change once a user changes its location or has accessed no. of packets.

C. Adoption of FRS aims to provide intrusion tolerance and secure storage. It allows secure storage by breaking down sensitive data into insignificant fragments so any fragment does not have any significant information by itself.

D. Use of Digital Signatures that has embedded RSA algorithm while the data is being transferred over the Internet. By allowing RSA algorithm in cloud one can achieve data protection.

E. Use of Fully homomorphic encryption in cloud allows performing arbitrary computation on cipertexts without being decrypted. However using homomorphic operations need huge amounts of processing power and is not recommended for small projects and startups.

F. Web Application Scanners is a programs which scans web applications through the web front-end in order to identify security vulnerabilities. This can be used in conjunction with web application firewalls.

G. HyperSafe can be used to ensure control flow integrity. HyperSafe's goal is to protect hypervisors by using two techniques such as non-bypassable memory lockdown which protects write protected memory pages from being modified and restricted pointed indexing that converts control data into pinter indexes.

H. Use of only trusted virtual machines for controlling execution environment for applications.

IX. CONCLUSION AND FUTURE SCOPE

Security in Cloud Computing is involving and it raises some security problems which may slow down its growth. Understanding the security would enable the companies adopt cloud systems at faster rate. Virtualisation is an inseparable part of the cloud offerings as every cloud service provider use virtualisation to offer a variety of services. Virtual networks are also target for some attacks when communicating with remote virtual machines. The future work on the matter will include creating relationships between different threats and providing conjunctional countermeasures.

REFERENCES

Journal References

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread-spectrum watermarking for multimedia”, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 64 – 69, December 1997.

[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) CloudComputing: A Statistics Aspect of Users. In: First International Conference onCloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg,pp 347–358

[3] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1stInternational Conference on Cloud Computing (CloudCom), Beijing, China.Springer-Verlag Berlin, Heidelberg

[4] KPMG (2010) From hype to future: KPMG’s 2010 Cloud Computing survey.Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

[5] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysisin the migration to cloud environments. Future Internet 4(2):469–487

[6] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O’ReillyMedia, Inc., Sebastopol, CA

[7] Kitchenham B (2004) Procedures for perfoming systematic review, softwareengineering group. Department of Computer Scinece Keele University,United Kingdom and Empirical Software Engineering, National ICT AustraliaLtd, Australia. TR/SE-0401

[8] Kitchenham B, Charters S (2007) Guidelines for performing systematicliterature reviews in software engineering. Version 2.3 University of keele(software engineering group, school of computer science and mathematics)and Durham. Department of Conputer Science, UK

[9] Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessonsfrom applying the systematic literature review process within the softwareengineering domain. J Syst Softw 80(4):571–583

[10] Hashizume et al. Journal of Internet Services and Applications 2013, 4:5http://www.jisajournal.com/content/4/1/

[11] Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security:Challenges and solutions. In: the 7th International Conference onInformatics and Systems (INFOS), Potsdam, Germany. IEEE ComputerSociety, Washington, DC, USA, pp 1–8

[12] Popovic K, Hocenski Z (2010) Cloud Computing Security issues andchallenges. In: Proceedings of the 33rdInternational convention MIPRO.IEEE Computer Society Washington DC, USA, pp 344–349