IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 5, Ver. II (Sep - Oct 2018), PP 46-52
www.iosrjournals.org

Challenges In Cloud Computing on Security Issues And Solutions

Dr.K.Sasikala, Mr. M.Annamalai
Associate Professor Department of CSE Vinayaka Mission's KirupanandaVariyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University),
Assistant Professor Department of CSE Vinayaka Mission's KirupanandaVariyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University),
Corresponding Author: Dr.K.Sasikala,

Abstract : *Cloud computing is a technology concept that enables organizations or individuals to share various services in a seamless and cost-effective manner. Technology innovation and its adoption are two critical successful factors for any business/organization. This paper describes cloud computing challenges. A computing platform which faces various challenges in securing the data of the cloud environment. This paper discuss about the cloud, cloud types, security issues, cloud security attacks, applications and methodologies of security solutions in Cloud Computing.*

Keywords: *Noc- network architects, data center, Cloud Security Alliance, Distributed Denial of Service, Advanced persistent threats*

Date of Submission: 2-10-2018 Date of acceptance: 19-10-2018

I. Introduction

The Layers of the Cloud

Too often the vast majority of online articles and blogs concerning the Cloud talk about the technology through the guise of generalization as if saying "the Cloud" multiple times succinctly and clearly explained everything about "the Cloud"Well, as a believer in the more knowledge you have the better, below is a quick starter course in Cloud education aimed at peeling back the layers of "Cloud Computing" to introduce you to SaaS, PaaS and IaaS. In this entry of "How the Internet Works", the Cloud is broken down into its core elements.Like an onion, the Cloud has layers. Not just made up of catchy marketing terms and lingo which goes out of its way to remain obtuse, Cloud Computing is comprised of three major layers - SaaS, PaaS and IaaS. Of the three, IaaS is the foundation while SaaS is the top layer functioning off both PaaS and IaaS. Interestingly enough, although SaaS is normally represented in graphics as the smallest layer of Cloud infrastructure.

TYPES OF CLOUD PROVIDERS

IaaS - Infrastructure as a Service

IaaS or Infrastructure as a Service refers to the hardware, network equipment and web hosting servers which web hosting companies rent out to consumers. The IaaS layer of Cloud Computing is comprised of all the hardware needed to make Cloud Computing possible. Used day in and day out by network architects (sometimes called NOC's) and web hosting professionals, the IaaS layer is the physical foundation of Cloud Computing which can be and is leased out to users to run their own Cloud based services.

The IaaS layer of Cloud Computing is physical hardware. Regardless of what anyone tells you, the Cloud is based on physical computing hardware (servers, nodes, PDU's, blades, hypervisors, cooling gear etc.) stored in a data center (also called a DC) operated by network architects, network engineers and web hosting professionals/companies. The big take away here: the Cloud is physical and without the IaaS layer, both PaaS and SaaS would not be possible.

PaaS - Platform as a Service

PaaS or Platform as a Service refers to the middle layer of the Cloud used for development by web developers, programmers and coders. The PaaS layer of the Cloud is used by developers and programmers to create applications, programs, software and web tools. PaaS works by developers renting raw hardware from an IaaS provider which can then be used as the platform to build software, applications, programs and web tools.In most cases, developers will purchase the PaaS layer of the Cloud from infrastructure providers like RackSpace, Amazon EC2, Linode and Digital Ocean. The purchased infrastructure will come with pre-installled developer tools like Apache, MySQL, Ruby, LAMP Stack, Dokku and GitLab etc.

Getting a bit more granular with PaaS, the majority of providers sell PaaS level servers to consumers on a per resource allocation. Whereas you might purchase a car with 255 horsepower, leather seats and heated

review mirrors, developers will purchase a Cloud server with a specific allotment of RAM, Disk Space, CPU Cores and Bandwidth. A typical Cloud server might look like 4GB of RAM, 60GB of Disk Space, 4 CPU Cores and 8TB of Bandwidth.The big take away here: the PaaS layer of the Cloud is based on the IaaS layer of the Cloud and is used to build the highest layer of the Cloud, SaaS applications.

SaaS - Software as a Service

SaaS or Software as a Service is the top most layer of the Cloud. SaaS serves as the layer of the Cloud which the vast majority of consumers utilize. Built on top of both IaaS and PaaS, Software as a Service provides applications, programs, software and web tools to the public for free or for a price. Accessible via a computer, tablet or smartphone, the SaaS layer of the Cloud encompasses the largest and most accessible layer of Cloud Computing.Every time you use the Google Play Store, the App Store, Dropbox, Salesforce, Adobe Cloud Suite, Spotify or any other Cloud based software which is stored in a web server located in a data center halfway around the world, you are accessing the SaaS layer of the Cloud.As eluded to, the basic premise of SaaS is user friendly software accessed via a computing device of choice stored in a server the world away. A perfect example of SaaS is Microsoft Office 365. Without Microsoft Office 365, a company would be forced to:

- Purchase individual copies of software or software bundles driving up per seat cost
- Worry about per seat software upkeep
- Purchase new versions of software based on a per seat basis

With SaaS enabled Microsoft Office 365:

- SaaS eliminates per seat software purchases. Companies purchase/rent a license to utilize a single version of the software in question which is stored, maintained and updated in a central server.
- SaaS eliminates the need for software maintenance, upkeep or upgrade. As the software is hosted by a parent company, the parent company updates the software and that update filters down the line.
- SaaS enables is scalable. Without SaaS, a company continually purchases new copies of software for new employee. With SaaS, a company rents the license to the software from the hosting company. With new employees, the software is scaled to meet demand.

COMPONENTS OF CLOUD COMPUTING

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers,storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud).The foure types of cloud computing models is shown in figure 1.

The Four Types of Cloud Computing Models

Their exist four types of cloud computing models as shown in the figure….

- Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)
- Community cloud
- Public cloud
- Hybrid cloud

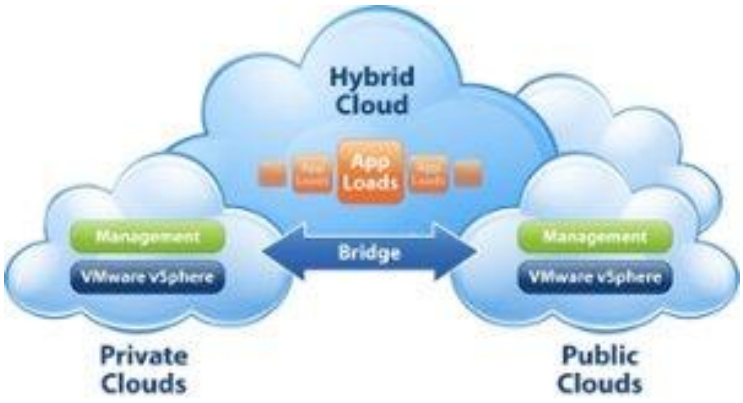

Figure 1: Cloud Types

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider

interaction[2]. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Common Cloud Computing Security Issues

The biggest challenge in cloud computing is to successfully address the security and privacy issues associated with their deployment. The security and privacy problems in cloud computing are mainly due to its multi-tenancy nature and the outsourcing of sensitive data, critical applications and infrastructure onto the cloud. Visual model view of cloud computing is shown in figure 2. There are many concerns from organizations and individuals about how security and privacy can be maintained in the new cloud environment[3].

Affordable, efficient, and scalable, cloud computing is still the best solution for most businesses but it can still leave you vulnerable if the proper precautions aren't taken.

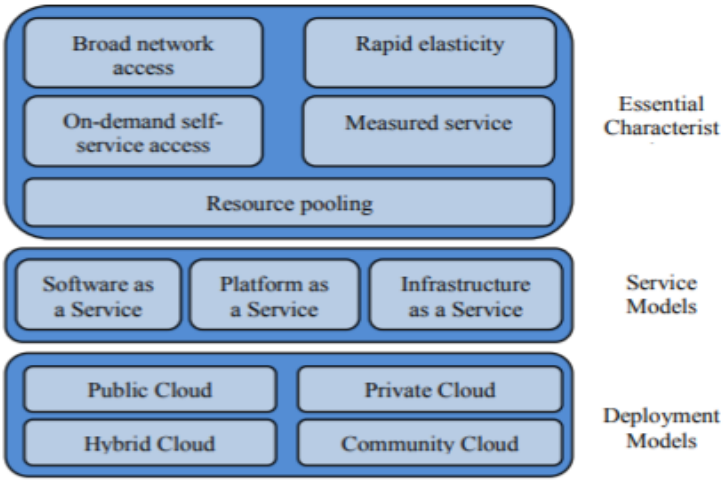

Figure 2: Visual model of cloud computing

Here are six of the most common cloud computing security risks[4]:

1. Distributed-Denial-of-Service Attacks

When cloud computing first became popular, Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable; the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices, smartphones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

2. Shared Cloud Computing Services

Not all cloud hosting solutions and cloud computing services are made equal. Many cloud solutions do not provide the necessary security *between clients*, leading to shared resources, applications, and systems. In this situation, threats can originate from *other clients* with the cloud computing service, and threats targeting one client could also have an impact on other clients.

3. Employee Negligence

Employee negligence and employee mistakes remain one of the biggest security issues for all systems, but the threat is particularly dangerous with cloud solutions. Modern employees may log into cloud solutions from their mobile phones, home tablets, and home desktop PCs, potentially leaving the system vulnerable to many outside threats.

4. Data Loss and Inadequate Data Backups

Inadequate data backups and improper data syncing is what has made many businesses vulnerable to *ransomware*, a specific type of cloud security threat. Ransomware "locks" away a company's data in encrypted files, only allowing them to access the data once a ransom has been paid. With appropriate data backup solutions, companies need no longer fall prey to these threats.

5. Phishing and Social Engineering Attacks

Due to the openness of a cloud computing system, phishing and social engineering attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can potentially break into a system with ease -- as the system itself is available from anywhere. Employees must be knowledgeable about phishing and social engineering enough to avoid these types of attackS.

6. System Vulnerabilities

Cloud computing systems can still contain system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms. Once a vulnerability becomes known with a popular third-party system, this vulnerability can be easily used against organizations. Proper patching and upgrade protocols -- in addition to network monitoring solutions are critical for fighting this threat. Cloud computing security issues are not insurmountable; in fact, many of the risks above can be protected against through the use of a dedicated data protection service. Cloud data protection solutions will both protect data from loss and against cyber security threats, allowing businesses to leverage the power of the cloud without the associated risk.

CLOUD SECURITY THREATS

Cloud computing continues to transform the way organizations use, store, and share data, applications, and workloads. It has also introduced a host of new security threats and challenges. With so much data going into the cloud and into public cloud services in particular these resources become natural targets for bad actors[5]. The volume of public cloud utilization is growing rapidly, so that inevitably leads to a greater body of sensitive stuff that is potentially at risk. The main responsibility for protecting corporate data in the cloud lies not with the service provider but with the cloud customer. We are in a cloud security transition period in which focus is shifting from the provider to the customer, Heiser says. Enterprises are learning that huge amounts of time spent trying to figure out if any particular cloud service provider is 'secure' or not has virtually no payback.

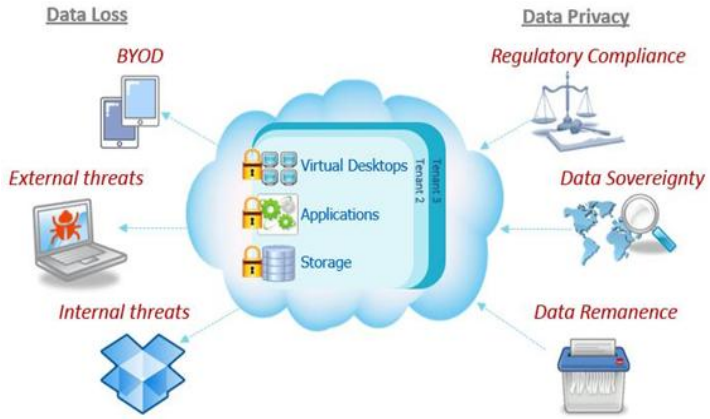

Figure 3 : Type of threats in cloud data

To provide organizations with an up-to-date understanding of cloud security concerns so they can make educated decisions regarding cloud adoption strategies, the Cloud Security Alliance (CSA) has created the latest version of its Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights report.

The report reflects the current consensus among security experts in the CSA community about the most significant security issues in the cloud. While there are many security concerns in the cloud, as shown in figure 3, CSA says, this list focuses on 12 specifically related to the shared, on-demand nature of cloud computing.

To identify the top concerns, CSA conducted a survey of industry experts to compile professional opinions on the greatest security issues within cloud computing. Here are the top cloud security issues (ranked in order of severity per survey results):

1. Data breaches

A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices, CSA says. It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property. An organization's cloud-based data may have value to different parties for different reasons. The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

2. Insufficient identity, credential, and access management

Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source, CSA says. As a result, insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

3. Insecure interfaces and application programming interfaces (APIs)

Cloud providers expose a set of software user interfaces (UIs) or APIs that customers use to manage and interact with cloud services. Provisioning, management, and monitoring are all performed with these interfaces, and the security and availability of general cloud services depends on the security of APIs, CSA says. They need to be designed to protect against accidental and malicious attempts to circumvent policy.

4. System vulnerabilities

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a system to steal data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system put the security of all services and data at significant risk, CSA says. With the advent of multi-tenancy in the cloud, systems from various organizations are placed close to each other and given access to shared memory and resources, creating a new attack surface.

5. Account hijacking

Account or service hijacking is not new, CSA notes, but cloud services add a new threat to the landscape. If attackers gain access to a user's credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information and redirect clients to illegitimate sites. Account or service instances might become a new base for attackers. With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

6. Malicious insiders

While the level of threat is open to debate, the fact that insider threat is a real adversary is not, CSA says. A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on cloud service providers for security are at greater risk.

7. Advanced persistent threats (APTs)

APTs are a parasitical form of cyber attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives, CSA says.

8. Data loss

Data stored in the cloud can be lost for reasons other than malicious attacks, CSA says. An accidental deletion by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, following best practices in business continuity and disaster recovery.

9. Insufficient due diligence

When executives create business strategies, cloud technologies and service providers must be considered, CSA says. Developing a good roadmap and checklist for due diligence when evaluating technologies and providers is essential for the greatest chance of success. Organizations that rush to adopt cloud technologies and choose providers without performing due diligence expose themselves to a number of risks.

10. Abuse and nefarious use of cloud services

Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models to malicious attacks, CSA says. Bad actors might leverage cloud computing resources to target users, organizations, or other cloud providers. Examples of misuse of cloud-based resources include launching distributed denial-of-service attacks, email spam, and phishing campaigns.

11. Denial of service (DoS)

DoS attacks are designed to prevent users of a service from being able to access their data or applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space, or network bandwidth, attackers can cause a system slowdown and leave all legitimate service users without access to services.

12. Shared technology vulnerabilities

Cloud service providers deliver their services scalably by sharing infrastructure, platforms or applications, CSA notes. Cloud technology divides the "as-a-service" offering without substantially changing the off-the-shelf hardware/software—sometimes at the expense of security. Underlying components that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture or multi-customer applications. This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models.

13. Bonus cloud threat for 2018: Spectre and Meltdown

In January, researchers revealed a design feature common in most modern microprocessors that could allow content, including encrypted data, to be read from memory using malicious Javascript code. The two variations of this issue, called Meltdown and Spectre, affect all devices from smartphones to servers. It's because of the latter that we are adding them to the most significant cloud threats for 2018, making it a dirty baker's dozen.

Both Spectre and Meltdown permit side-channel attacks because they break down the isolation between applications. An attacker that is able to access a system through unprivileged log in can read information from the kernel, or attackers can read the host kernel if they are a root user on a guest virtual machine (VM).

This is a huge issue for cloud service providers. While patches are becoming available, they only make it harder to execute an attack. The patches might also degrade performance, so some businesses might choose to leave their systems unpatched. The CERT Advisory is recommending the replacement of all affected processors—tough to do when replacements don't yet exist.

So far, there are no known exploits that have taken advantage of Meltdown or Spectre, but experts agree that they are likely and relatively soon. The best advice for cloud providers to guard against them is to make sure all the latest patches are in place. Customers should demand information on how their cloud providers are responding to Meltdown and Spectre.

II. Conclusion

Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. To achieve comprehensive cloud security, Data and cloud infrastructure must be protected against known/unknown attacks across all cloud components. In this survey paper we studied all the possible attacks possible on cloud environment which can harm the user's data. This survey can support the endeavors to provide preventive measures as well as proactive tools in defending the clouds from different threats. Cloud computing infrastructure is changing fast requiring security measures and policies to be updated regularly at the same pace to match the changing behaviour of the clouds.

References

[1]. PankajSareen, "Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.

[2]. Md. Sakib Bin Alam, "Cloud Computing – Architecture, Platform and Security Issues: A Survey",World Scientific News

[3]. Ahmed E. Youssef and ManalAlagee, "A Framework for A Framework for Framework forSecure Cloud ureCloudure Cloud ureCloudComputing Computing Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012

[4]. BhushanRathod, PrashantYelmar, PrachiSarode , " A Survey Paper on Cloud Security Threats Issues and Attack Detection" available from:https://www.researchgate.net/ publication/313222138

[5]. AnamikaChoudhary ,SunitaGodara, "Internet of Things: A Survey Paper on Architecture and Challenges" , IJETSR, June 2017.

[6]. https://www.paranet.com/blog/bid/128265/The-Four-Types-of-Cloud-Computing-Models

[7]. www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for- 2018.html

[8]. www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security- threats/

[9]. Top Threats to Cloud Computing V1.0, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[10]. SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models, http://www.csoonline.com/article/print/660065.

[11]. The Open Web Application Security Project, "10 Risks with Cloud IT Foundation Tier",https://www.owasp.org/index.php/Cloud-10_Risks_with_Cloud_IT_Foundation_Tier, (2009).

[12]. Cloud Computing and Security, A Natural Match, http://www.trustedcomputinggroup.org/files/ resource_files/1F4DEE3D-1A4B-B294- D0AD0742BA449E07/Cloud%20Computing%20and%20Security% 20Whitepaper_July29.2010.pdf, (2010).

[13]. P. A. Karger, "Multi-Level Security Requirements for Hypervisors", ISBN: 0-7695- 2461-3, 21st Annual Computer Security Applications Conference, (2005) December 5-9, pp. – 275. [20] RSA Office of the CTO, "A Proposed Security Archit

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

* Dr.K.Sasikala. " Challenges In Cloud Computing on Security Issues And Solutions." IOSR Journal of Computer Engineering (IOSR-JCE) 20.5 (2018): 46-52.