International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X

National Conference on Recent Trends in Computer Science and Technology (NCRTCST)-2013

Cloud Outcome and Troubles with Safety Solutions

K. Madan Mohan
Department of IT
Malla Reddy Engineering College,
Hyderabad, A.P., India
Email: madan.keturu@gmail.com

Dr. P. Premchand
Prof., Department of CSE,
Osmania University,
Hyderabad, A.P., India,
Email: p.premchand@gmail.com

Dr. K. Chandrasekharaiah
Prof., Department of CSE,
JNT university,
Hyderabad, AP, India,
Email: chandra2ksekharaiah@gmail.com

***Abstract* – The present paper is an introduction of terms cloud security practices, security compliance against standards and best practices, how the cloud changes the role of IT security. Cloud computing executives have pinpointed the rise of security solutions as a key factor in the future of the IT industry. There is hardly a topic creating more of a hum in today's' software industry, Cloud computing is a dramatic shift in the way we think about providing computing resources. 72% plan on deploying cloud services within 3 years. While there is still general confusion about what cloud services are, what benefits they offer, what the disadvantages may be and particularly how secure they are, the trend toward the cloud is accelerating.Let's take a closer look at the state of cloud computing and what you should know about it today.**

***Keywords* – Cloud Computing, SaaS (Software as a Service), IaaS (Infrastructure as a Service) XaaS (Anything as a Service), Shadow IT (Shadow Information Technology), Amazon Web Services (AWS), Customization.**

I. INTRODUCTION

The terms Cloud Computing and Software as a Service or in short SaaS are commonly used among most people who work with a computer. Cloud Computing is the generic term for a technological concept of allowing people to access technology-enabled, highly scalable services in real time over the Internet[2]. Cloud Computing can thus be understood as "IT businesses in the Cloud" and could even replace an entire in-house IT infrastructure. The provided IT services can include the use of the basic infrastructure, hardware, data storage, and software or development platforms. They are offered flexibly and in line with the businesses' requirements. Software-as-a-Service falls under the larger cloud computing definition and offers software solutions which are commonly charged on a pay-per-use or subscription basis. The service is platform independent, so the user need not require any specific form of operating system to run it.There fore the user is free from the burden of installing various forms of services or software's so as to run a particular application. Also the user need not pay for the technology whenever he is not utilizing the service.The cloud is considered to be both software and infrastructure. It serves as an application when accessing it via web browsers (or) web servers.

SaaS is working as follows in IT Industry: In the past, software licenses had to be purchased, today, thanks to higher bandwidths, the concept of Software as a Service (SaaS) fills a perpetual need of IT:

All users need is an Internet-ready PC or device, an Internet connection to the external IT service provider and a web browser which allows access to the SaaS application. These rentable web applications can then be accessed from anywhere and at any time.

II. CLOUD COMPUTING EMERGENCE

Cloud computing is the outsourcing of your IT infrastructure via the Internet. Comparatively than maintaining your own hardware and software atmosphere, cloud computing provides computing resources (such as processor compute time and data storage) on demand via a service provider. Cloud services are often compared in their nature to utility services such as gas or electricity. It is there when you need it, as much as you need, and you pay as you go and only for what you consume. Cloud computing is the next major computing development that will match our project and business needs as well as personal lifestyle to computing capacity.

This situation has several implications: Businesses will have to change their resource planning strategy; small businesses and startups have access to the same computing resources and capabilities as large corporations. Cloud computing architectures follow the idea of flexible resource sharing; this means that a company s usage of hardware resources is dynamically adjusted to their actual needs at any time. Companies start operating in an environment in which cloud services expand or contract without the need for significant configuration changes. Current cloud computing started with the introduction of Amazon Web Services (AWS) in 2006.Google has also been a driving force in giving cloud computing a much more visible face, especially though its popular cloud web backed applications.

III. WHAT IS SPI (SaaS, PaaS, AND IaaS)?

Cloud Computing can be broadly classified into three layers of Cloud Stack, also known as Cloud Service Models or SPI Service Model:

SPI is an acronym for the most common cloud computing service models, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a Service (IaaS) Software (SaaS) 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. Platform as a Service (PaaS) is a paradigm for delivering operating systems and associated services over the Internet without downloads or installation. Infrastructure involves outsourcing the equipment used to support operations, including storage, hardware, servers and networking components. The increasing selection of services delivered over the Internet is sometimes referred to as *XaaS (anything as a service).*

Why SaaS?

• No open fixed cost.we just need a web browser to access the application. No other hardware pay for or software installation. Quick deployment or it's already deployed & ready to use. Cloud architecture makes SaaS highly scalable. Multi-tenant architecture makes SaaS highly efficient as the source code is same for every customer. Unlike conventional apps where customization is the key; a true SaaS can meet any requirement by simple arrangement. Upgrades are pushed directly at the SaaS provider's end. No bother at the customer end. Since all the customers are using same code base, any new tech-innovation is easily incorporated by the source, and is available for all the subscribers.

Examples for SaaS (software as a service):

A. Sales Force CRM
B. Google Apps
C. Desk Away
D. Impel CRM
E. Wipro w-SaaS

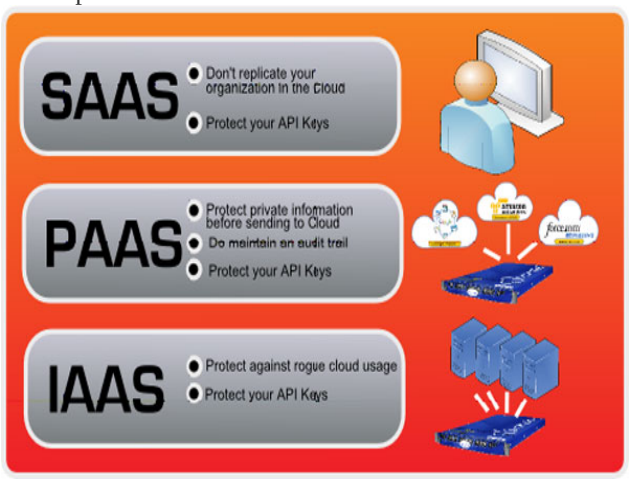

Figure 1

IV. The Software Industries Choose for IaaS Why?

1. The billing is on hourly or monthly basis. we pay only for the resources your actually consume. This is unlike the traditional services where you pay a fixed amount even if you don't use the resources, or don't have enough clients to consume the preconfigured resources. In cloud computing, i.e., IaaS, you pay less if you have a lower customer base and vice-versa. Sounds quite rational!
2. Cloud is elastic in nature, i.e., you can control the number of resources you use at any given point in time. Compare this with traditional hosting, where you rent a fixed number of resources for fixed amount of time. Using IaaS you can easily configure your resources for unexpected spikes in traffic. Based on your computing requirements and configuration, your IaaS provider can respond quickly to*scale up or down*.
3. One more feature I liked about Amazon EC2, which is perhaps provided by other IaaS providers as well, is Elastic Load Balancing. This feature auto-distributes an application's incoming traffic across multiple Amazon EC2 instances (virtual computers).
4. The Amazon EC2 SLA (Service Level Agreement) guarantees 99.95% availability of the service within a region over a trailing 365 day period. GoGrid has the most generous SLA with a guarantee of *100% Uptime* and 24/7 Support.
5. An Amazon EC2 customer can increase or decrease capacity *within minutes*. we can commission one, hundreds or even thousands of server instances simultaneously. This is true for other IaaS providers as well.

V. Five Security Risks of Cloud Computing

1. Although cloud computing can offer small businesses significant cost-saving benefits—namely, pay-as-you-go access to sophisticated software and powerful hardware—the service does come with certain security risks. When evaluating potential providers of cloud-based services, you should keep these top five security concerns in mind.
2. Secure data transfer. All of the traffic travelling between your network and whatever service you're accessing in the cloud must traverse the Internet. Make sure your data is always travelling on a secure channel; only connect your browser to the provider via a URL that begins with "https."
3. Secure software interfaces. The Cloud Security Alliance (CSA) recommends that you be aware of the software interfaces, or APIs, that are used to interact with cloud services. "Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability," says the group in its Top Threats to Cloud Computing document.
4. Secure stored data. Your data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service. In Q&A: Demystifying Cloud Security, Forrester warns that few cloud providers assure protection for data being used within the application or for disposing of your data.

5. User access control. Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people. First, consider carefully the sensitivity of the data you're allowing out into the cloud. Second, follow research firm Gartner's suggestion to ask providers for specifics about the people who manage your data and the level of access they have to it.
6. Data separation. Every cloud-based service shares resources, namely space on the provider's servers and other parts of the provider's infrastructure. Hypervisor software is used to create virtual containers on the provider's hardware for each of its customers. But CSA notes that"attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments."
7. Although you should address these security issues with the cloud provider before you entrust your data to its servers and applications, they shouldn't be a deal breaker. Cloud computing offers small businesses too many benefits to dismiss out of hand. After all, you already met many of these security challenges the first time you connected your network to the Internet.

Solution to Secure stored data:

In the cloud, the data is transferred among the server and client. Cloud security is the current discussion in the IT world. This research paper helps in securing the data without affecting the network layers and protecting the data from unauthorized entries into the server, the data is secured in server based on users' choice of security method so that data is given high secure priority.

Figure 2

VI. Current Problems and Solutions in Cloud Computing in Industry

The main problems cloud computing faces are preserving confidentiality and integrity of data in aiding data security. The primary solution for these problems is encryption of data stored in the cloud. However, encryption of data also brings up new problems. Here is an overview of some of the main problems faced by cloud systems and some solutions.

A. Trust

Trust between the Service provider and the customer is one of the main issues cloud computing faces today. There is no way for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do. However, there is currently no clear format for the SLA, and as such, there may be services not documented in the SLA that the customer may be uninformed that it will need these services at some later time.

B. Legal Issues

There are several regulatory requirements, privacy [9] laws and data security laws that cloud systems need to adhere to. One of the major problems with adhering to the laws is that laws vary from country to country, and users have no control over where their data is physically located.

C. Confidentiality

Confidentiality is preventing the improper disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems since the information is stored at a remote location that the Service Provider has full access to. Therefore, there has been some method of preserving the confidentiality of data stored in the cloud. The main method used to preserve data confidentiality is data encryption; however encryption brings about its own issues, some of which are discussed later.

D. Authenticity (Integrity and Completeness)

Integrity is preventing the improper modification of information. Preserving Integrity, like confidentiality is another major issue faced by cloud systems that needs to be handled, and is also mainly done by the use of data encryption.

In a common database setup, there would be many users with varying amount of rights. A user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete that is, not poisoned, altered or missing anything.

E. Encryption

The main method used for ensuring data security in the cloud is by encryption. Encryption seems like the perfect solution for ensuring data security; however, it is not without its drawbacks. Encryption takes considerably more computational power, and this is multiplied by several factors in the case of databases Cryptography greatly affects database performance because each time a query is run, a large amount of data must be decrypted; and since the main operation on a database is running queries, the amount of decryption operations quickly become excessive. Early approaches have used extensions to the query language that simply applied encryption before writing to the database and apply decryption before reading from the database.

VII. Querying Encrypted Data

In the proposed scheme, several cryptographic methods were used to encrypt the data in each cell of each table to be stored in the cloud. When a user needs to query this data, the query parameters are encrypted and checked against the stored data. No data decryption is done in the cloud, thus protecting the Authenticity and integrity of the information. When the results of the query is returned (in encrypted form) to the user, the user then decrypts the data and uses it.

VIII. Cloud Computing Continues to Drive IT Growth and Shapes Industry

The IT industry is undergoing a paradigm shift with cloud computing with no trouble being one of the main drivers. Industry forecaster firm IDC has coined this shift as the "third platform," following on its previous two technology shifts. And while questions remain about whether this platform is anything new, enterprises that choose to disregard it might not properly develop.

Cloud computing plays a main role in transforming enterprise IT's system design. Cloud software development will become increasingly important.

IX. Conclusion

Cloud Computing offers some incredible benefits: unlimited storage, access to lightening quick processing power and the ability to easily share and process information; though, it does have several issues, and most of them are security [7] related. Cloud systems must overcome many obstacles before it becomes widely adopted, but it can be utilized right now with some compromises and in the right conditions.

We have discussed several security issues that currently affect cloud systems [8]; however, there may be many unspecified and undiscovered security issues. Research is currently being done on the different known issues faced by cloud systems and possible solutions for these issues, however there is still a need for better solutions if cloud systems are to be expansively adopted.

One of the main problems that need to be addressed is coming up with a clear and standardized format for the Service Level Agreement (SLA), a format that fully documents all of the services, what services and processes would be provided by the service provider to back up its assurances.

Another major issue cloud systems face is Encryption. Encryption is the main method of ensuring security of data stored in the cloud; however, encryption is computationally costly. Encryption methods specific to DaaS (Cloud Databases) has been developed and more research is currently being done on Encryption mechanisms for cloud systems, however, more efficient methods are still needed to help increase speed the acceptance of cloud systems.

References

[1] Amazon,"s3" http://aws.amazon.com/s3/2008
[2] A vision for the internet, ST journal of research, 2(1):4-5, Nov.2005
[3] GoogleAppEngine: http://appengine.google.com
[4] Microsoft Azure, http://Microsoft.com/azure/
[5] http://doi.ieeecomputersociety.org/
[6] "Risks to privacy and confidentiality from cloud computing" http://www.worldprivacyforum.org
[7] Scalable security solutions, check point open performance Architecture http://oreilly.com
[8] A journal of "The case for cloud computing" It professional
[9] "Data security in the world of cloud computing"IEEE security and privacy journal
[10] A journal of "A survey on security issues delivery models of cloud"
[11] Securing the cloud: Addressing the cloud computing security concerns with private cloud" http://www.rackspace.com