ABHINAV
International Monthly Refereed Journal of Research In Management & Technology
ISSN – 2320-0073 Volume II, June'13

CLOUD COMPUTING, SECURITY IMPLICATIONS AND BEST PRACTICES

Snehlata Kothari[1] and Dr. Sanjay Gaur[2]

[1]Assistant Professor (FCA), Pacific University, Udaipur, India
Email: skothariudr@gmail.com
[2]Associate Professor and Coordinator of FCA, Pacific University, Udaipur, India

ABSTRACT

Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. In this paper we assess how can cloud providers earn their customers' trust and provide the security, privacy and reliability, when a third party is processing sensitive data in a remote machine located in various countries? A concept of utility cloud has been represented to provide the various services to the users. Emerging technologies can help address the challenges of Security, Privacy and Trust in cloud computing. While the economic case for cloud computing is compelling, the security challenges it poses are equally striking. In this work we strive to frame the full space of cloud-computing security issues, attempting to separate justified concerns from possible over-reactions.

Keywords: Cloud Computing, Utility computing, Risk Management, Access Control Model, Quality Assurance.

What Is Cloud Computing?

Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices. Cloud infrastructure can reside within the company's datacenters (as internal clouds or on-premise solutions) or on external cloud computing resources (off-premise solutions available through service providers). It encompasses any subscription- based or pay-per-use service that extends existing IT capabilities.

Typically, Clouds utilize a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed (also referred to as utility computing). By design, cloud computing is scalable, flexible and elastic –offering IT staff a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software.

Different Types of Cloud Computing

Companies can leverage cloud computing for access to software, development platforms and physical hardware. These assets become virtualized and available as a service from the host:

1. Application and Information clouds – Sometimes referred to as Software-as-a-Service (SAAS), this type of cloud is referring to a business-level service. Typically available over the public Internet, these clouds are information-based.
2. Development clouds – Sometimes referred to as Platform-as-a-Service (PAAS), cloud development platforms enable application authoring and provide runtime environments without hardware investment.
3. Infrastructure clouds – Also referred to as Infrastructure-as-a-Service (IAAS), this type of cloud enables IT infrastructure to be deployed and used via remote access and made available on an elastic basis.

Cloud Computing Benefits

Cloud computing is enabling the enterprise to:

Expand scalability – By utilizing cloud computing, IT staff can quickly meet changing user loads without having to engineer for peak loads.

Lower infrastructure costs – With external clouds, customers do not own the infrastructure. This enables enterprises to eliminate capital expenditures and consume resources as a service, paying only for what they use. Clouds enable IT departments to save on application implementation, maintenance and security costs, while benefiting from the economies of scale a cloud can offer compared to even a large company network.

Increase utilization – By sharing computing power between multiple clients, cloud computing can increase utilization rates, further reducing IT infrastructure costs.

Improve end-user productivity – With cloud computing, users can access systems, regardless of their location or what device they are using (e.g., PCs, laptops, etc.).

Improve reliability – Cloud computing can cost-effectively provide multiple redundant sites, facilitating business continuity and disaster recovery scenarios.

Increase security – Due to centralization of data and increased security-focused resources from cloud computing providers, cloud computing can enhance data security. Cloud computing can also relieve an IT organization from routine tasks, including backup and recovery. External cloud service providers typically have more infrastructure to handle data security than the average small to midsize business.

Gain access to more sophisticated applications – External clouds can offer CRM and other advanced tools that were previously out of reach for many businesses with smaller IT budgets.

Downsize the IT department – By moving applications out to a cloud, IT departments can reduce the number of application administrators needed for deployment, maintenance and updates. It departments can then reassign key IT personnel to more strategic tasks.

Save energy – Going "green" is a key focus for many enterprises. Clouds help IT organizations reduce power, cooling and space usage to help the enterprise create environmentally responsible datacenters.

Challenges Of Existing Cloud Computing Solutions

Like any new trend or technology, we must address some challenges that cloud computing poses before we can recognize its full value. These include:

A lack of interoperability – The absence of standardization across cloud computing platforms creates unnecessary complexity and results in high switching costs. Each compute cloud vendor has a different application model, many of which are proprietary, vertically integrated stacks that limit platform choice. Customers don't want to be locked into a single provider and are often reluctant to relinquish control of their mission-critical applications to hosting service providers.

Application Compatibility – Most of the existing public compute clouds are not interoperable with existing applications and they limit the addressable market to those willing to write new applications from scratch.

Difficulty in meeting compliance regulations – Regulatory compliance requirements may limit the use of the shared infrastructure and utility model of external cloud computing for some environments. Achieving compliance often requires complete transparency of the underlying IT infrastructure that supports business-critical applications, while cloud computing by design places IT infrastructure into a 'black box' accessible only through well-defined interfaces. As a result, internal compute clouds may be a better solution for some applications that must meet stringent compliance requirements.

Inadequate security – By design, cloud vendors typically support multi-tenancy compute environments. IT managers must look for a balance between the security of an internal, dedicated infrastructure versus the improved economics of a shared cloud environment.

Research – cloud computing provides many securities but many issues the data are leak and hackers access the important data In our research paper we implement many new ideas to handle the situation the user cannot access the data and we safe to our policies and data threats or many policies we can implement to the purpose of data security.

Top seven security threats to cloud computing

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

Problem Statement

Name of attacks	Description
Repudiation	Sender tries to repudiate, or refute the validity of a statement or contract which is sent by him/her.
Replay Attack	A replay attack is defined as when an attacker or originator sends a valid data with intention to use it maliciously or fraudulently.
Differential Analysis Threat	When new versions are released, a differential analysis of the new and old version would indicate where differences in the code exist.
Viruses and Worms	Viruses and worms are very common and well known attacks. These are piece of code that decrease the performance of hardware and application even these malicious codes corrupts files on local file system
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.
Man-in-the-Middle Attack	This type of attack occurs when an attacks infiltrates the communication channel in order to monitor the communication and modify the messages for malicious purposes

These table 8shown below are used for protect the data and helpful to the cloud customers and companies –

Solution	Description
Data Handling Mechanism	• Classify the confidential Data. • Define the geographical region of data. • Define policies for data destruction.
Data Security Mitigation	• Encrypting personal data. • Avoid putting sensitive data in cloud.
Design for Policy	Fair information principles are applicable.
Accountability	• For businesses having data lost, leakage or privacy violation is catastrophic • Accountability needs in legal and technical. • Audit is need in every step to increase trust • All CSP make contractual agreements.

There Are Many Network Attacks to Damage Our Application

DNS Attacks

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed.

Sniffer Attacks

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured.

Issue of Reused IP Addresses

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user.

BGP Prefix Hijacking

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbors.

Application Level Security

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. Now a days, attacks are launched, being disguised as a trusted user and the system considering them as a trusted user, allow full access to the attacking party and gets victimized.

SUGGESTIONS

- URL to be displayed of the server and entered by the user; however the URL of database access should be different. This can be implemented by server side scripting.
- In the browser data should be displayed only.
  - No data could be copied by the user
  - Flash may be used to stop Web scrapping
  - To minimize screen scrapping, special types of fonts and background can be used.
- Any III Party tool or service should be executed by server side scripting and only output to be shown to the user.
- Minimum or no use of cookies and multiple time authentication, which accessing sensitive data.
- Log IP Address of a request and response in case any change found, make proper inquiry.
- Diskless computer systems may be used for client to avoid virus/malware.
- Assign static IP addresses instead of DHCP in client network

- Any up-gradation should be well tested before implementation.
- If the client could procure Static IP address for his Internet, then SaaS services may be bounded with that only.
- Protection against malware, spyware, viruses, etc.
- Public Key / Private Key and Certificate Server With encryption of data and transport level encryption.
- Firewall Protection
- Proper SLA
- **Bug Exploration Technique**: All bugs should be tracked in a log, immediately disconnect database (relation with SaaS), clear the session and its associated variables and then show a particular page with error detail. Ask client to note it down with date time. Reconciliation with the client for the bugs should be made at the end of the day or week.
- **Versioning of DB** : However is not possible due to fluent entries, that versioning of database could be maintained. But a log of actions with IP and user can be maintained.
- In any case, some level of auditing is obviously required. In the cloud scenario, one assumes it would be completed by the vendor's auditors with the results federated to yours. If every auditor is equally certified and follows the same rules -- which, in a perfect world, they do -- this federation of auditing could be considered valid fulfillment.
- VM monitoring is important to virtual security, because it can alert you about malicious resource usage. Reporting systems that profile typical resource usage for VMs are particularly helpful, so you will know when abnormal behavior occurs. By using VM monitoring in conjunction with scripting, you can impose resource restrictions, isolate the offending VMs and even power them off. With virtual security, the main task is to secure the virtual host's management console. Attackers that gain access to the console can then easily get into VMs that reside on the host.
- The management network should be isolated physically and virtually. The Cloud Provider should also create isolated virtual switches for the host management network, and never mix virtual-switch traffic with normal VM network traffic

CONCLUSION

Suggested Remedies of Few Problems Related To Security

- Password must be secure
- Stricter initial registration and validation processes.
- Web Password is same and the password is changed in automatically and user gets a message from your mobile.
- Enhanced credit card fraud monitoring and coordination.

- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.
- Analyze the security model of cloud provider interfaces.
- Microsoft azure and AWS and Google App Engine is provide cloud safely and security.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.
- Encrypt and protect integrity of data in transit.
- Analyze data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually specify provider backup and retention strategies.
- 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 SLA's.
- Disclosure of applicable logs and data.

REFERENCES

1. http://www.vmware.com/solutions/desktop/mobile.html.
2. Gansen Zhao Chunming Rong Jin Li Feng Zhang Yong Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers" in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Nov 30 – Dec 3, 2010, pp. 97-103.
3. Hyunjoo Kim, Parashar M., Foran D.J. and Lin Yang, "Investigating the use of autonomic cloudbursts for highthroughput medical image registration" in 2009 10th IEEE/ACM International Conference on Grid Computing (GRID 2009) , 2009.
4. Security and Economic Benefits of standardization for security as a service
5. Saaikala S., & Prema, S. (2010). Massive Centralized Cloud Computing (MCCC) Exploration Higher Education. Advances in Computer Sciences and Technology 111-118.
6. Jian Wang ,Yan Zhao ,Shuo Jiang and Jiajin Le, "Providing privacy preserving in Cloud computing", in 2009 International Conference on Test and Measurement, 2009,pp. 213-216.
7. Gansen Zhao Chunming Rong Jin Li Feng Zhang Yong Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers" in 2010 IEEE Second International Conference

on Cloud Computing Technology and Science (CloudCom), Nov 30 – Dec 3, 2010, pp. 97-103.

8. VMWARE, "The Open Virtual Machine Format – Whitepaper for OVF Specification", v0.9, 2007,
9. http://www.vmware.com/pdf/ovf whitepaper specification.pdf