ISSN : 2231-0711

Nilotpal Chakraborty et al | International Journal of Computer Science Engineering and Technology( IJCSET) | January 2014 | Vol 4, Issue 1,1-4

# Security Challenges in Cloud Computing: A Comprehensive Study

Nilotpal Chakraborty [#], Raghvendra Singh Patel [*]

[#] *SPARK Student, CSIR- Fourth Paradigm Institute, Bangalore*
M.Tech student, School of Future Studies & Planning, Devi Ahilya University, Indore

[*] *Project Assistant, Indian Institute of Science Education Research, Bhopal*
M.Tech student, School of Future Studies & Planning, Devi Ahilya University, Indore

***Abstract*— In today's advanced computing era, where all the organizations are looking to cut their operational cost, alongside increasing their efficiency and productivity, cloud computing is the most viable solution to their needs. Cloud computing offers prominent and efficient services in terms of software, hardware, server, databases etc in a more flexible, highly-scalable and cost-effective manner than the traditional mode of in-housing computational infrastructure. But as with the case of traditional computing, cloud computing also has some serious challenges regarding its security. Before migrating to cloud infrastructure, one needs to be clear about the risks and security issues associated with it and the necessary actions to be taken in order to mitigate the problems. As the cloud infrastructure and service attain maturity, the number of security attacks is also increasing exponentially. In this paper, we discuss about the major security threats that can hamper cloud and computing infrastructure and what protection mechanism needs to be taken to withstand the attacks.**

***Keywords*— *Cloud computing, cloud security, security threats, cloud cryptography, cloud security controls*.**

## I. INTRODUCTION

Cloud computing is a computational model with the help of which a user or an organization can have various computing services and infrastructure available to him. It provides an efficient and seamless connectivity to the various resources such as data, software, hardware, databases, servers, compilers etc to the user that can be used as per the needs and requirements. Formally cloud computing [1] can be defined as—

*"It is a model for enabling ubiquitous , convenient, on-demand, network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

In any application development environment, the most important factor is maintaining the computing infrastructure. In a typical software development process, 40% of the effort is needed just to maintain the developed application and the development platform. With the help of the concept of cloud computing, the entire necessary software development infrastructure along with the data, are stored in some remote servers, without the knowledge of the developers and the organizations. They are only the users of the services and resources, as per their needs and requirements and pay accordingly. They are free from all the burdens of maintaining the systems of their own, thus increasing the efficiency and productivity of the organizations and reducing the associated maintenance costs.

Cloud computing represents a different way to architect and remotely manage computing resources. One has only to establish an account with any cloud service provider (CSP), such as Microsoft or Amazon or Google, to start developing and deploying applications on a cloud. The applications can be web applications that require only http services or a relational database. There might be a need of web service infrastructure and message queues or the need to interoperate with CRM or e-commerce application services, necessitating construction of a custom technology stack to deploy into the cloud if these services are not already provided there. They might require the remote hosting and use of custom or third party software systems. And they might require the capability to programmatically increase or decrease computing resources as a function of business intelligence about resource demand using virtualization. While not all of these capabilities exist in today's clouds, nor are all that do exist fully automated, a good portion of them can be provisioned [2].

With its various service models viz. Software-as-a-service (Saas), Platform-as-a-service (Paas) and Infrastructure-as-a-service (Iaas), cloud computing reduces the operational and capital costs for the service providers on one hand, and for the users by providing the opportunity to access services according to their needs. Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs [3]. They are excited for a chance to divest them of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, despite the surge in activity and interest, there are significant, persistent security concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Cloud computing offers many benefits, but it also is vulnerable to threats. As the uses of cloud computing increase, it is highly

likely that more criminals will try to find new ways to exploit vulnerabilities in the system. There are many underlying challenges and risks in cloud computing that increase the threat of data being compromised. To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed in order to establish trust in cloud computing technology.

While there are important security, privacy and regulatory issues that enterprises need to sort through before full migration to the cloud, and cloud vendors need to strengthen cloud capabilities in these areas before enterprise applications can be effectively hosted in the cloud

## II. SECURITY REQUIREMENTS IN CLOUD COMPUTING

For any computing resource, security has always been a critical factor. The resources which need protection from malicious access and use are hardware, software and data. Since cloud computing provides all these resources to its users, all the security measurements that needed in traditional computing are applicable in cloud environment also. In cloud computing, a cloud service provider (CSP) provides a user the computational services on a leased basis over the internet. Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing paradigm [4]. This is particularly true for the SaaS provider.

There is a number of security issues associated with cloud computing but these issues fall under two broad categories: security issues face by the CSPs and security issues faced by the cloud users. Cloud computing helps users to store their data on a remote server which is being provided and managed by the CSPs and proper security measures must be taken from both the CSPs and the clients to ensure that the data in the cloud is secured.

To assure security in cloud, proper security assessment must be done in order to build trust among the clients. This trust will act as the basis for security assurance as provided by the CSPs. Till date, there has not been much development in cloud security assurance, and this is mainly due to the unclear and ambiguous roles and responsibilities among the cloud service providers and their clients. In most cases, the CSPs must ensure that their infrastructure is secure and that their client's data and applications are protected while the clients must ensure that the provider has taken the proper security measures and are following the standard compliance guidelines to protect their data.

Advocates of cloud computing promise great things, and many believe that the claims are not merely hype—that cloud services will be a defining characteristic of the next era of computing [5]. However, Security could be the cloud's Achilles' heel and must be sorted out for cloud computing to reach its potential. Information systems cover a spectrum of requirements—from total protection to complete openness—and internal risk assessments are the means by which an organization evaluates the trade-offs and decides what level of security is acceptable and appropriate. Cloud security involves the fundamental issues as any computer security program: restricting access to authorized users, maintaining the integrity of data, and ensuring the availability of data and services. Proper security mechanisms have to be undertaken to fully realize the potential and the benefits of this modern computing paradigm

## III. SECURITY THREATS IN CLOUD COMPUTING

Cloud computing promises to help organizations and their IT departments be more agile, efficient, and able to cost-effectively deliver new services that enable their businesses to thrive. But the promise of the cloud cannot be fulfilled until IT professionals have more confidence in the security and safety of the cloud. We know that IT concerns with cloud computing security are major barriers to business adoption of the cloud. But before the IT industry can address these concerns, better understanding of them is required.

Many security and privacy threats, such as malware or the risk of a malicious insider, appear to be omnipresent aspects the information technology landscape today, and must be addressed as part of a larger national and international cyber security agenda. The security challenges faced by organizations wishing to use cloud services are not radically different from the traditional security issues and threats. The same internal and external threats are present and require proper risk mitigation and disastrous management policies in order to protect privacy and security.

To identify the top most security threats impending in cloud computing, Cloud Security Alliance conducted a survey of industry experts to compile professional opinion on the greatest vulnerabilities within cloud computing. In this most recent edition of this report, experts identified the following nine critical threats to cloud security [6] (ranked in order of severity)—

i. *Data Breaches*: A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. The cloud service provider must ensure the best level of security authentication and authorization procedure to ensure data protection. If a multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well.

ii. *Data Loss*: For both consumers and businesses, the prospect of permanently losing one's data is terrifying. Of course, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a

customer encrypts his or her data before uploading it to the cloud, but loses the encryption key, the data will be lost as well.

iii. *Account Hijacking*: Account hijacking is not a new threat to computing. It is a type of identity theft in which the attacker uses stolen account information to carry out malicious or unauthorized activities. Typically account hijacking is carried our through phishing, sending spoofed emails to the user, password guessing or a number of other hacking techniques. In many cases, an email account is linked to a person's social networks and financial networks etc. and by impersonating the account; a hacker can gain access to these confidential data for illegitimate activity.

iv. *Insecure APIs*: Users of cloud services access their data through some interfaces as provided by the service providers. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

v. *Denial of Service*: Denial of Service (DOS) attacks are nothing new and they've been a thorn in the sides of data center managers and IT staff for more than a decade now. Through DOS, a hacker doesn't need to attack the entire infrastructure anymore. They can simply choose the most resource intensive app that the user is running on the cloud and use simple low band width attacks to take out that service.

vi. *Malicious Insiders*: Cloud computing as a process is governed, managed, and maintained by site administrators. By default, they hold the key to managing all the data, files and privileged company resources and files. These administrators sometimes because of some personal differences can leak out the important data of a client or can distribute confidential financial or official data of the organization.

vii. *Abuse of Cloud Services:* One of cloud computing greatest benefits is that it allows even small organizations access to vast amounts of computing power. Any organization irrespective of its size, can rent computing resources based on its needs and requirements. However, not everyone wants to use this power for good. Using the enormous computational resources provided by the cloud, an attacker can attack a high performance machine in a convenient amount of time, which otherwise would have taken years to accomplish.

viii. *Insufficient Due Diligence*: ever since its introduction, the demand for cloud computing has always been increasing and it is mainly due to its promising cost cutting technology and increasing operational efficiency. But without fully understanding the CSP functioning and environment, migrating to cloud would lead to chaos for the organizations.

ix. *Shared Technology Issues*: Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. A defensive in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or wrong configuration can lead to a compromise across an entire provider's cloud

## IV. SECURITY MEASUREMENTS: TRADITIONAL VS. CLOD

Although, security threats and issues are omnipresent in all sorts of computing environment, cloud computing needs special form of security measurement and assurance than that of traditional computing paradigm. The primary difference between the traditional and cloud computing is that in cloud, the client's data reside in some remote storage space as provided by the CSP. As the remote server is used store important data of many of the CSP's clients, it is very essential to protect the server from mishandling or unauthorized access. In cloud computing, both the user and the service providers are responsible for securing the computing resources.

The unconventional mode of functioning of cloud computing leads information security engineers and scientists to rethink the security mechanisms needed to secure the underlying computing infrastructure of cloud. Cloud computing appears to be a black box to the client as they are completely unaware of what happens inside the cloud and how their data are being stored. Thus the security mechanisms undertaken to protect the privacy, confidentiality and integrity of their data and other resources also remain to be hidden. Due to this fact, users of cloud computing are still in a fear of losing their data, ultimately hindering the progress of cloud computing up to a lot of extent.

Cloud provides a user, as a service, not only the provision to store their data online, but it also provides them with a virtual machine and hardware, which makes it more prone to security threats. An intruder or hacker can affect the user data, the applications he uses, the server where the data is stored, the underlying hardware platform etc. The cloud gives a user the privilege to access a huge amount of computing resources which in general could not have been affordable. But with this, the security threats also increases as now the service providers have to protect a huge cloud infrastructure

## V. CLOUD SECURITY TECHNIQUES

To protect the data stored in the cloud and to ensure security for the clients, scientists have come up with the following four security techniques—

- *Homomorphic encryption*: This is an encryption scheme that provides a mechanism to perform some specific type of computation on encrypted data which is not possible with any other encryption schemes. With the help of this technique, a user can store data in the cloud in an encrypted form, and can perform any required computation without the need to decipher the encrypted data.

- *Searchable/ structured encryption*: This type of technique also uses the homomorphic encryption as its base. Searchable encryption mechanism helps in searching the database of encrypted data with an encrypted keyword. It guarantees that cloud never sees the data and what computation is performed on the data.
- *Proofs of storage*: A proof of storage is a service level agreement between the CSPs and its clients and it ensures that the client data stored in the CSP's servers would never be tempered or used by the CSP without the client's permission. This guarantees that the data stored in the cloud would remain intact.
- *Server aided secure computation*: This security mechanism provides a server and users to perform some computation on their encrypted data jointly without revealing the contents of the original data. The communicating parties and the cloud remain completely unaware of the computations performed and the outcome.

## VI. CLOUD SECURITY CONTROLS

The cloud security architecture is only useful when proper security controls are in place. To control security breaches, an organization needs to be ensured that their security softwares are up to date, and their system is compliant with standard security guidelines. The security management of cloud addresses these issues with various security controls, broadly classified into the following four categories—

- *Deterrent controls*: these are the security control measures that prevent any potential attack on cloud architecture. Deterrent controls warn the security management about any purposeful attack that may have been taking place so that proper preventive controls can be taken.
- *Preventive controls*: as suggested by the name, these control techniques will detect any potential attack on to the cloud system and will take proper actions to mitigate the damage and violations occurring in the system.
- *Corrective controls*: corrective controls are used t reduce the effect of an attack. Unlike the preventive controls, the corrective controls take actions as an attack is occurring.
- *Detective controls*: These control techniques are used to detect any potential attack that may be occurring in the system. If an attack has occurred, detective controls will signal the preventive or corrective controls to address the issue.

## VII. CONCLUSIONS

Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. Cloud computing is a paradigm shift in which computing is moved away from personal computers and even the individual enterprise application server to a 'cloud' of computers. But along with its various efficient computing promises, cloud computing brings another dimension of security challenges that are to be addressed before its full potential can be realized.

Cloud computing adoption and diffusion are threatened by unresolved security issues that affect both the cloud provider and the cloud user. Cloud nodes are inherently more vulnerable to cyber attacks than traditional solutions, given their size and underlying service-related complexity—that brings an unprecedented exposure to third parties of services and interfaces. An organization or any other individual must make sure that standard security compliance guidelines are being followed properly, before migrating to cloud. Protecting sensitive data and systems as well as providing visibility to the security of those systems is the key for the transition to the cloud.

## ACKNOWLEDGMENT

The authors would like to thank Dr. V.B. Gupta, Head, School of Future Studies and Planning, Devi Ahilya University, Indore for his constant guidance. Nilotpal in particular is thankful to Dr. D S Bhilare, Heaad, Computer Centre, Devi Ahilya University, Indore for his encouragement and guidance.

## REFERENCES

[1] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, Dawn Leaf ; NIST Cloud Computing Reference Architecture; NIST Special Publication 500-292, 2011.

[2] Thomas Winans and J S Brown, Cloud Computing: A Collection of Working Papers, May 2009.

[3] Bouayad, A.; Blilat, A.; El Houda Mejhed, N.; El Ghazi, M., "Cloud computing: Security challenges," *Information Science and Technology (CIST), 2012 Colloquium in* , vol., no., pp.26,31, 22-24 Oct. 2012 doi: 10.1109/CIST.2012.6388058

[4] N Jenefa, N Jayalaxmi, A Cloud Storage System with Data Confidentiality and Data Forwarding, International Journal of Soft Computing and Engineering, ISSN: 22312307, Vol X Issue X, March 2013

[5] DS Bhilare and Nilotpal Chakraborty Enhanced Security in Cloud Computing Environment, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3 Issue 9, September 2013.

[6] "The Notorious Nine: Cloud Computing Top Threts in 2013", Top Threats Working Group, Cloud Security Alliance, February 2013

[7] C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC '09, pages 169-178, ACM, 2009

[8] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing: http://www.cloudsecurityalliance.org/csaguide.pdf.