RISKS, CHALLENGES, AND MITIGATION STRATEGIES IN CLOUD COMPUTING

Alpana M. Desai, Computer Information Systems, University of Alaska Anchorage, 3211 Providence Dr., Anchorage AK 99508, 907-786-4111, afamd@uaa.alaska.edu
Kenrick Mock, Computer Science, University of Alaska Anchorage, 3211 Providence Dr., Anchorage AK 99508, 907-786-1956, kjmock@uaa.alaska.edu

ABSTRACT

Many organizations have recently turned to cloud computing because of its ability to make flexible tradeoffs between cost and performance. However, IT executives cite security as the top concern for the adoption of cloud computing [5][9]. Enterprise organizations that intend to utilize cloud services must understand the security and privacy risks involved. This paper discusses the technical, legal, and organizational security risks of cloud computing along with strategies to mitigate these risks.

INTRODUCTION

Enterprises utilize cloud services for their infrastructure, platform, and/or software needs. Cloud computing has many benefit for customers. Deployment is simple, cost scales with performance and capacity, and fewer in-house IT staff and resources are needed. In light of these benefits, it is important for IT managers to understand the risks associated with cloud computing. Some of the technical security risks we discuss include insecure interfaces and APIs, risks associated with multi-tenancy, data leakage, malicious insider, and data protection risks. We also examine legal and organizational security risks such as data ownership and accountability, compliance risks, and customer lock-in issues.

RISKS AND CHALLENGES IN CLOUD COMPUTING

In this paper we discuss high security risks that need to be considered when enterprises plan to utilize cloud services for their infrastructure, platform, and/or software needs. The technical, organizational, and legal security risks of cloud computing will also be discussed. We also discuss specific strategies that can be used to alleviate security risks that occur in traditional environments as well as in cloud environments.

Technical Risks

APIs: Internet-accessible cloud interfaces and Application Programming Interfaces (APIs) are used to provision, manage, and monitor processes running in the cloud environment. Two categories of web-accessible APIs are used by cloud service providers: SOAP (based on web services) and REST (based on HTTP). REST-style APIs are prime targets for man-in-the-middle or replay attacks but some cloud providers offer these since they allow for rapid development. To prevent security breaches due to this threat experts recommend (1) a security model analysis of cloud APIs, (2) strong authentication, access controls, encryption and activity monitoring mechanisms, and (3) API dependency chain evaluation [4]. Many efforts are being made to develop open and proprietary APIs. Open API efforts are underway by the Open Cloud Computing Interface Working Group, Oracle's Open Cloud, and VMware's DMTF-submitted vCloud. Proprietary APIs include Amazon EC2, Rackspace, and GoGrid. DMTF's Open Virtualization Format (OVF) is being developed to help with portability and interoperability issues.

Multi-tenancy: A tenant is an application or service running on a cloud that requires its own exclusive environment. Multiple tenants may be initiated by multiple users or possibly multiple enterprises. To make multi-tenancy possible, physical resources are shared among tenants through common software virtualization layers. A virtualization hypervisor provides access between users' operating systems and physical compute resources. Strict isolation for multi-tenancy is not offered by the physical resources such as CPU caches, GPUs, etc. that make up the infrastructure. These shared environments propagate security risks if inappropriate access is allowed to the underlying platform. Cloud users' neighbor's virtual machine could be malicious as they are not aware of whom they are sharing their physical resources with and what their intentions are. Negligent access management or malicious attack can compromise data since common storage hardware is used to house different cloud consumers' data. For example, researchers disclose the possibility of a side-channel attack in a cloud environment where an attacker could insert malicious code into a neighbor's VM environment with minimal chance of detection [14].

A defense in depth strategy that should include compute, storage, and network security enforcement and monitoring is recommended by the Cloud Security Alliance [4]. The Cloud Security Alliance also recommends implementation and enforcement of best practices for installation and configuration. Cloud environment must be monitored for unauthorized changes and activities. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers' access to any other tenant's actual or residual data, network traffic, etc. should not be allowed. Strong authentication and access control for administrative access and operations must be promoted. Service level agreements for patching and vulnerability remediation must be enforced. Timely and scheduled vulnerability scanning and configuration audits must be conducted.

Data leakage and remanence: When cloud service providers recycle storage resources there is no clear standard on how to recycle memory or disk space [15]. If the hardware resources are not properly cleaned there is a high risk of misuse as previous tenants' data could still be accessible to new tenants. Data deletion is more problematic in clouds due to multi-tenancy. Cloud customers must insist on contractual provisions that clearly outline the standards and guidelines used by cloud providers for data deletion to safeguard their interests.

Malicious insider: A malicious insider is a general threat but it is amplified for cloud services because of the general lack of transparency of procedures and processes of cloud providers. The provider's guidelines on employee monitoring and organizational policy compliance may be deficient or unknown to the customer. Remediation steps include enforcing transparency into overall information and management practices and specifying human resource requirements as part of legal contracts [4].

Legal Risks

Data protection: Cloud computing causes several data privacy and data confidentiality risks for cloud customers and providers. Cloud providers may not be practicing secure and safe data handling and may not have proper data controls in place. Inversely, cloud providers may not be aware if data collected by a customer was done in a lawful manner. Strategies to minimize data protection risks include implementing strong API access control, encrypting and protecting integrity of data, and contract stipulations pertaining to lawful data collection on the part of the customer and secure data handling practices on the part of the cloud provider.

Data ownership and accountability: Legal complications arise due to the mobile nature of data residing in clouds. Data may be replicated and stored virtually anywhere. The European Union Data Protection Directive, officially Directive 95/46/EC, requires that user data be kept secure, be used only for the purpose stated, that users be given notice when data is collected, data is not disclosed without user consent, users be allowed to access their data, and that data collectors be accountable. The United States does not have such strong privacy regulations. As a result, an organization may be in violation of the directive if data crosses international boundaries. US companies can do business with the EU if they adhere to Safe Harbor Privacy Principles which includes the principles of Directive 95/46/EC [6].

Policy and Organizational Risks

Compliance: Organizations that have earned certifications to either meet industry standards or regulatory requirements or to gain competitive edge are at risk when migrating to clouds if the cloud provider does not adhere to their own compliance requirements and if the cloud provider does not allow audit by the cloud customer [5].

Customer portability and lock-in: Customers face lock-in issues when they are unable to move their data and/or processes away from the cloud provider [3]. Cloud customers face major portability challenges when they have to change their cloud service provider. Evolving standards and procedures for data and service portability exacerbate portability challenges. Customers become vulnerable to price increases, reliability issues, acquisition of providers, or when providers go out of business. Different types of cloud services (IaaS, PaaS, HaaS, or SaaS) create different lock-in challenges. SaaS lock-in affects both data and application. If the provider does not offer a routine or process for data migration, the customer has to develop programs to export data and import it to the new provider. Providers have customized applications and if a customer has a large user base it can incur very high switching costs [5]. PaaS lock-in occurs at the API and component levels. It is the customer’s responsibility to develop compatible code that uses the provider’s custom APIs since different providers offer different APIs. IaaS lock-in occurs at the application and data levels. Migration between providers is a major concern due to lack of portability standards.

GENERAL MITIGATION STRATEGIES FOR MANAGEMENT OF SECURITY RISKS

Organizations should evaluate and classify the importance of their assets. Assets could be data and/or applications, functions, and processes. Organizations must assess the confidentiality, integrity, and availability (CIA) for their assets and if that asset is moved to the cloud how the CIA are affected for these assets. It is imperative to determine the specific cloud deployment option that will be pertinent for any particular asset. It may be a good strategy for highly sensitive data to reside in a private cloud.

A set of key recommendations published by ENISA can be used by cloud customers and cloud providers [5]. A set of assurance criteria that should be used to determine risks associated with the adoption of cloud services, to compare and evaluate various offers by cloud providers, to obtain assurance from cloud providers, and to reduce the assurance burden on cloud providers is recommended by ENISA. The information assurance requirements and checklist must contain questions that evaluate (a) personnel security, (b) supply-chain assurance, (c) operational security, (d) identity and access management, (e) asset management, (f) data and services portability, (g) business continuity management, (h) physical security, (i) environmental controls, and (j) legal requirements. In addition, cloud customers need to pay special attention to data protection, data security, data transfer, intellectual property, confidentiality, and non-disclosure when assessing the service level agreements.

VENDOR STRATEGIES TO MITIGATE SECURITY RISKS

Cloud vendors are implementing a number of approaches to allay customer concerns. Most of these approaches apply to IT security in general, although some are specific to cloud computing.

Standards and Statutes

A common strategy to convey system security is to obtain certification or accreditation in known security standards. For example, vendors that process credit cards are required to meet the Payment Card Industry Data Security Standard (PCI DSS) [13]. Certification requires the vendor to demonstrate their network is secure, that steps are in place to protect cardholder data, and that an information security policy is in place with at least 128 bit security measures. Cloud vendors can go a step further and become a PCI validated service provider, which means that the vendor has been audited by an independent Qualified Security Assessor. PCI DSS is designed around the security of payment card transactions. More generally, many vendors seek ISO/IEC 27001 certification which covers more general information security principles and practices [10]. Certified companies can claim to have implemented a systematic, comprehensive, and holistic security management program that includes planning and regular security assessment.

Several cloud vendors have also announced compliance with regulatory statutes such as HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes–Oxley Act), or attestations with SAS 70 (Statement on Auditing Standards No. 70). For example, HIPAA's privacy rule prohibits the unencrypted transmission of protected health information while HIPAA's security rule requires controls to access protected health information. SAS 70 provides guidance for an auditor to assess the internal controls of an organization. The SAS 70 audit attests that the controls are in place for effective financial reporting, such as those specified by SOX. However, the SAS 70 report is not proof of security or compliance, although some vendors mischaracterize it as a security certificate [7].

The National Institute of Standards and Technology (NIST) publishes a set of security recommendations which cloud vendors may implement, especially if there is the intent to host federal applications. NIST 800-53, "Recommended Security Controls for Federal Information Systems," documents baseline security controls and processes [11]. For example, processes include auditable events, contingency plans, and procedures to update security controls. Terremark is one cloud vendor that has specifically designed their multi-tenant environment to meet federal regulations up to the Top Secret level. To achieve this level their Culpepper data center includes over 250 motion sensitive cameras; Department of Defense approved fences, blast-proof exteriors, multi-factor authentication, and 128 bit encryption [8]. Some cloud vendors also offer to host private clouds on dedicated hardware at the customer's site, although this arrangement limits the on-demand scalability aspect of the cloud computing model.

Common Security Practices

In terms of specific security practices and controls, virtually all cloud vendors offer basic packages of firewalls, VPN tunnels, VLAN access, and full data encryption. Some vendors offer additional security based on one-time tokens or hardware keys. For example, Fujitsu's cloud service offers one-time passwords provided via SMS [12] while Amazon's EC2 supports multi-factor authentication with the option to require a hardware device in addition to standard login credentials [1]. For authentication exchange between security domains, both the Security Assertion Markup Language (SAML) and WS-Federation are being promoted. Access control and authentication are central components to any security architecture, and this is one area where cloud vendors offer different approaches. For example, Fujitsu plans to utilize open ID management frameworks [12] while Windows Azure's access control use claims-based authentication issued by identify providers (active directory, Facebook, Google, etc.).

Customer education is an integral component to a secure cloud platform. Customers must know how to securely access and utilize cloud services. As a result, many cloud vendors publish white papers describing their security architecture. Amazon's white paper describes multiple levels of security. Multi-factor authentication is required to access the host and SSH2 to access the guest operating system. Amazon's customized hypervisor isolates different customer instances on a virtual machine (VM) to ensure that each customer has access only to their virtual memory and virtual disk [1]. Documentation is also provided for customers to develop applications securely. Amazon's SimpleDB provides domain level access controls for authenticated users. The RDS service allows customers to easily build relational databases and the SQS service supports messaging. By providing these services with appropriate security controls, Amazon PaaS applications transparently enforce security constraints to authenticated user accounts.

Auditing and Security Monitoring Tools

Customers' security concerns are addressed by cloud vendors by providing audits and regular security reports. At the request of the user, Amazon Web Services will conduct penetration testing. Tools also exist to help customers visualize their cloud security and provide regular security reports. Visualization tools can depict the efficiency and security coverage in terms of requirements met, measures in place, or highlight suspicious activity. For example, ArcSight's security monitoring tools analyze and correlate events such as logins, file accesses, database queries, etc. to find security risks or compliance violations and summarize them in an understandable report [2].

Expertise in Security

Finally, although the cloud computing model brings with it new security concerns, there is a strong argument that overall security is increased as more customers adopt the cloud model. It is very easy for businesses to put a web application online using their own host with little regard to security, maintenance, or audit tracking. Moving these hosts to a cloud service provider consolidates customers under an umbrella that is presumably maintained by security experts with considerable resources devoted to security and privacy issues.

CONCLUSION AND FUTURE DIRECTIONS

The focus and objective of this paper is to discuss the most critical security risks to cloud computing and to present mitigation strategies that are used to manage security challenges in cloud computing. Technical risks include insecure interfaces, multi-tenancy, data leakage, and malicious insiders. Special care must be taken on behalf of the vendor and customer to address cloud specific risks such as multi-tenancy. Legal risks include data protection, data ownership, and accountability. Strong data handling practices and conformance to laws and regulations such as the EU Privacy Act must be considered. Many of these risks can be mitigated by adopting common information security principles such as defense in depth, access controls, encryption techniques, and auditing tools. Policy and organizational risks include compliance and lock-in issues. Lock-in is particularly problematic as vendors have already introduced proprietary architectures and portability standards are lacking. While cloud vendors are addressing security concerns, there is still great variation in the depth, breadth, and implementation of security measures. Standards related to cloud computing are mostly nonexistent or in draft form.

The efforts of the Trusted Computing Group (TCG) may also have a significant influence on cloud security in the future. The TCG is an initiative with the backing of large technology firms that aims to create hardware meeting the Trusted Platform Module (TPM) specification. The TPM supports machine authentication, which secures data via encryption and enables attestation at a hardware level. Attestation is particularly relevant to cloud computing security because it provides a secure report on what is running on a machine and could be used to detect malware or to provide hardware-based verification that the hypervisor is properly separating tenants [16].

REFERENCES

[1] Amazon.com. (2010, 8). *Amazon Web Services Overview of Security Processes whitepaper* . Retrieved 12 27, 2010, from AWS Security Center: http://aws.amazon.com/security

[2] ArcSight. (n.d.). *ArcSight - Protect Your Business*. Retrieved 12 28, 2010, from http://www.arcsight.com

[3] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., et al. (2009). *Above the Clouds: A Berkeley view of cloud computing.* Retrieved March 15, 2011, from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[4] Cloud Security Alliance. (2010). *Top Threats to Cloud Computing V1.0.*

[5] ENISA. (2009). *Cloud computing: benefits, risks and recommendations for information security.*

[6] EU Directive. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[7] Gartner. (2010, 6 25). *SAS 70 Is Not Proof of Security, Continuity or Privacy Compliance.* Retrieved 12 28, 2010, from http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1390444

[8] Hoover, J. N. (2009, July 28). Inside Terremark's Secure Government Data Center. *Information Week.*

[9] IDC. (2010, July 1). *IDC's Public IT Cloud Services Forecast: New Numbers, Same Disruptive Story.* Retrieved 4 2, 2011, from IDC eXchange: http://blogs.idc.com/ie/?p=730

[10] International Organization for Standards. (2008). *ISO/IEC 27001:2005.*

[11] NIST. (2007, 7 3). *NIST, Computer Security Division, Computer Security Resource Center*. Retrieved 12 27, 2010, from http://csrc.nist.gov/publications/PubsSPs.html

[12] Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security Architectures for Cloud Computing. *Fujitsu Scientific and Technical Journal , 46* (4), 397-402.

[13] PCI Security Standards Council. (2010). *PCI DSS v2.0.*

[14] Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Part Compute Clouds. CCS 2009: *Proceedings of the 2009 Conference on Computer and Communications Security*. ACM.

[15] Trend Micro. (2010). *Addressing Data Security Challenges in the Cloud.*

[16] Trusted Computing Group. (2010). Cloud Computing and Security – A Natural Match. Retrieved 9 11, 2011, from http://tinyurl.com/48ulgyg