International Journal of Research
Available at https://edupediapublications.org/journals

E-ISSN: 2348-6848
P-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

Cloud Computing: A Security Issues in Cloud

Dr.B.Mahesh[1]

[1]*Associate Professor, Department of CSE, Malla Reddy Engineering College and Management Sciences,Telangana*
[1]mahesh.bhasutkar@gmail.com

***Abstract*—Cloud computing is the expansion of parallel computing, distributed computing, grid computing and virtualization technologies which define the nature of a new era. Cloud computing is an emerging model of business computing. It is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. In this paper, we explore the concept of cloud architecture. We also address the characteristics and applications of several popular cloud computing platforms. We aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. The major concern of cloud environment is security during upload the data on cloud server. Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party. The importance of third party is to prevent and control unauthorized access to data store to the cloud In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.**

***Keywords*—Cloud Computing, Cloud Server, Security, Data Protection, Service Models.**

I. Introduction

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. 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. According to the definition of[1], cloud computing is "it is a significant distributed computing model that is directed by financial prudence of balance, in which stake of isolate, fundamental, loading, podium in which a facilities are supplied as per the request of exterior foreign clients through the internet". There are some examples of cloud services like webmail, online file and business applications. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage [2] specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. The mechanism [2] model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform. There is a critical need to securely store, manage, share and analyse massive amounts of complex data to determine patterns and trends in order to improve the quality and safeguard the nation and explore alternative energy. Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore we need to safeguard the data in the midst of untrusted processes. Our cloud system will (a) support efficient storage of encrypted sensitive data, (b) store, manage and query massive amounts of data, (c) support fine grained access control and (d) support strong authentication. This paper describes our approaches to securing the cloud. This paper is organized as follows: in section 2 we will give an overview of cloud computing models, in section 3 will discuss about security issues for cloud and in section 4 we will discuss secure third party publication of data in clouds.

II. Cloud models

1. Software as a Service (SaaS). The traditional model of software distribution, in which software is purchased for and installed on personal computers, is sometimes referred to as Software-as-a-Product. Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and

service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Mean-while, broadband service has become increasingly available to support user access from more areas around the world. Examples are Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google.

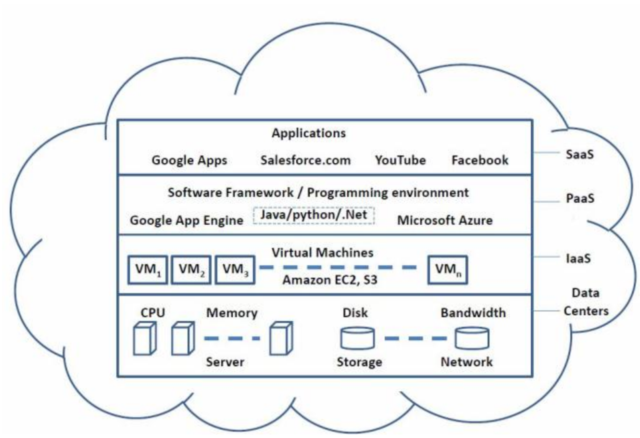

Figure 1: A View of Cloud Computing Architecture

2. Platform as a Service (PaaS). Cloud computing has evolved to include platforms for building and running custom web-based applications, a concept known as Platform-as-a-Service. PaaS is an outgrowth of the SaaS application delivery model. The PaaS model makes all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet, all with no software downloads or installation for developers, IT managers, or end users. Examples include Microsoft's Azure and Salesforce's Force.com.

3. Infrastructure as a Service (IaaS). The capability provided to the consumer is the provision of grids or clusters or virtualized servers, processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems. The highest profile example is Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service, but IBM and other traditional IT vendors are also offering services, as is telecom-and-more provider Verizon Business.

4. Communication-as-a-Service (CaaS) [3] : A CaaS model allows a CaaS provider's business customers to selectively deploy communications features and services throughout their company on a pay-as-you go basis for service(s) used. CaaS is designed on a utility-like pricing model that provides users with comprehensive, flexible, and (usu-ally) simple-to understand service plans

III. Security Issues

1. Data Breaches

Cloud computing and services are relatively new, yet databreaches in all forms have existed for years. The question remains: "With sensitive data being stored online rather than on premise, is the cloud inherently less safe?"

A study conducted by the Ponemon Institute entitled "Man In Cloud Attack" reports that over 50 percent of the IT and security professionals surveyed believed their organization's security measures to protect data on cloud services are low. This study used nine scenarios, where a data breach had occurred, to determine if that belief was founded in fact.

After evaluating each scenario, the report concluded that overall data breaching was three times more likely to occur for businesses that utilize the cloud than those that don't. The simple conclusion is that the cloud comes with a unique set of characteristics that make it more vulnerable.

2. Hijacking of Accounts

The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking.

Attackers now have the ability to use your (or your employees') login information to remotely access sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials.

Other methods of hijacking include scripting bugs and reused passwords, which allow attackers to easily and often without detection steal credentials. In April 2010 Amazon faced a cross-site scripting bug that targeted customer credentials as well. Phishing, keylogging, and buffer overflow all present similar threats. However, the most notable new threat – known as the Man In Cloud Attack – involves the theft of user tokens which cloud platforms use to verify individual devices without requiring logins during each update and sync.

3. Insider Threat

An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

Additionally, these insiders don't even need to have malicious intentions.

A study by Imperva, "Inside Track on Insider Threats" found that an insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controling access, and implementing technology.

4. Malware Injection

Malware injections are scripts or code embedded into cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.

Once an injection is executed and the cloud begins operating in tandem with it, attackers can eavesdrop, compromise the integrity of sensitive information, and steal data. Security Threats On Cloud Computing Vulnerabilities, a report by the East Carolina University, reviews the threats of malware injections on cloud computing and states that "malware injection attack has become a major security concern in cloud computing systems."

5. Abuse of Cloud Services

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

In some cases this practice affects both the cloud service provider and its client. For example, privileged users can directly or indirectly increase the security risks and as a result infringe upon the terms of use provided by the service provider.

These risks include the sharing of pirated software, videos, music, or books, and can result in legal consequences in the forms of fines and settlements with the U.S. Copyright Law reaching up to $250,000. Depending on the damage, these fines can be even more cost prohibitive. You can reduce your exposure to risk by monitoring usage and setting guidelines for what your employees host in the cloud. Service providers and legal entities, such as CSA have defined what is abusive or inappropriate behavior along with methods of detecting such behaviors.

6. Insecure APIs

Application Programming Interfaces (API) give users the opportunity to customize their cloud experience.

However, APIs can be a threat to cloud security because of their very nature. Not only do they give companies the ability to customize features of their cloud services to fit business needs, but they also authenticate, provide access, and effect encryption.

As the infrastructure of APIs grows to provide better service, so do its security risks. APIs give programmers the tools to build their programs to integrate their applications with other job-critical software. A popular and simple example of an API is YouTube, where developers have the ability to integrate YouTube videos into their sites or applications.

The vulnerability of an API lies in the communication that takes place between applications. While this can help programmers and businesses, they also leave exploitable security risks.

7. Denial of Service Attacks

Unlike other kind of cyberattacks, which are typically launched to establish a long-term foothold and hijack sensitive information, denial of service assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legitimate users. In some cases, however, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls.

8. Insufficient Due Diligence

Most of the issues we've looked at here are technical in nature, however this particular security gap occurs when an organization does not have a clear plan for its goals, resources, and policies for the cloud. In other words, it's the people factor.

Additionally, insufficient due diligence can pose a security risk when an organization migrates to the cloud quickly without properly anticipating that the services will not match customer's expectation.

This is especially important to companies whose data falls under regulatory laws like PII, PCI, PHI, and FERPA or those that handle financial data for customers.

9. Shared Vulnerabilities

Cloud security is a shared responsibility between the provider and the client.

This partnership between client and provider requires the client to take preventative actions to protect their data. While major providers like Box, Dropbox, Microsoft, and Google do have standardized procedures to secure their side, fine grain control is up to you, the client.

As Skyfence points out in its article "Office 365 Security & Share Responsibility," this leaves key security protocols – such as the protection of user passwords, access restrictions to both files and devices, and multi-factor authentication – firmly in your hands.

The bottom line is that clients and providers have shared responsibilities, and omitting yours can result in your data being compromised.

10. Data Loss

Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider. Losing vital information can be devastating to businesses that don't have a recovery plan. Amazon is an example of an organization that suffered data loss by permanently destroying many of its own customers' data in 2011.

Google was another organization that lost data when its power grid was struck by lightning four times.

Securing your data means carefully reviewing your provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

IV. Third Party Secure Data Publication Applied to CLOUD

Cloud computing facilitates storage of data at a remote site to maximize resource utilization. As a result, it is critical that this data be protected and only given to authorized individuals. This essentially amounts to secure third party publication of data that is necessary for data outsourcing as well as external publications. We have developed techniques for third party publication of data in a secure manner. We assume that the data is represented as an XML document. This is a valid assumption as many of the documents on the web are now represented as XML documents. First we discuss the access control framework and then discuss secure third party publication. In the access control framework security policy is specified depending on user roles and credentials. Users must possess the credentials to access XML documents. The credentials depend on their roles.

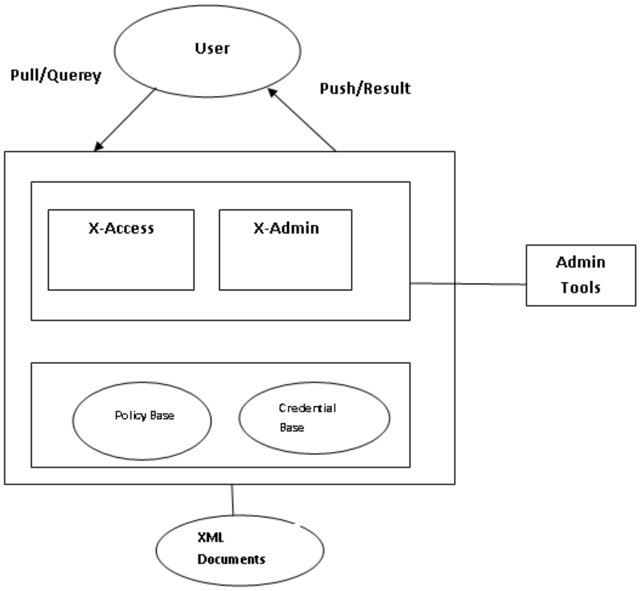

Figure 2: Access Control Framework

The owner of a document specifies access control policies for the subjects. Subjects get policies from the owner when they subscribe to a document. The owner sends the documents to the publishers. When the subject requests a document, the publisher will apply the policies relevant to the subject and give portions of the documents to the subject. Now, since the publisher is untrusted, it may give false information to the subject. Therefore, the owner will encrypt various combinations of documents and policies with his/her private key. Using Merkle signature and the encryption techniques, the subject can verify the authenticity and completeness of the document. In the cloud environment, the third party publisher is the machine that stored the sensitive data in the cloud. This data has to be protected.

V. Conclusion

There are several other security challenges including security aspects of virtualization. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. However the challenge we have is to ensure more secure operations even if some parts of the cloud fail. For many applications, we not only need information assurance but also mission assurance. As such, building trust applications from untrusted components will be a major aspect with respect to cloud security.

References

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

[1] Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. *abs/0901.0131*.

[2] Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.5 (2013): 571-575.

[3] "CLOUD COMPUTING" book authored by John W. Rittinghouse and James F Ransome.

[4] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[5] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[6] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[8] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[9] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.