Review on Cloud Computing Security Solutions Against Various Issues

M V Narayana
Associate Professor, Department of CSE, Vivekananda Group of Institutions, Greater Hyderabad.

Abstract— Cloud computing, a rapidly developing information technology, has aroused the concern of the whole world. Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid. Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. Cloud computing has attracted more attention. More and more enterprises or government agencies started to explore cloud computing. However, with the extensive use of cloud computing, security issues came out on a growing scale. It is necessary to solve these security issues to promote the wider applications of cloud computing. This study aims to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing. This will enable researchers and security professionals to know about users and vendors concerns and critical analysis about the different security models and tools proposed.

Keywords— grid computing, middleware, redundancy, threats, encryption, virtualization.

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have been developed. Arguably, one of the most discussed among all of these is Cloud Computing. Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The cloud is emerging as the latest way to approach alternative delivery models for IT capabilities. It is a way of delivering IT- enabled services in the form of software, infrastructure and more.

Cloud computing can be defined as "A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing platforms on Demand, which could be accessed in a simple and pervasive way"[1]. In simple words, Cloud computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Demand computing infrastructures with good quality of service. Cloud Computing is the implementation of engineering principals to obtain high quality applications through Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing Infrastructures with good quality of service levels. Cloud computing provides the internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The advantages of using cloud computing are:

i) reduced hardware and maintenance cost,
ii) accessibility around the globe, and

Flexibility and the highly automated process wherein the customer need not worry about software up-gradation which tends to be a daily matter. Cloud computing can be divided into two sections, the user and the cloud. In most scenarios, the user is connected to the cloud via the internet. It is also possible for an organization to have a private cloud in which a user is connected via a intranet. The user sends requests to the cloud and the cloud provides the service. Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

II. CLOUD COMPUTING ARCHITECTURE

When talking about a cloud computing system, it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system.

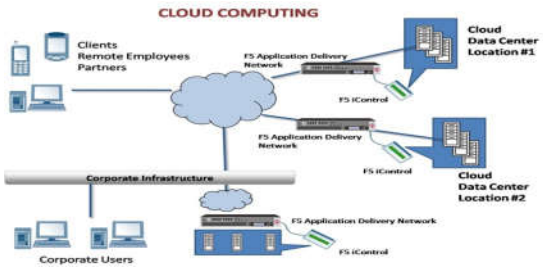

Fig 1:-The architecture of cloud data storage service

The front end includes the client's computer and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services.

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity.

A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called **redundancy**.

Cloud service providers tend to offer services that can be grouped into three categories: software as a service, platform as a service, and infrastructure as a service.

i) Software as a Service (SaaS):

If provide software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

ii) Platform as a service (PaaS):

Platform as a service encapsulates a layer of software and provides it as a service that can be used to build higher level services. There are at least two perspectives on PaaS depending on the perspective of the producer or consumer of the services:

• Someone producing PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service.

• Someone using PaaS would see an encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale it to provide a given level of service. Virtual appliances can be classified as instances of PaaS. Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google's infrastructure. PaaS services such as these can provide a powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

iii) Infrastructure as a service (IaaS):

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications. Commercial examples of IaaS include Joyent, whose main product is a line of virtualized servers that provide a highly available on demand infrastructure.

III. THREATS IN CLOUD COMPUTING

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

- **Network security:**

Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks [2], adopting the same protection measures and security precautions that are locally implemented.

And allowing them to extend local strategies to any remote resource or process.

- **Transfer security:**

Distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, and man-in-the-middle and side-channel attacks.

- **Firewalling:**

Firewalls protect the provider's internal cloud infrastructure against insider and outsiders [3]. They also enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of-Service (DoS) and detection of external security assessment procedures. Efforts for developing

Consistent firewall and similar security measures specific for cloud environments reveal the urge for adapting existing solutions for this new computing paradigm.

- **Security configuration:**

Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency [4].

IV. SECURITY ISSUES

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

A. Data security:

Data of "Cloud" is stored in different physical locations, distributed in various parts of the Earth, in the absence of corresponding technical and regulatory constraints, data security is difficult to get protection. First of all, different places have different levels of technology, some advanced and some behind. Data is safe somewhere, but there may be some risk in another place. Secondly, there are different regulations in different places.

B. Interfaces**:**

Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.

API: Programming interfaces (essential to IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use [5].

- Administrative interface:

Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, and testing) and application tools for SaaS (user access control, configurations).

- User interface:

End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment.

- Authentication:

Mechanisms required to enable access to the cloud. Most services rely on regular accounts consequently being susceptible to a plethora of attacks whose consequences are boosted by multi-tenancy and resource sharing.

C. Virtualization:

Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies [6].

- Isolation:

Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks [7]. The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.

- Hypervisor vulnerabilities:

The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.

- Data leakage:

Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.

D. Governance:

Issues related to (losing) administrative and security controls in cloud computing solutions. [8, 9]

i) Data control

Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.

ii) Security control:

Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps

iii) 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." Also, your data should always be encrypted and authenticated using industry standard protocols, such as IPSec (Internet Protocol Security), that have been developed specifically for protecting Internet traffic.

E. Loss of service:

Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown

in many examples [10-12]. This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.

V. CRITICAL EVALUATION

Cloud computing from its early years to Current State:

The forerunners of cloud computing emerged decades ago—first as time- and compute-sharing on mainframes, then as utility computing through private network services. When the Internet became established in the late 1990s, application service providers (ASPs) and grid computing started to get some traction. However, all of them had to DEAL with limitations, the main one being not enough network bandwidth to make them workable for large numbers of users. Now, thanks to broadband, fiber-optic cable, improved software and many other advances, cloud computing has the power and pipes it needs and has branched into public, private and hybrid cloud services. But it's still early in cloud history.

I. SMBs Lead the Charge

Although the majority of enterprises, both large and small, have adopted cloud computing in some way, small and midsize businesses (SMBs) are leading the pack when it comes to the percentage of services they rely on from the cloud. A recent survey from Spice works showed that more than 60 percent of SMBs responding to the survey are using cloud-based services today; spending on these services is projected to grow almost 20 percent in the next five years, according to IDC [13].

II. Clouds Getting More Complex to Administer

For many large enterprises, increasing user demand, shorter timelines, the growth of mobile devices and the bring-your-own-device (BYOD) age has resulted in a complex mix of data centre infrastructure and public, private and hybrid cloud services by large organizations. In addition, the growth of big data presents a huge challenge in terms of both storage and computing capacity. In response to these variables, the cloud computing benefits of dynamic scalability and pay-as-you-go are driving cloud adoption in large enterprises to help meet these challenges.

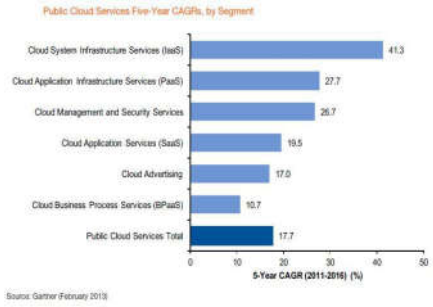

Fig 2:-Evaluation of cloud computing:

- Security Still the Main Source of Distrust

Despite these trends and the benefits of the cloud model, a high degree of concern about security of systems and data still prevents many key corporate applications from moving to cloud services. For most large organizations, mission-critical apps have remained in-house and under the control of IT. According to management consulting and technology services firm Trianz, cloud-based services will soon enable a mere 30 to 40 percent of business functionality while the remaining 70 to 60 percent of functionality will rely on home-grown IT delivered solutions.

III. More Clouds Gathering Inside the Firewall

Surveys are indicating growing use of internal and hybrid clouds as IT starts to transform internal infrastructure into more flexible and cost-effective private cloud services

IV. More Key Business Apps Will Be Cloud-Based

With new technologies and services emerging that can support the provisioning of full physical servers while enabling them to retain the flexibility and automation that cloud services provide, mission-critical apps will become increasingly cloud-based.

V. Automation, Easy Configurability: Keys to the Cloud's Future

To spur future adoption, cloud services must include the following: the ability to seamlessly provision hybrid clouds that include internal and public cloud computing resources; the ability to provision virtual and physical resources to support a broad range of apps, including performance-intensive mission-critical apps; comprehensive functionality to deliver user self-service with a high level of security, availability and management ; and ease of use for end users and the IT personnel who need to implement cloud service.

VI. SAFETY MEASURES FOR CLOUD COMPUTING:

Considering the major security issues of Cloud computing, this paper summed up several appropriate solution measures:

a. Strengthen the anti-attack capability:

It is important to deploy the Anti-attack technology, anti-virus software, and firewalls in the clouds. Many security vendors have launched "cloud security" and "cloud antivirus" and other technologies.

b. Information-centric security:

In order for enterprises to extend control to data in the cloud, we propose shifting from protecting data from the outside (system and applications which use the data) to protecting data from within. We call this approach of data and information protecting itself information-centric [14]. This self-protection requires intelligence be put in the data itself. Data needs to be self-describing and defending, regardless of its environment. Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment using virtualization and reveal itself only if the environment is verified as trustworthy (using Trusted Computing). Information-centric security is a natural extension of the trend toward finer, stronger, and more usable data protection.

c. Information Encryption:

A different approach to retaining control of data is to require the encryption of all cloud data. The problem is that encryption limits data use. In particular searching and indexing the data becomes problematic. For example, if data is stored in clear-text, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. State-of-the-art cryptography may offer new tools to solve these problems. Cryptographers have recently invented versatile encryption schemes that allow operation and computation on the cipher text.

The cloud service provider is empowered with some ability to search the encrypted data, the proliferation of cloud data can potentially enable better insider threat detection (e.g. by detecting user activities outside of the norm) and better data loss prevention (DLP) (e.g. through detecting anomalous content).

Apart from ensuring privacy, applied cryptography may also offer tools to address other security problems related to cloud computing. For example, in proofs of retrievability the storage server can show a compact proof that it is correctly storing all of the client's data.

d. High-Assurance Remote Server Attestation:

Currently customers must be satisfied with cloud providers using manual auditing procedures like SAS-70.

A promising approach to address this problem is based on Trusted Computing. Imagine a trusted monitor installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide "proofs of compliance" to the data owner, stating that certain access policies have not been violated. To ensure integrity of the monitor, Trusted Computing also allows secure bootstrapping of this monitor to run beside (and securely isolated from) the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a "proof of compliance", the code of the monitor is signed, as well as a "statement of compliance" produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies

e. Selecting the reasonable storage location:

Based on cloud computing, users do not know where the data stored in, which will bring more security issues. Firewalls and intrusion detection and prevention can keep out most intruders, and data encryption keeps the data safer, but we don't know where the data goes when we terminate our service or when the cloud provider goes out of business. Dedicated hardware is the key that allows for cloud computing services to pass the most stringent security guidelines. Therefore, when the user selects cloud computing providers, they should select reputable service providers, and also need to read the privacy statements carefully.

f. Establishing uniform safety standards:

Currently, many governments and businesses have noticed this problem, and are active in discussing to establish a common standard to advance the popularity of cloud computing. Safety standards, include not only the technical standards, should also include the safety standards for using, to establish a secure privacy mechanism.

g. Selecting reputable service providers:

Considering their own long-term development and their own reputation, a company with mature technical and service will not disclose of user information by knowing which server and data centre your data is being stored at, you can probe them for all applicable security measures that are in place.

VII. CONSIDERATIONS AND FUTURE WORK

We are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. To be able to resolve such problem we need to capture different stakeholders security requirements from different perspectives and different levels of details map security requirements to the cloud architecture, security

patterns and security enforcement mechanisms and Deliver feedback about the current security status to the cloud providers and consumers.

Security is a crucial aspect for providing a reliable environment and then enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. Many of the security issues identified are observed in other computing environments: authentication, network security and legal requirements, for example, are not a novelty. However, the impact of such issues is intensified in cloud computing due to characteristics such as multi-tenancy and resource sharing, since actions from a single customer can affect all other users that inevitably share the same resources and interfaces. On the other hand, efficient and secure virtualization represents a new challenge in such a context with high distribution of complex services and web based applications, thus requiring more sophisticated approaches.

It is strategic to develop new mechanisms that provide the required security level by isolating virtual machines and the associated resources while following best practices in terms of legal regulations and compliance to SLAs. Among other requirements, such solutions should employ virtual machine identification, provide an adequate separation of dedicated resources combined with a constant observation of shared ones, and examine any attempt of exploiting cross-VM and data leakage.

VIII. CONCLUSION

Cloud, is lying face down to various security threats varying from network level threats to application level threats. In order to keep the cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like security issues, accessibility issues, confidentiality, and integrity of data. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed.

References:

[1] Song, D., Wagner, D., and Perrig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in Security and Privacy. 2000.

[2] L. Wang, G. Laszewski, M. Kunze and J. Tao, "Cloud computing: a perspective study", J New Generation Computing, 2010, pp 1-11.

[3] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[4] R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[5] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay.

[6] http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

[7] An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.

[8] http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf

[9] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. In EUROCRYPT. 2004.

[10] Boneh, D and Waters, B. Conjunctive, Subset, and Range Queries on Encrypted Data. In The Fourth Theory of Cryptography Conference (TCC 2007), 2007

[11] Shen, E., Shi, E., and Waters, B. Predicate Privacy in Encryption Systems. In TCC. 2009.

[12] Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, A. Multi-Dimensional Range Query over Encrypted Data. In IEEE Symposium on Security and Privacy. 2007.

[13] TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper

[14] Genovese S (2009) Akamai Introduces Cloud-Based Firewall.http://cloudcomputing.sys-con.com/node/1219023