Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.558 – 563

RESEARCH ARTICLE

Challenges and Security Issues in Cloud Computing

Joshna S[1], Manjula P[2]

[1]Student, Department of Network Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India
[2]Assistant Professor, Department of Information Technology, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India
[1] joshna.cs@gmail.com; [2] manjula.arunraj@gmail.com

Abstract— Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. The aim of this paper is to render a more elaborated and complete understanding of the issues and challenges related to Cloud security and provide major research directions for future to the researchers in concerned areas

Keywords— Cloud Security; Challenges in Cloud Security; Issues in Cloud Security; Vulnerabilities; Threats; Counter measures

I. INTRODUCTION

Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models. The five key characteristics of cloud computing include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service, all of which are geared toward using clouds seamlessly and transparently. The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Software as a Service (SaaS) makes use of a cloud computing infrastructure to deliver one application to many users, regardless of their

location, rather than the traditional model of one application per desktop. It allows activities to be managed from central locations in a one-to-many model, including architecture, pricing, partnering, and management characteristics. With Platform as a Service (PaaS), you can develop new applications or services in the cloud that do not depend on a specific platform to run, and you can make them widely available to users through the Internet. PaaS delivers cloud-based application development tools, in addition to services for testing, deploying, collaborating on, hosting, and maintaining applications. IaaS is the virtual delivery of computing resources in the form of hardware, networking, and storage services. It may also include the delivery of operating systems and virtualization technology to manage the resources [1],[2]. Rather than buying and installing the required resources in their own data centre, companies rent these resources as needed. Cloud deployment models include public, private, community, and hybrid clouds. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers.

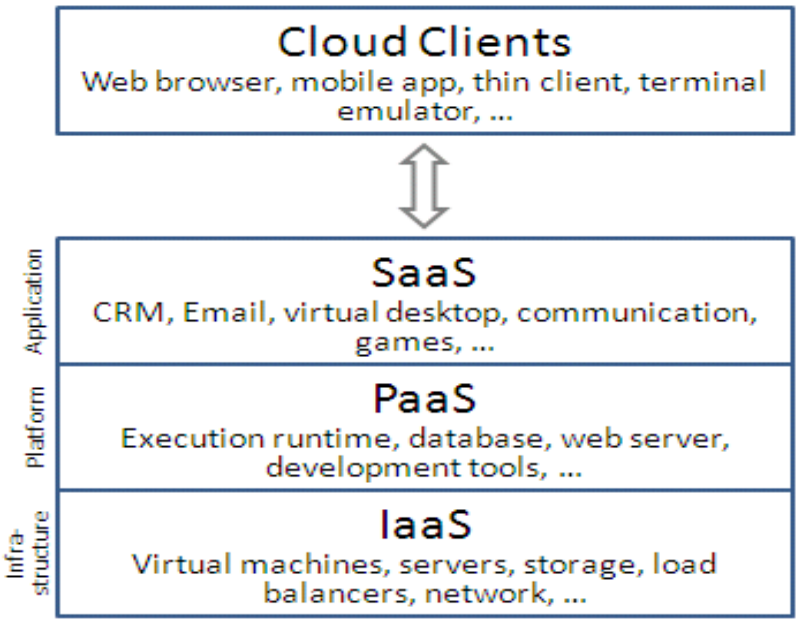

Fig 1. Cloud Delivery Model

II. CLOUD COMPUTING SECURITY ISSUES

Data breaches and account hijackings were in the middle of CSA's 2013 list of top threats rose to the number one and three spots, respectively, this year.[3]-[7] At the same time, denial of service attacks made their debut as the fifth most worrisome threat.

A. Nine critical threats to cloud security

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

1) Data Breaches

One of the top threats to cloud computing is data breaches. All the computer systems connected to the Internet can be accessed by virtually any person. This exposes cloud computing service providers to the threat of skilled hackers with malicious intentions. In 2013 the number of reported cases of server breaches was over 200 and they resulted in the loss of about 9 million data records. More and more breaches are expected as the number of national and international underground hacking communities continues to grow.

2) Data Loss

Another serious threat stems from cloud computing service providers' potential inability to prevent data loss. In our plugged in world, most people know that loss of data is inevitable at one point or another. However, this threat is compounded by the sheer amount of data handled by cloud computing service providers. There is increasing amount of sensitive data relayed to cloud computing firms and this data could get lost in any number of ways, including through accidental deletion or corruption. While interruptions and business continuity can be expensive in terms of lost productivity, the bigger issue may be the way it makes you look in front of your clients. Not only could data loss cause your customers to lose faith and take their business somewhere else; depending on the kind of data lost, it could cause legal issues that could go on for years. In the case of data loss, there's really only one thing you can do is to backup your data. Back it up, monitor that backup, and make sure that if you accidentally lose something that you can restore it with just a few clicks.

3) Account Hijacking

Hijacking of accounts at cloud computing companies is another potentially serious threat. It is usually possible for authorized company personnel to remotely access cloud data via mobile devices or remote computers. The potential for account hijacking, or data hijacking, increases when employees are accessing sensitive information via remote platforms that don't necessarily have the security mechanisms in place that would otherwise exist at a workstation computer. Traffic hijacking is a threat to any type of Internet-based service, not specifically cloud computing. Two of the key protocols that make the Internet work, DNS and Border Gateway Protocol (BGP), can both be used to launch traffic hijacking attacks by using fundamental flaws in the protocols themselves. BGP, for example, which calculates the quickest, most efficient route for Internet traffic to travel in order to reach the destination IP address, can be subverted by abusing the trust relationship established by default between low-level Internet protocols.

4) Insecure application programming interfaces (APIs)

Insecure application programming interfaces (APIs) are another threat to cloud computing. These interfaces offer ways for programs to communicate with each other and their security is not always completely guaranteed. The loopholes in security might grant people with malicious intentions access to sensitive information passing through the communication channel.

5) Denial of Service

Although it doesn't gravely affect integrity of the data stored in cloud computing servers, denial of service can temporarily deny access of data to legitimate users. It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable. While DDoS attacks tend to generate a lot of fear and media attention, they are by no means the only form of DoS attack. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases, or other cloud resources, allowing a malicious individual to take out an application using a single extremely small attack payload – in some cases less than 100 bytes long. Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there's no way to get to your destination, and nothing you can do about it except sit and wait. As a consumer, service outages not only frustrate you, but also force you

to reconsider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile after all.

6) Malicious Insiders

The potential for malicious insiders should be taken seriously. The incredible growth of cloud computing has to have led to short cuts by some providers when it comes to checking the credentials of new employees. A malicious or disgruntled employee could try to instigate a traffic hijacking attack or harvest data some other way. If unauthorized users gain access to your credentials, for example, they could monitor your activities and redirect your clients to other sites.

7) Abuse of Cloud Services

One of cloud computing's greatest benefits is that it allows even small organizations access to vast amounts of computing power. It would be difficult for most organizations to purchase and maintain tens of thousands of servers, but renting time on tens of thousands of servers from a cloud computing provider is much more affordable. However, not everyone wants to use this power for good. It might take an attacker years to crack an encryption key using his own limited hardware, but using an array of cloud servers, he might be able to crack it in minutes.

8) Insufficient Due Diligence

Cloud computing has brought with it a gold rush of sorts, with many organizations rushing into the promise of cost reductions, operational efficiencies and improved security. While these can be realistic goals for organizations that have the resources to adopt cloud technologies properly, too many enterprises jump into the cloud without understanding the full scope of the undertaking.

9) Shared Technology Issues

Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms, and applications. Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models. 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 misconfiguration can lead to a compromise across an entire provider's cloud.

B. Steps to reduce the risk of suffering security breaches

1. Authenticate all people accessing the network.
2. Frame all access permissions so users have access only to the applications and data that they've been granted specific permission to access.
3. Authenticate all software running on any computer — and all changes to such software. This includes software or services running in the cloud. Your cloud provider needs to automate and authenticate software patches and configuration changes, as well as manage security patches in a proactive way. After all, many service outages come from configuration mistakes.
4. Formalize the process of requesting permission to access data or applications. This applies to your own internal systems and the services that require you to put your data into the cloud.
5. Monitor all network activity and log all unusual activity. Deploy intruder-detection technology. Even if your cloud services provider enables you to monitor activities on its environment, you should have an independent view. Even when cloud operators have good security (physical, network, OS, application infrastructure), it is *your* company's responsibility to protect and secure your applications and information.

6. Log all user activity and program activity and analyze it for unexpected behavior. Nearly 70 percent of security breaches are caused by insiders (or by people getting help from insiders). Insiders rarely get caught.
7. Encrypt, up to the point of use, all valuable data that needs extra protection.

III. CLOUD COMPUTING CHALLENGES

Some common challenges [8]-15] to cloud Computing are:

1. Data Protection

Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

- Appropriate clustering and Fail over
- Data Replication
- System monitoring
- Maintenance
- Disaster recovery
- Capacity and performance management

3. Management Capabilities

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like "Auto-scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

4. Regulatory and Compliance Restrictions

In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

IV. CONCLUSIONS

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures.

REFERENCES

[1] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", *IDC eXchange*, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].
[2] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." *Infoworld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1>
[Mar. 13, 2009].Kuyoro S. O., Ibikunle F. & Awodele O.International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 254
[3] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010
[4] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].
[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[6] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
[7] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.
[8] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul., 2010.
[9] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[10] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.
[11] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]
[12] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." *KM World*, pp14-22.
[13] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.
[14] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
[15] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." *IEEE Xplore*, pp 23-31, Jun. 2009.

AUTHORS PROFILE

Ms. S. Joshna is currently a student of Vel Tech Multi Tech Dr. Rangarajan Dr.Sakunthala Engineering college, Chennai and she is doing her Masters in "Network Engineering". She received her Bachelor's degree in Computer Science from Karpagam College of Engineering in 2012, Coimbatore. Her areas of interest are Ad Hoc networks, WSN and Network Security. She has published several research journals in Wireless Sensor Networks and Ad Hoc Networks.

Mrs. P. Manjula received her M.Tech in Information Technology from Sathyabama University in 2007. She received her Bachelor's degree in Information Technology from AVC Engineering College, Mayiladuthurai in 2003. She is currently doing her Ph.D. in Veltech University. Her area of research includes Wireless Sensor Networks, Network Security and Ad-Hoc networks. . She has published several research journals in Wireless Sensor Networks, Network Security and Ad Hoc Networks.

