ADDRESSING THE CLOUD COMPUTING SECURITY MENACE

Abha Thakral Sachdev[1], Mohit Bhansali[2]

[1] Assistant Professor,[2] Student, Department of Computer Science and Engineering, Amity University, Noida, India,
aabhathakral@yahoo.co.in, mohitbhansali@outlook.com

Abstract

Cloud Computing is fast gaining popularity today with its scalable, flexible and on-demand service provision. It brings cost saving and agility to organization with pay-as-you-go approach. Abundant resources are available and the user has a huge range to select from. Cloud facilitates virtualization, simplification, automation and accelerated delivery of application and services for a sustainable business advantage. As much as the technological benefit, cloud computing also has security issues. Security in cloud computing is essential for providing quality of service. In this paper we address security issues which concern cloud computing environment today. We analyze Cloud Computing and security menace it faces due to different threats.

Index Terms: *Cloud Computing, Cloud Service Provider (CSP), Cloud Security, Cloud User, SaaS, PaaS, IaaS, StaaS*

---***---

1. INTRODUCTION

Cloud Computing is the future generation in computation. It is a trope for the Internet. In Cloud Computing, all information, application and resources are handled in a virtual environment. It brings an open, standards-based architecture that maintains user choice and increases business value, substantially minimizing the managing effort and total cost of ownership. Cloud Computing involves virtual hosted environments allowing users to access the services being hosted over the Internet. It is a mode of computing in which IT-related potentialities are provided “as a service”. Cloud users can access technology-enabled services from the Internet without any prior knowledge of the technology that holds them. According to Cisco Global Cloud Index, Annual global cloud IP traffic will reach 4.3 zeta-bytes by the end of 2016. It will grow at a CAGR of 44 percent from 2011 to 2016 and account for nearly two-thirds of total data center traffic by 2016 [4].

Examples of Cloud Computing are Microsoft’s SkyDrive, Google Drive, dropbox.com, box.com etc. There is no need to have a server or any software to employ it. Internet connection is all that is required. The server and email management software is on the cloud and is totally managed by the cloud service provider (CSP) like Microsoft, Google, and Amazon etc. The user gets to use the services and enjoy the benefits. Cloud clearly has financial and operational benefits, but they have to be carefully weighed against the contradictory security concerns.

2. WHY CLOUD COMPUTING

Cloud Computing is more beneficial as compared to traditional computing. The major cloud providers such as Microsoft, Google, and Amazon are working on building the world’s largest data centers across the Globe. Each data center includes thousands of computer servers, substation power transformers and cooling equipment. For example, Microsoft’s data center in Quincy, Washington has 43,600 square meters of space and 965 kilometers of electric wire, uses 4.8 kilometers of chiller piping, 92,900 square meters of drywall and 1.5 metric tons of backup batteries. The company does not reveals the number of servers however it says that the data center consumes 48 megawatts which is adequate to power 40,000 homes [12]. As another example, the National Security Agency is planning to build a massive data center at Utah which is expected to take in 70 megawatts electricity. Hardware has been replaced by environment friendly Cloud Computing technology which reduces CO2 emissions. It benefits business through its huge infrastructure, as businesses do not have to directly implement or administer over it; its initial cost reduces the overall implementation and maintenance costs; it has comfort of backup system; it has mobility of information which can be easily use across globe; its IT resources enables scalability during the peak time and according to the needs of the user; its usage further adds to innovation because of its minimized huge upfront costs for test and development environments.

3. CHARACTERISTICS OF CLOUD COMPUTING

- The important characteristic of Cloud Computing is that it takes less IT skills for execution.
- In Cloud Computing, users access the data, applications or any other services with the help of a browser regardless of the device used and the user’s location. The infrastructure which is provided by a third-party is accessed with the aid of internet.
- Consistent service can be obtained by the use of various sites which is appropriate for business continuity and tragedy healing.

- Efficient operation of infrastructure takes place as the resources and costs are pooled among a large set of users.
- Maintenance is easier in case of Cloud Computing applications as they need not be installed on each user's computer.
- Pay per use service allows measuring the usage of application per cloud user on regular basis. User has to pay only for the resources he consumes.
- Performance can be monitored and thus it is scalable. Also, it has rapid elasticity i.e. cloud users can increase or decrease capacity on demand.

4. CLOUD COMPUTING – DEPLOYMENT AND DELIVERY MODELS

Cloud Computing can be classified and deployed in a number of ways i.e. public, private or hybrid clouds.

A. Public Cloud

Public Cloud are cloud services provided by third parties and hosted and managed by the service providers. It is also known as External Clouds. The cloud providers assume the responsibilities of installation, management, provisioning and maintenance. Users access and consume the services and IT resources. Users are charged only for the resources and services they use, following a pay-as-you-go approach. Major drawbacks are lack of appropriate security, reliability and regulatory compliance. Amazon.com is one of the largest public cloud providers.

B. Private Cloud

Private Cloud are proprietary networks, often data centres, residing within the enterprise for the exclusive use of the organization or for a known group of users. It is also known as Internal Clouds. A local or private network infrastructure is employed. Here, the enterprise is in charge of setting up and maintaining the cloud and thus the enterprise can take better control of all aspects of the provisioning and functioning. The added advantage is in terms of better control of security, more effective regulatory compliance and improved quality of service. For mission critical processes and for location of sensitive data, this type of cloud infrastructure provides much more privacy than a Public Cloud.

Private Clouds are, generally, Clouds that reside within the organization, however, private clouds, outside the organization, are also becoming a possibility, where the resources inside a Cloud are available only to the organization concerned and totally invisible to others.

When a service provider uses public cloud resources to create their private cloud, the result is a virtual private cloud. A Community Cloud is a semi-private cloud that is used by the defined group of tenants with shared backgrounds and requirements [2]. This, then, becomes a private cloud for this community, where the management responsibility is shared amongst the members of the community.

C. Hybrid Cloud

Hybrid Cloud are a combination of private and public clouds. Here, the management responsibilities are split between the enterprise and the public cloud providers, which can often become an issue of concern. For mission critical processes, this type of cloud infrastructure can also be highly effective because of enhanced control and management by the enterprise itself. For example, the organization can keep the sensitive data within the private cloud and the rest in the public cloud.

The Cloud model generally consists of three types of architecture which provide services, namely: Software Services, Platform Services, and Infrastructure Services. These are generally referred as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS), respectively [3].

Presenting the model as pyramid, the Software Services will be at the top and the Infrastructure Services will be the bottom of the pyramid. Based on this anatomy, the Cloud Services are often defined, as in the following sections and as shown in Figure below.

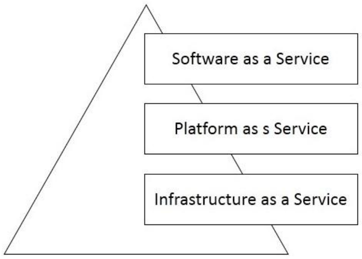

Fig -1: A 3-Layer Model of Cloud Computing

1) Software as a Service (SaaS)

This refers to prebuilt and vertically integrated applications (e.g. an email system, human resource management, payroll processing, database processing and other application processes) that are delivered to and purchased by users as services. Here, cloud users are looking to purchase functionality. Applications are normally designed for ease of use based on proven business models. This may be regarded as a user level layer and it can be further classified into: 1) Services (which are often standalone applications e.g. a billing service); and 2) Applications (which are often units of functionalities). SaaS is a very broad market where services can be anything from Web-based email to inventory control, even in some cases outline banking services, as well as database processing. Gmail, Hotmail, Quicken Online, IBM®Websphere, Boomi and SalesForce are some of the well-known SaaS products and providers.

2) Platform as a Service (PaaS)

This layer refers to software and product development tools (e.g. application servers, database servers, portal servers, middleware, etc.) which cloud user purchase so they can build and deploy their own applications, thus providing a much increased flexibility and control to the user. However, there may sometimes be a certain amount of dependence upon the infrastructure and platform providers. The services, here, are intended to support the 'software services' at top layer of the pyramid. The cloud users are looking to buy time and cost savings in deploying their applications. Typical offerings include runtime environment for application code, compute power, storage, and networking infrastructure. This level of services may be regarded as a developer level layer. The pricing structure is often along the lines of: compute usage per hour; data transfer per GB; I/O requests per million; storage per GB; data storage requests per thousand etc. All charges are per each billing period. Google App Engine, Heroku, Mosso and Engine Yard are examples of PaaS products and providers.

3) Infrastructure as a Service (IaaS)

This layer is essentially hardware (e.g. visualized servers, storage, network devices, etc.) and hardware services to enable Cloud Platforms and Applications to operate. These services support the 'software services' at top layer of the pyramid. Users get full control over server infrastructure and that sometimes comes with a price premium. Here, users are looking to buy 'computing', without making upfront investment. Since, the infrastructure is offered on a pay-for-what-you-see basis, it is sometimes referred to as utility computing, as there is similarity with the provision and use of services such as electricity and gas. The pricing structure is often similar to the provision for PaaS. Amazon EC2, IBM BlueHouse, VMWare, GoGrid, RightScale and Linode are some of the IaaS products and providers.

4) Storage as a Service (StaaS)

It facilitates cloud applications to scale beyond their limited servers. StaaS allows users to store their data at remote disks and access them anytime from any place.

Cloud storage systems are expected to meet several rigorous requirements for maintaining user's data and information, including high availability, reliability, performance, replication and data consistency; but because of the conflicting nature of these requirements, no user implements all of them together.

5) Other Provisions as a Service

The dividing line between the three layers as shown in Figure 1 is not clear and, in fact there is a considerable amount of overlap. For example, a software system may be considered as part of a software platform. It is for this reason that researchers have also discussed combined models such as: SaaS & PaaS; SaaS & IaaS; IaaS & PaaS; and even SaaS & PaaS & IaaS. Numerous other categories have also been suggested in recent years e.g.:

5.1 Database-as-a-Service
5.2 Security-as-a-Service
5.3 Communication-as-a-Service
5.4 Management/ Governance-as-a-Service
5.5 Integration-as-a-Service
5.6 Testing-as-a-Service
5.7 Business Process-as-a-Service

In this respect, any provision that is available and that provides support in some sense to the user is regarded as a 'service'. For an enterprise, it is not enough to have services available in the Cloud. There is, often, also a requirement of expertise available to help the enterprise to interface, sequence, and integrate the services with what already exists. So, Integration-as-a-Service or 'Solution-as-a-Service' can be particularly important service.

5. CLOUD SECURITY

Security concerns, which arise specifically due to virtualization, are common to all cloud models. As compared to Private Clouds, Public Clouds have additional security concerns which demand specific counter measures. This is because, in a Private Cloud, a cloud user has complete control over the resources and can enforce security policies. In Public and Hybrid Clouds, however, cloud users usually do not have that much control over the resources and therefore, enforcement of security mechanisms is comparatively difficult for them. For CSPs also, it is not easy to enforce all the security measures that meet the security needs of all the users, because different users may have different security demands based upon their objective of using the cloud services.

A. Multi Tenancy

Cloud services work on multi-tenancy model where the same resources are shared by multiple independent cloud users. Many times this would lead to a situation where competitors co-exist on the same cloud. Such an environment opens up a whole lot of possibility of data stealth. So, how can cloud user place sensitive information like personal details, bank details, passwords, keys etc. on the cloud?

From a CSP's perspective enforcing uniform security measures and controls is difficult as each user has different security demands. Each cloud user enters the cloud with its own objective of using a certain service. From the user's perspective, ensuring security is not possible as he does not have much access control.

To address this unwanted situation, isolation is a key remedy. This includes isolation of data, applications and virtual machines. Also CSP at no juncture should be allowed to make any changes to the cloud user's data.

B. Data Loss and Leakage

Data can be compromised in multiple ways. Access of sensitive data to unauthorized entities can expose it. Removal or modification of data without having backup can lead to its loss. Storage of data on unreliable media can make it vulnerable to multiple attacks, thereby compromising its integrity. Also if linked/indexed records are wrongly stored, blocks of orphan data will be generated. Such a loss leads to huge brand damage and existing users may also loose trust. This can lead to financial, legal and competitive implications.

To curb such situations, strong encryption algorithm must be applied for data in transit. Tough storage management procedures should be implemented. Stringent access control mechanism with sensitive data access notifications should be in place. Also best backup and retention strategies must be practised.

C. Easy Accessibility of Cloud

Cloud services are open for all to use. A simple registration model where anybody with a valid credit card can register and become a cloud user, open a world of opportunity for the wily minds. The anonymity model can serve as a beacon for malicious users who freely enter the cloud and can then attack innocent users. The attacks can range from password and sensitive data cracking to host overt and covert channels.

Rigorous registration model with stringent processes in place is required to prevent the occurrence of such attacks. Also attacking network addresses should be blacklisted and the list should be made public for others to save themselves from nefarious attackers.

D. Identity Management

Cloud Computing is uniting of multiple technologies coming together to satisfy the needs of diversified users through a labyrinth of services and software's. This requires Identity Management (IDM) for different technologies to inter-operate and function as a single entity in a shared landscape.

Thereby, IDM in cloud needs to be looked upon with a new eye, detached from traditional IDM's. Its concern areas are provisioning/de-provisioning, synchronization, entitlement, lifecycle management etc. Provisioning and de-provisioning means just-in-time or on-demand provisioning and de-provisioning. Just-in-time provisioning indicates the federation of user accounts without sharing prior data, based on some trust model. Real time de-provisioning of a user account has to synchronize instantaneously with all participating service providers.

Identity lifecycle management specifies what personal details can be edited by the users, their self-service components and delegation rules. Entitlement specifies access rights of authenticated security principal. Synchronization smoothens the movement and growth of Identity Management capabilities by enabling services that facilitate building of trust [11].

E. Unsafe API's

Application program interface is a set of routines and protocols describing how software components will communicate with each other. API is a user manual. Every CSP publishes its API for reference of cloud users while they are deploying their data on cloud. These are not only very useful from cloud user's perspective; but also can act as a great guiding tool for attackers. The architectural and design specification details mentioned in the API can be studied by attackers and then used to formulate shortcomings and flaws; which can then be exploited. Also, other vendors and third parties use these interfaces to build their own applications and provide value-added services to cloud users. This going further adds to complexity.

To avoid such an attack each API's dependency chain should be analysed. Unknown API dependencies and layering should be minimised. While designing API's, procedures to maintain confidentiality and integrity of data should be implied.

F. Service Level Agreement

Service Level Agreement is the legal document signed by CSP and cloud user defining their business relationship. It enlists the services to be delivered by the CSP, their evaluation criteria, tracking and compliance of offered services and legal measures to be taken in case of unsatisfactory performance. It should specify security mechanisms which will be deployed for ensuring his privacy; as data being placed in the cloud may be highly sensitive and of utmost importance to the user. Specifications of authentication, authorization and audit controls must be enlisted. Details of logging, patching and configuration hardening should be given. What level of recovery and backup will be provided in worst case scenarios should be given. Also how data will be erased in case of exit of user from the cloud should be mentioned as improper disposal may lead to undue exposure and exploitation of data.

G. Patch Management

A patch is a piece of code written to fix bugs, or update/enhance an existing computer program. This includes fixing security vulnerabilities and other errors, and improving its usability and performance. Patch management is the process of planning which patches should be applied where and how. It is an ongoing process, and becomes a vicious circle in case of poorly designed patches as a weak patch can introduce new bugs. Also, a carefully written patch applied today can introduce novel vulnerabilities which need to be addressed tomorrow. This becomes more critical in cloud environment which is being used 24*7, with no shutdown time. For example, Dropbox made a code update at 1:54pm Pacific time on 19th June, 2011, that introduced a bug affecting their authentication mechanism. Though its fix was made live after 5 minutes of its detection but still for around 4 hours an account could be opened without correct password [5]. Such dynamic vulnerability poses serious threat.

With huge number of users and applications residing in the public cloud, it becomes difficult for the CSP to ensure that all applications are working correctly after the latest patch update. So, the responsibility for patch management resides with the user. Still on CSP's end, bidirectional firewalls should be deployed. Firewalls should cover all IP protocols and network interfaces.

H. Internal Threats

Internal safe guarding is as important as external security. A cloud user has placed his confidential data on the cloud, with little or no control over it. CSP does not display transparency in term of its processes and procedures about recruiting of employees and their specialization and skills. Also there is no way to know what level of access control is given to CSP's employees handling this confidential information. A malicious mind in disguise of an employee can lead to accessing of confidential data, stealing it and passing it on to user's competitors. This results in sensitive information for the user being lost and brand damage for the CSP.

To curb this situation, there should be processes on CSP's end to detect and avoid internal attacks. A thorough and hierarchical access control mechanism should be applied for compliance by all the employees. Stronger credentials should replace usernames and passwords as the foundation of the access management system [9]. Multi-layer background check of newly hired employees should be conducted.

CONCLUSIONS

Cloud Computing predictions indicate significant growth in coming years. The global market for Cloud Computing is going to increase from about $41 billion in 2011 to $241 billion in 2020 [10]. Security is inevitable in cloud computing, given that all sensitive information is placed on the cloud by users. It will become a great business differentiator and the CSP's who provide and prove their secure space will only be able to flourish. With addressing major menace causing factors in this research paper, we can expect organizations to offer safer and secure services. It provides a clear reference for cloud users to evaluate CSP's on the basis of security provided.

REFERENCES:

[1]. ENISA, Cloud Computing: benefits, risk and recommendations for information security, [Online] Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport/

[2]. Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges, [Online] Available: http://www-03.ibm.com/press/us/en/pressrelease/22414.wss.

[3]. SearchCloudComputing, Definition – Cloud Computing; [Online] Available: http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[4]. Cisco, Cloud Index White Paper, [Online] Available: http://cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf

[5]. Dropbox Security Bug Made Passwords Optional for Four Hours (2011). [Online]. Available: http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/

[6]. Srinivasan, Madhan Kumar, et al. "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment." Proceedings of the International Conference on Advances in Computing, Communications and Informatics. ACM, 2012.

[7]. Cloud Security Alliance, Top Threats to Cloud Computing V1.0 (2010), [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v.1.0.pdf

[8]. Boampong, Philogene A., and Luay A. Wahsheh. "Different facets of security in the cloud." Proceedings of the 15th Communications and Networking Simulation Symposium. Society for Computer Simulation International, 2012.

[9]. Roger Halbheer, Chief Security Advisor, Public Sector, EMEA Doug Cavit, Principal Security Strategist Lead, Trustworthy Computing USA (2010), Cloud Computing Security Considerations [Online]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=1013.

[10]. The Wallstreet Journal, More Predictions on the Huge Growth of Cloud Computing, [Online]. Available: http://blogs.wsj.com/digits/2011/04/21/more-predictions-on-the-huge-growth-of-cloud-computing/

[11]. Gopalakrishnan, Anu. "Cloud computing identity management." SETLabs briefings 7.7 (2009): 45-54.

[12]. Katz, R.H.; , "Tech Titans Building Boom," Spectrum, IEEE , vol.46, no.2, pp.40-54, Feb. 2009

[13]. P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.