Cloud Computing – Understanding Risk, Threats, Vulnerability and Controls: A Survey

Manish M. Potey,
Department of Computer Engineering,
K. J. Somaiya College of Engineering,
Mumbai, India

C A Dhote, PhD.
Department of Computer Science & Engineering,
P. R. M. I. T & R,
Amravati, India

Deepak H. Sharma,
Department of Computer Engineering,
K. J. Somaiya College of Engineering,
Mumbai, India

ABSTRACT
As an embryonic technology, cloud computing has attracted more attention. More and more enterprises or government agencies started to explore cloud computing. However, with the extensive use of cloud computing, security issues came out on a growing scale. This paper highlights and categorizes many of security issues introduced by the "cloud"; surveys the risks, threats, vulnerabilities and controls. Besides, the paper summarizes some corresponding solutions that can help promote the benefits and mitigate the risks associated with Cloud Computing.

Keywords
Cloud Computing, Risk, Threat, Vulnerability, Controls

1. INTRODUCTION
Cloud computing is not a new technology but rather a new delivery model for information and services using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs both offer services. The cloud provides a layer of abstraction between the computing resources and the low level architecture involved. The clouds have different architecture based on the services they provide. The data is stored on to centralized location called data centers having a large size of data storage. The data as well as processing is somewhere on servers. So, the clients have to trust the provider on the availability as well as data security.
This paper discusses the concept of "cloud" computing, some of the issues likethreats, vulnerability and controls related to Cloudcomputing security. Section 2 discusses concepts and components of "cloud" computing. Section 3 describes Cloud Security reference Model and Cloud computing Security. Section 4 discusses "cloud"-related threats, vulnerabilities and controls and section five summaries and concludes the paper.

2. WHAT IS CLOUD COMPUTING

What Comprises Cloud Computing?
NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models.

Service Delivery Model

Software as a Service (SaaS)
This is where users simply make use of a web-browser to access software that others have developed and offer as a service over the web.

Platform as a Service (PaaS)
This is where applications are developed using a set of programming languages and tools that are supported by the PaaS provider.

Infrastructure as a Service (IaaS)
This is where users acquire computing resources such as processing power, memory and storage from an IaaS provider and use the resources to deploy and run their applications.

Cloud Computing Definition
Vaquero et al. [5] concur with the NIST definition to a significant extent. For example, Vaquero et al. studied 22 definitions of cloud computing and proposed the following definition:
Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure Provider by means of customized SLAs[26].

Cloud Computing Deployment Models[7][9][16]

Private cloud
The cloud infrastructure is operated solely within a single organization, and managed by the organization or a third party regardless whether it is located on premise or off premise.

Public cloud
The public cloud is used by the general public cloud consumers and the cloud service provider has the full ownershipof the public cloudwith its own policy, value, and profit, costing, and charging model.

Hybrid cloud
The cloud infrastructure is a combination of two or more clouds (private or public) that remain unique entities but are

bound together by standardized or proprietary technology that enables data and application portability.

Community cloud

Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community

3.CLOUD SECURITY REFERENCE MODEL

The cloud security reference model addresses the relationships of the classes and places them in context with their relevant security controls and concerns[8].The deployment and consumption modalities of cloud should be thought of not only within the context of 'internal' vs. 'external' as they relate to the physical location of assets, resources, and information; but also by whom they are being consumed by; and who is responsible for their governance, security, and compliance with policies and standards. This is not to suggest that the on- or off-premise location of an asset, a resource, or information does not affect the security and risk posture of an organization because they do — but to underscore that risk also depends upon:

- The types of assets, resources, and information being managed
- Who manages them and how
- Which controls are selected and how they are integrated
- Compliance issues
- The figure 1 shows an example of how a cloud service mapping can be compared against a catalogue of compensating controls to determine which controls exist and which do not — as provided by the consumer, the cloud service provider, or a third party. This can in turn be compared to a compliance framework or set of requirements such as PCI DSS, as shown.
- There is gap in each model - cloud model, security control model and Compliance model. Once this gap analysis is complete, it becomes much easier to determine what needs to be done in order to feed back into a risk assessment framework; this, in turn, helps to determine how the gaps and ultimately risk should be addressed: accepted, transferred, or mitigated. It is important to note that the use of cloud computing as an operational model does not inherently provide for or prevent achieving compliance. The ability to comply with any requirement is adirect result of the service and deployment model utilized and the design, deployment, and management of theresources in scope.

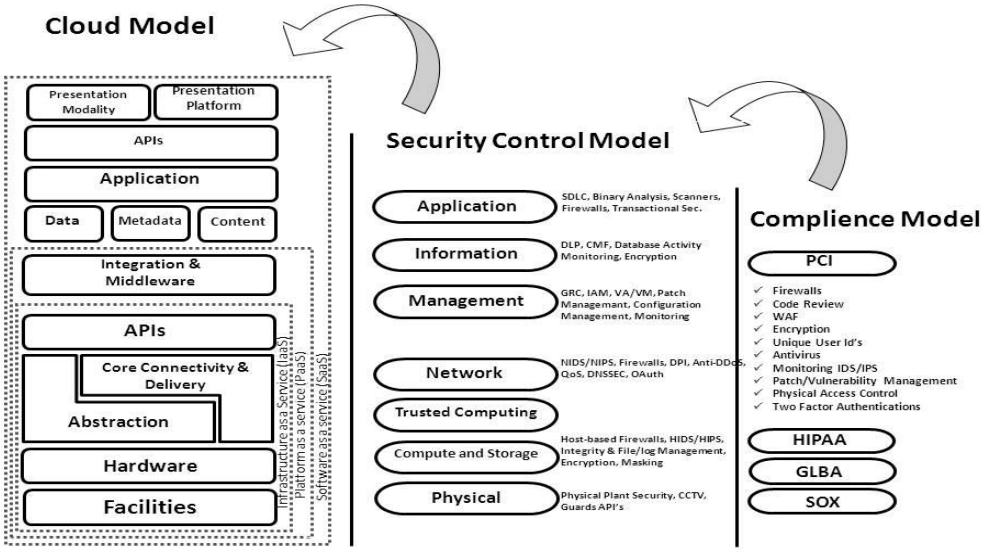

Fig1. Mapping the Cloud Model to the Security Control & Compliance Model [8]

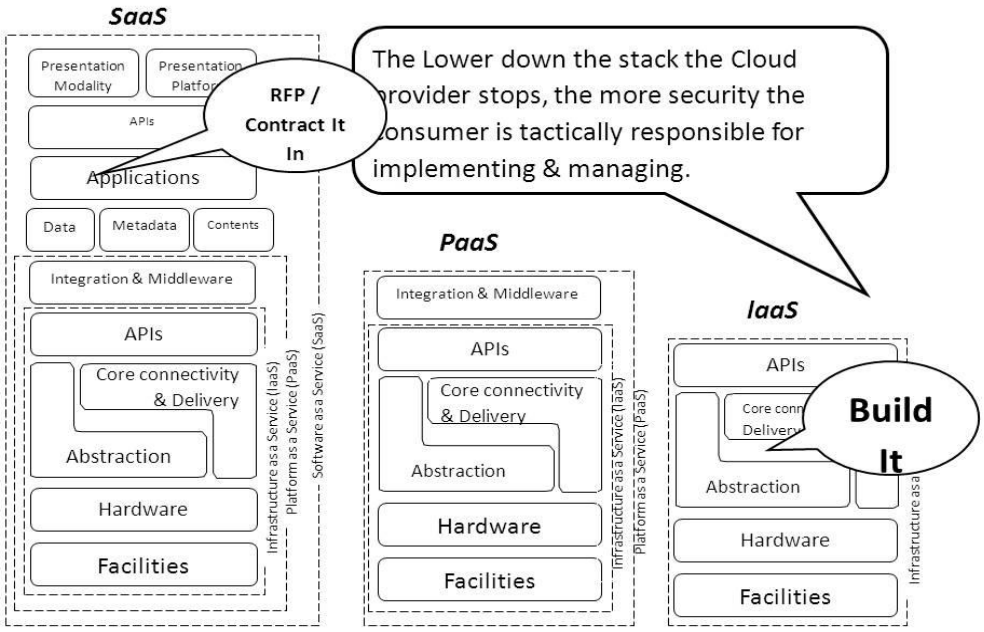

Fig. 2 How Security Gets Integrated [8]

What Is Security for Cloud Computing?

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjustedsecurity controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the ITsystems (system security), and all the way to the information and applications (application security)[8].

The figure 2 illustrates issues: in SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts. In an IaaS offering, while the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform itself falls onto the provider, but securing the applications developed against the platform and developing them securely, both belong to the consumer.

4. CLOUD COMPURING RISK THREATS, VULNERABILITIES AND CONTROLS

The words "Vulnerability," "Threat," "Risk," and "Exposure" often are used to represent the same thing even though they have different meanings and relationships to each other.

"Vulnerability" refers to a software, hardware, or procedural weakness that may provide an attacker the open door to enter acomputer or network and have unauthorized access to resourceswithin the environment. Vulnerability characterizes the absenceor weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software, or an unsecuredphysical entrance [17].

A "Threat" is any potential danger to information or systems. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. Threats exploit existing vulnerabilities in an attempt to cause damage or destruct a resource.

A "Risk" is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact.

A controlis generally put into place to mitigate the potential risk. A control may be a policy, procedure, a software configuration, or a hardware device thateliminates vulnerability or reduces thelikelihood that a threat agent will be able to exploit vulnerability. Strong authentication mechanisms, computer antivirus software and information security awareness are some examples of proper countermeasures. In any enterprise, information security risks must be identified, evaluated, analyzed, treated and properly reported. Businesses that fail in identifying the risks associated with the technology they use, the people they employ, or the environment where they operate usually subject their business to unforeseenconsequences that might result in severe damage to the business. Because risks cannot be completely eliminated, they need to be lowered into acceptable levels. Acceptable risks are risks that the business decides to live with, given that proper assessment for these risks was done and the cost of treating these risks might outweigh the benefits.

4.1Cloud Specific Vulnerabilities

Other researchers prefer to focus on cloud specific vulnerabilities, without much focus on threats and risks [14]. According to such research, a particular vulnerability can be considered specific to cloud computing if it meets any of thefollowing criteria [17]:

- it is intrinsic to or prevalent in a core technology of cloud computing, such as virtualization, service oriented architecture, and cryptography
- it has its root cause in one of essential cloud characteristics, such as elasticity, resource pooling, and pay-as-you-go model
- it is caused by cloud innovations making exiting (tried and tested) security controls hard or impossible to

implement; for example, management procedures that were created initially for a fixed hardware structure do not port correctly to virtual machines [5]
- it is prevalent in established state-of-the-art cloud services

4.2 Threats and their respective controls

As given in paper from CSA [13], the threats have been classified as below:

4.2.1 Abuse and Nefarious Use of Cloud Computing

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers havebegun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Examples

IaaS offerings have hosted the Zeus botnet, InfoStealertrojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

Remediation

- Stricter initial registration and validation processes.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

4.2.2: Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Examples

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring andlogging capabilities, unknown service or API dependencies.

Remediation

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

4.2.3: Malicious Insiders

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure.

Examples: No public examples are available at this time.

Remediation

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

4.2.4: Shared Technology Issues

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up thisinfrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement andmonitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenantsrunning on the same cloud provider. Customers should not have accessto any other tenant's actual or residual data, network traffic, etc.

Example

Joanna Rutkowska's Red and Blue Pill exploits

Remediation

- *Implement security* best practices for installation/configuration.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

4.2.5: Data Loss or Leakage

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media.

Examples

Insufficient authentication,authorization, and audit (AAA) controls;inconsistent use of encryption and software keys; operational failures;persistence and remanence challenges: disposal challenges; risk ofassociation; jurisdiction and political issues; data center reliability; anddisaster recovery.

Remediation

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management,and destruction practices.
- Contractually demand providers wipe persistent media before itis released into the pool.

- Contractually specify provider backup and retention strategies.

4.2.6: Account or Service Hijacking

Account or service hijacking is not new. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.

Examples

Nopublic examples are available at this time.

Remediation

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs

4.2.7: Unknown Risk Profile

Description

One of the tenets of Cloud Computing is the reduction of hardware andsoftware ownership and maintenance to allow companies to focus on their core business strengths. Information about who is sharing your infrastructure may be pertinent, inaddition to network intrusion logs, redirection attemptsand/or successes, and other logs.Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas.

Examples

- IRS asked Amazon EC2 to perform a C&A; Amazon refused. http://news.qualys.com/newsblog/forrester-cloud-computingqa.html
- Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected, but Heartland was "willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data has been stolen." http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html

Remediation

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

5. CONCLUSION

In this paperit is started with Cloud Computing Definition and explained various types of clouds and their deployment models. Then it addressed issues related to cloud computing security using Cloud security reference model. The various Cloud specific vulnerabilities were explored and their corresponding threats, risks were examined and some remediation and controls were proposed. With more devices getting added to cloud worldwide daily there are going to be more security issues that will need to be addressed by various researchers at appropriate level in cloud computing security reference model. There are going to be security threats at network-, host-, and application-level, security and the issues surrounding each level with specific regard to cloud computing will have to be resolved in future. Another issue regarding security arises because of cloud APIs which are not yet standardized, so each cloud provider has its own specific APIs for managing its services which needs to be integrated across multiple vendors.

6. REFERENCES

[1] Tim Mather, SubraKumarswamy, and ShahedLatif, Cloud Security and Privacy,s.l; O'Reilly, 2010

[2] T Grance, K Kent and B Kim. NIST SP800-61 computer security incident handling guide, 2008

[3] Gartner."Seven cloud computing security risks".http://www.infoworld.com July 2,2008

[4] Charles P Pfleeger, Security in Computing. Pearson Education.

[5] Vaquero, Luis Rodero-Merino Juan Caceres et. al "A break in clouds : Towards a cloud definition." ACM SIGOMM Computer Communication Review Archive, Volume 39, Issue 1 (January 2009).

[6] RichMaggini, Solari communication. "Cloud Computing is changing how we communicate",IEEE,2009.

[7] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and security issues", ProfessionalCommunication Conference, 2009.IECC 2009. IEEE International

[8] Adrian Seccombe, Alex Hutton, Alexander Meisel, et, al.Security Guidance for Critical Areas of focus in Cloud Computing V 2.1, Cloud Security Alliance , 2009

[9] Meiko Jensen JorgSchwenk, Nils Gruschka,Luigi Lo Icono, "On Technical Security Issues in Cloud Computing", 2009 IEEE conference on Cloud Computing.

[10] Kaufman, L.M. " Data Security in the World of Cloud Computing". Security& Privacy, IEEE, vol. 7 , pp. 61 - 64 , July-Aug. 2009

[11] La'Quata Sumter, " Cloud Computing : Security Risk", ACM SE '10 Proceedings of the 48th Annual Southeast Regional Conference ACM New York, NY, USA ©2010

[12] ENISA, Cloud Computing: Benefits, risks and recommendation for information security,2010

[13] Dan Hubbard, Michael Sutton, AmerDeeba, Andy Dancer, et. al,Top Threats to cloud Computing v1.0, 2010

[14] Bernd Grobaur,TobiasWalloschek and Elmer Stocker, "Understanding cloud computing vulnerabilities",IEEE security and privacy, 10 Jun 2010, IEEE computer society digital library, IEEE Computer Society

[15] Minqui Zhou, Rong Zhang, wieXie, WeiningQian, Aoying Zhou, Security and Privacy in Cloud Computing : A Survey, 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), IEEE Conferences.

[16] KresimirPopovic,ZeljkoHocenski, "Cloud Computing Security Issues and Challeges", MIPRO 2010 Proceedings of 33 International Convention ,IEEE,, May24-28, 2010,Opatija, Croatia

[17] Kamal Dahbur, Bassil Mohammad, Ahmed BisherTarakji, A Survey of risks, threats, and vulnerabilities in cloud computing, ACM 978-1-4503-0474-0/04/2011

[18] Jaeger, T.; Schiffman, J. "Outlook: Cloudy with a Chance of Security Challenges and Improvements", Security & Privacy, IEEE, vol. 8, pp. 77-80, Jan- Feb 2010.

[19] Takabi, H.; Joshi, J.B.D.; Ahn, G. "Security and Privacy Challenges in Cloud Computing Environments", Security & Privacy, IEEE, vol. 6, pp. 24-31, Nov.-Dec. 2010

[20] NIST,"NIST.gov-Computer Security Division-Computer Security Resource Centre" Wayne Jansen, Timothy Grance,"Guidelines on Security and privacy in public cloud computing" , Draft NIST special publication, January 2011.

[21] Wang Jun-jui, Mu Sen ,2011, "Security Issues and Counter Measures in Cloud Computing", IEEE 2011.

[22] FarzadSabahi, "Cloud Computing Security Threats and Responses", IEEE 2011.

[23] Tharam Dillon, Chen Wu, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010

[24] Sean Carlin, Kevin Curran, "Cloud Computing Security", International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011

[25] Balachandra Reddy Kandukuri et al., "Cloud Security Issues",IEEE International Conference on Services Computing, 2009

[26] IIangoSriram, Ali KhajehHosseni, "Research Agenda in Cloud Technology", 1st ACM Symposium on Cloud Computing, SOCC 2010