Cloud Computing Architecture, Security Trends and Assessment

Molkar Raj Kumar
Assistant Professor, KG Reddy College of Engineering & Technology, Hyderabad,T.S.
E-mail:- raj.kmolkar@gmail.com

ABSTRACT

Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is real and perceived lack of security. In this paper, we take a holistic view of cloud computing security - spanning across the possible issues and vulnerabilities connected with virtualization infrastructure; software platform; identity management and access control; data integrity; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. Cloud computing system delivers computing resources as a service over the network. During the last few years clod computing technology has gained attention due to its autonomous and cost effective services. It is responsible for the growth of IT industry. But cloud computing has various security challenges that hinder the rapid adoption of this computing paradigm. Efficient steps should be taken to make cloud computing more secure and reliable. This paper works on overview of clod computing as well as related security issues.

Keywords: Cloud Computing; Security; Trusted Computing; Service, Models, Deployment Models,

1. INTRODUCTION

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services (called Infrastructure as a Service or IaaS) [1]; for remote platform building and customization for business processes (called Platform as a Service or PaaS) [2]; and for renting of business applications as a whole (called Software as a Service or SaaS) [3]. The cloud infrastructure has been further sub-divided into Public cloud – where the infrastructure resides totally outside of the tenant / enterprises‟ firewall; Hybrid cloud – where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party; and Private cloud – where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in “per transaction” basis. Technology consulting firm Gartner has estimated market size of $59 billion for Public and Hybrid cloud and has predicted it to grow to $149 billion by 2014 with a compounded annual growth rate of 20% [4]. However, real and perceived security concerns remain one of the greatest inhibitors for adoption of Cloud computing. The primary concerns for cloud security are around cloud infrastructure, software platform and user data; as well as access control and identity management. Researchers also include broader issues of data

integrity and compliance under security. Additionally, physical data center security and processes play an important role.

There is a growing body of work dealing with various cloud computing security issues. Authors have mostly discussed about singular aspects of cloud security such as vulnerabilities in platform layer (virtualization, network, or common software stacks); vulnerabilities with co-located user data and multi-tenancy; access control; identity management and so on. However, barring a few [5] [6], there has not been a holistic treatment on cloud security issues and state of research in each of these issues. In this paper we provide a concise but all-round survey on cloud security trends and research.

We recognize that there are three major groups involved in cloud security. First group is the providers of Public and Hybrid clouds. Second group is the individuals / organizations which use cloud services – either by migrating and hosting their applications binaries / data to cloud, or by having an interface or a “pipe”

connected to an external cloud to do some activities (may be to download cloud public data / modules or to route messages through cloud). The third group is the Govt. and other third-party regulatory entities that may have fiduciary roles (audit, forensic etc.). In our paper, we have tried to map security concerns and obligations of each of these groups.

We observe that data, platform, user access and physical security issues; although accentuated in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks will be present in any virtualized environment not specific to cloud. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications. The paper outlines how research around Trusted Computing, Information Centric Security and Privacy Preserving Models may provide answer to some of these difficult challenges. Since private clouds are operating inside enterprise firewalls, we exclude them from this discussion.

1. 1. Characteristics of Cloud Computing

According to the NIST cloud computing contains following five essential characteristics:

A. On-demand self-service: Provision computer services such as email, network, application and computer capabilities. It also provision server service without human interaction from each service provider.

B. Broad network access: Computing capabilities are available over the network and can be accessed through standard mechanisms that promote the use of heterogeneous thin or thick client platform.

C. Resource pooling: The computing resources of the providers are pooled to support multiple consumers using a multi-tenant model with different virtual and physical resources dynamically assigned and reassigned according to consumer demand. The consumer has no idea or knowledge over the exact location of the resources but can access and use data at any time from any location.

D. Rapid elasticity: Computing capabilities can be rapidly and elastically provisioned. The resource pooling and self-service make it possible. The provider can automatically distribute more or less resources from available pool.

E. Measured Service: Cloud systems, in this case, automatically control and manage resource use by leveraging a metering capability at some level of abstraction as it seen appropriate to the type of service.

1. 2. Advantages of Cloud Computing

Some major advantages of cloud computing are given below:

- Greater Mobility: Information can be accessed at anytime from anywhere unlike traditional system (storing information in personal computer and accessing only when near it).
- Cost Reduction: Reduced costs due to more rapid deployment services and operational efficiencies.
- Increased Storage: At the point when compared to private computer systems, large amount of data can be stored than usual.
- Elasticity: Elastic nature of the infrastructure allows to swiftly allocate and de-allocate vastly scalable resources to business services on a demand basis.

2. CLOUD ARCHITECTURE

In order to analyze cloud security issues it is important to understand cloud architecture. According to NIST's cloud reference architecture [3], there are five most important factors that have an effect on and are impacted by cloud computing, along with its security implications.

- **Cloud Consumer:** An individual or organization that keeps up a business association with, and uses services from cloud provider.
- **Cloud Provider:** An individual or organization for creating a service accessible to interested parties.

- **Cloud Auditor:** A party that can conduct autonomous appraisal of cloud administrations, data framework operations, performance and security of the cloud usage.
- **Cloud Broker:** An entity that deals with utilization, performance and delivery of cloud services and negotiates relationships between cloud consumers and providers.
- **Cloud Carrier:** A medium that provides network and transport of cloud services from cloud providers to cloud consumers.

Figure 1 shows the architecture of cloud computing. The figure represents an end-to-end reference architecture that represents the layers of high level cloud architecture with Security Services. As it is apparent, cloud computing is a complex arrangements with numerous areas of vulnerabilities.

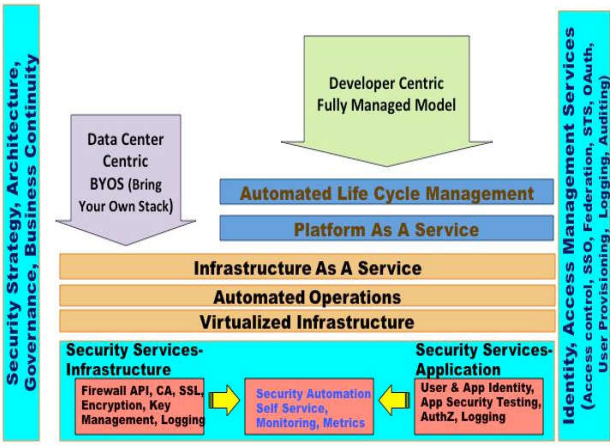

Figure 1. High level Cloud Architecture with Security Services.

Cloud application developers and devops have been successfully developing applications for IaaS (Amazon AWS, Rackspace, etc) and PaaS (Azure, Google App Engine, Cloud Foundry) platforms. These platforms provide basic security features including support for authentication, DoS attack mitigation, firewall policy management, logging, basic user and profile management but security concerns continue to be the number one barrier for enterprise cloud adoption. Cloud security concerns range from securely configuring virtual machines deployed on an IaaS platform to managing user privileges in a PaaS cloud.

Given that the cloud services can be delivered in many flavors i.e. in any combination of service delivery models, SaaS, PaaS and IaaS (SPI), and operational models, public, private and hybrid, the cloud security concerns and solutions are context (pattern) dependent. Hence, the solution architecture should match these concerns and build security safeguards (controls) into the cloud application architecture.

So what are the architectural frameworks and tools that cloud application architects and devops have at their disposal when developing applications for IaaS and PaaS platforms? In this article, I'll discuss the approach to baking "adequate" security into your application deployed in IaaS and PaaS Clouds .

3. COMMON CONCERNS ABOUT CLOUD SECURITY AND IMPLICATIONS

We divide the common security issues around cloud computing across four main categories:

a) Cloud infrastructure, platform and hosted code. This comprises concerns related to possible virtualization, storage and networking vulnerabilities. We cover vulnerabilities that may be inherent in the cloud software platform stack and hosted code, which gets migrated to cloud. We also discuss the physical data- center security aspects here.

b) Data. This category comprises the concerns around data integrity, data lock in, data reminisce, provenance, and data confidentiality and user privacy specific concerns.

c) Access. This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.

d) Compliance. Because of its size and disruptive influence, cloud is attracting attention

from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

We believe that through this categorization we cover almost all common cloud security issues. To provide a perspective on why these issues are important; from cloud consumer (enterprises), providers, and third party points of view; we first lay out the paramount top-level security concerns (mainly on part of consumers and third party agencies) and sub-levels thereof with anecdotal evidences. We then discuss the technological implications (mainly on part of the cloud providers) of each of these concerns and related research issues. We defer discussion on some of the "cloud specific" advance research discussion to the next section.

Enterprise customers looking at public and hybrid clouds are generally accustomed to elaborate security arrangements in their data centers in forms of single sign-on technologies, identity management, and VLAN to separate different customer domains, storage appliances, VPN technologies etc. These provide a strong infrastructure for role-based access, logical partitioning of networks, controlled data and application, secure remote access etc. The situation with cloud gets fuzzy.

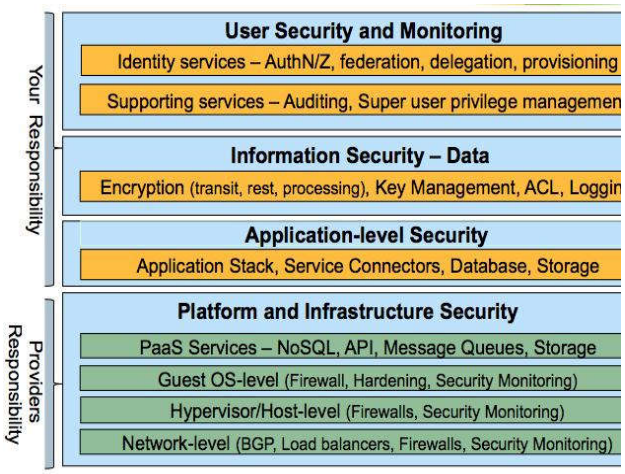

Figure 2. Layers, within a cloud service, that are secured by the provider versus the customer.

First, let's talk about the cloud security operational model. By definition, cloud security responsibilities in a public cloud are shared between the cloud customer (your enterprise) and the cloud service provider where as in a private cloud, the customer is managing all aspects of the cloud platform. Cloud service providers are responsible for securing the shared infrastructure including routers, switches, load balancers, firewalls, hypervisors, storage networks, management consoles, DNS, directory services and cloud API.

Prior to signing up with a provider, it is important to perform a gap analysis on the cloud service capabilities. This exercise should benchmark the cloud platform's maturity, transparency, compliance with enterprise security standards (e.g. ISO 27001) and regulatory standards such as PCI DSS, HIPAA and SOX. Cloud security maturity models can help accelerate the migration strategy of applications to the cloud. The following are a set of principles you can apply when evaluating a cloud service provider's security maturity:

- **Disclosure of security policies, compliance and practices**: The cloud service provider should demonstrate compliance with industry standard frameworks such as ISO 27001, SS 16 and CSA Cloud controls matrix. Controls certified by the provider should match control expectations from your enterprise data protection standard standpoint. When cloud services are certified for ISO 27001 or SSAE 16, the scope of controls should be disclosed. Clouds that host regulated data must meet compliance requirements such as PCI DSS, Sarbanes-Oxley and HIPAA.
- **Disclosure when mandated:** The cloud service provider should disclose relevant data when disclosure is imperative due to legal or regulatory needs.
- **Security architecture: The** cloud service provider should disclose security architectural details that either help or hinder security management as per the enterprise standard. For example, the architecture of virtualization that guarantees isolation between tenants should be disclosed.

- **Security Automation – The** cloud service provider should support security automation by publishing API(s) (HTTP/SOAP) that support:

1. Export and import of security event logs, change management logs, user entitlements (privileges), user profiles, firewall policies, access logs in a XML or enterprise log standard format.
2. Continuous security monitoring including support for emerging standards such as Cloud Audit.
3. **Governance and Security responsibility:** Governance and security management responsibilities of the customer versus those of the cloud provider should be clearly articulated.

3.1 Cloud Security Threats and Mitigation

Does cloud computing exacerbate security threats to your application? Which emerging threats are relevant? Which traditional threats are amplified or muted? Answers to these questions are dependent on the combination of cloud service deployment and operational models in play. The following table illustrates the dependencies which should be taken into consideration when architecting security controls into applications for cloud deployments:

3.2 Cloud Security Architecture Patterns

Architecting appropriate security controls that protect the CIA of information in the cloud can mitigate cloud security threats. Security controls can be delivered as a service (Security-as-a-Service) by the provider or by the enterprise or by a 3rd party provider. Security architectural patterns are typically expressed from the point of security controls (safeguards) – technology and processes. These security controls and the service location (enterprise, cloud provider, 3rd party) should be highlighted in the security patterns.

Security architecture patterns serve as the North Star and can accelerate application migration to clouds while managing the security risks. In addition, cloud security architecture patterns should highlight the trust boundary between various services and components deployed at cloud services. These patterns should also point out standard interfaces, security protocols (SSL, TLS, IPSEC, LDAPS, SFTP, SSH, SCP, SAML, OAuth, Tacacs, OCSP, etc.) and mechanisms available for authentication, token management, authorization, encryption methods (hash, symmetric, asymmetric), encryption algorithms (Triple DES, 128-bit AES, Blowfish, RSA, etc.), security event logging, source-of-truth for policies and user attributes and coupling models (tight or loose).Finally the patterns should be leveraged to create security checklists that need to be automated by configuration management tools like puppet.

In general, patterns should highlight the following attributes (but not limited to) for each of the security services consumed by the cloud application:

- **Logical location** – Native to cloud service, in-house, third party cloud. The location may have an implication on the performance, availability, firewall policy as well as governance of the service.
- **Protocol** – What protocol(s) are used to invoke the service? For example REST with X.509 certificates for service requests.
- **Service function** – What is the function of the service? For example encryption of the artifact, logging, authentication and machine finger printing.
- **Input/Output** – What are the inputs, including methods to the controls, and outputs from the security service? For example, Input = XML doc and Output =XML doc with encrypted attributes.
- **Control description** – What security control does the security service offer? For example, protection of information confidentiality at rest, authentication of user and authentication of application.
- **Actor** – Who are the users of this service? For example, End point, End

user, Enterprise administrator, IT auditor and Architect.

Here is a subset of the cloud security architecture pattern published by open security.

4. STEPS TOWARDS AN SECURITY ASSESSMENT FRAMEWORK

With such a wide spectrum of concerns, an enterprise has to be very careful in assessing potential security threats to its applications on a cloud. A three step approach will help in rigorous security assessment:

Step 1: Characterize the application's security requirements: Each application has different security requirement. E.g. security requirements for an e-commerce portal hosted on an IaaS are quite different from a hybrid cloud scenario where a cloud-hosted data analytics application interacts with data behind the enterprise firewall. It is important to identify if the current application requires compliance to domain-specific security and data protection policies like HIPPA, SAS 70 etc. Further, one should determine if the application requires a fully encrypted communication and if the application"s interaction with other applications (cloud hosted or on-premises) requires secure communication (e.g. HTTPS / SSL). Furthermore, the use Single Sign-on using SAML or non-SAML techniques need to be determined. Security requirements become stringent when applications require role-based access, particularly in a multi-cloud scenario or a hybrid cloud scenario. Access modes to the application characteristics – whether web, mobile, or mixed – also determine the additional security protocols the application needs to support. It is important to perform a security vulnerability analysis of the application to identify security loopholes. In a typical web-application, one should assess all three tiers – web application tier assessment for loopholes in CGI scripts, HTML/JSP/JavaScript loopholes etc., source code analysis of the business tier and database security assessment. For example, clear-text passwords and configuration files, often overlooked in secure enterprise computing, should be avoided in cloud.

Step 2: Characterize and review cloud provider's security strengths and vulnerabilities: Based on a mix of techno-commercial factors, the enterprise can decide on various cloud environments – IaaS, PaaS and SaaS – for potential hosting of applications. In selection of the cloud environment, security becomes an important factor. Similar to Step 1, it is essential to characterize provider"s security offering. In doing so, it is good to perform an in-depth security analysis across infra and platform, data, and access layers of the provider; on concerns depicted in section 2 of this paper. Such an analysis can be done by going through published documentation (security controls, protocol compliance and standard operating procedures) or by employing services of commercial / open-source cloud auditing agencies (such as *http://www.cloudaudit.org)*. Further, published audit reports and case studies, if available, provide an analysis of the provider"s „on-ground" adherence to security best-practices and techniques. One also needs to keep the local cyber-security and data location laws in mind. Cloud Security Alliance has also created a cloud Governance, Risk Management and Compliance (GRC) toolkit, supported by checklists and questionnaire, for cloud migration audit.

Step 3: Map application's security characteristics and cloud security characteristics to perform a fit analysis: Once the application and cloud provider assessments are performed, a fit analysis can be done to determine the best cloud-services provider for an application or class of applications from a security perspective. For enterprises that publish applications to cloud, as well as for the cloud providers, protocols like Security Control Automation Protocol (SCAP), promoted by NIST [39], should be a good choice for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities.

5. Conclusion

By understanding what you can leverage from your cloud platform or service provider, one can build security into your application without reinventing the capability within your application boundary thus avoiding costly "bolt-on" safeguards. A good practice is to create security principles and architectural patterns that can be leveraged in the design phase. Architectural patterns can help articulate where controls are enforced (Cloud versus third party versus enterprise) during the design phase so appropriate security controls are baked into the application design. Keep in mind the relevant threats and the principle of "risk appropriate" when creating cloud security patterns. Ultimately a cloud security architecture should support the developer's needs to protect the confidentiality, integrity and availability of data processed and stored in the cloud.

6. REFERENCES

[1] Amazon Elastic Compute Cloud web services at *http://aws.amazon.com/ec2*

[2] SalesForce Force.com Platform as a service at *http://developer.force.com*

[3] NetSuite SaaS portal at *http://www.netsuite.com*

[4] Gartner DataQuest Forecast on Public Cloud Services DocID G00200833, June 2, 2010

[5] Chow,R.,Gotlle,P.,Jakobsson, E.S.,Staddon,J., Masuoka,R., and Molina,J.;2009, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009

[6] Gellman, R., Privacy in the Cloud: Risks to Privacy and Confidentiality in Cloud Computing. *Technical Report prepared for World Privacy Forum*, 2009

[7] Novell Inc. survey on cloud computing, *http://www.novell.com/news/press/novell-survey-reveals-widespread-and-accelerating-enterprise-adoption-of-private-clouds*

[8] Telecommunication Industry Association, TIA-942: Data Center Standards Overview at *http://tiaonline.org*

[9] Carpenter, M., Liston, t., and Skoudis, E, Hiding Virtualization from Attackers and Malware. *IEEE Security and Privacy Magazine,* 2007

[10] Ristenport, T., Tromer, E., Shacham, H., and Savage, S., Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of the 16th ACM conference on Computer and Communication Security*, 2009

[11] MIT Exo-kernel operating system. Documentation at *http://pdos.csail.mit.edu/exo.html*

[12] Czajkowski, G., Application Isolation in the Java Virtual Machine. *ACM SIGPLAN Notices, vol 35, issue 10*. Oct 2000

[13] M. Jensen, N. Gruschka, and R. Herkenh¨oner, A survey of attacks on web services, *Computer Science Research and Development (CSRD)*, *Springer Berlin/Heidelberg*. 2009.

[14] Google Gears at *http://gears.google.com*

[15]*http://www.zdnet.com/blog/projectfailures/mediamax-the-linkup-when-the-cloud-fails/999*

[16] IBM Homomorphic Encryption research page at *http://domino.research.ibm.com/comm/research_projects.nsf/pages/security.homoenc.html*

[17] Plank, J.S., Erasure codes for Storage Applications,Tutorial given at *FAST-2005: 4th Usenix Conference on File and Storage Technologies* San Francisco, CA. December, 2005

[18] Zhong, S., Yang, Z., and Wright, R., Privacy-Enhancing *k* – anonymization of Customer Data, *Proceedings of the 24th ACM Symposium on Principles of Databases.* 2005

[19] Storage Network Industry Alliance at *http://www.snia.org*

[20] Cloud Security Alliance at *http://www.cloudsecurityalliance.org*

[21] OpenID foundation website at *http://www.openid.net*

[22]*http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf*

[23] *http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf*

[24] *http://ciocoo.com/clouds-and-data-jurisdiction-282*