IJETST- Vol.||03||Issue||11||Pages 4747-4752||November||ISSN 2348-9480 2016

Open access Journal International Journal of Emerging Trends in Science and Technology

IC Value: 76.89 (Index Copernicus) Impact Factor: 2.838 DOI: https://dx.doi.org/10.18535/ijetst/v3i11.04

Security Issues in Cloud Computing

Author
Sreejit Dutta
VIT University, Vellore, Tamil Nadu 632014, India
Email: *sreejit.dutta@gmail.com*

Abstract

Sharing of resources like processing, data, services etc. through a web based delivery system constitutes the concept of a cloud based computing normally. The supplier presents all its resources via the web which may be accessed by the buyer on multiple devices and platforms on-demand. These will be simply provisioned as per demand with very little or no effort. Examples of cloud computing resources are Google Maps by Google, Amazon Web Services by Amazon and so on. Over the past few years, there has been an exponential growth within the field of cloud computing because the need for services on-the-go for mobile platforms has seen a speedy increase in demand. This successively has spurred the requirement for multiplied security measures for cloud computing. Security is the primary issue for cloud as well as other internet services. The primary reason preventative of a complete adoption of cloud computing is in truth the various security problems it comes with, despite however useful it's going to be. A number of these problems like knowledge breach, hacking, malware, DoS attacks are fairly acquainted and almost like the protection issues of a familiarweb services and systems. Whereas threats like abusing cloud services, APT parasites etc are specific to cloud computing. The end-user of cloud services can perpetually be troubled by the protection, vulnerabilities and convenience of their knowledge on cloud servers. The principal objective of this paper is to debate such threats and vulnerabilities in cloud computing. This study will modify customers, vendors as well as fellow researchers to have an insight regarding key issues associated with cloud security.

Keywords: *Cloud computing, Cloud Computing Security, Knowledge privacy, Vulnerabilities, Threats, Data breach, Cloud service.*

Introduction

The rise of the web and its connected services has led to lots of development and analysis within the field of cloud computing. Cloud computing has become a progressively vital service in recent years owing to its extreme usability and omnipresent nature of delivery. The arrival of the web age has successively demanded such a service that is accessible throughout the globe on multiple devices facilitating a similar services on every device connected. The buyer and vendor relation has improved because of cloud computing. The buyer may be additionally specific regarding their needs which may be simply communicated to the seller. The seller will effortlessly offer its services to multiple customers, neutering and tweaking parts of the service as and once needed. “In a cloud based computing infrastructure, the resources are usually in somebody else's premise or network and accessed remotely by the cloud users.” [17] The processing is largely done on cloud servers of the seller whereas the user solely provides the seller with mostly knowledge and different info relating to the computation and process. This knowledge is kept on the cloud servers of the seller. Scalability is one of the most important blessings of cloud computing. There are three major styles of services that represent cloud computing, namely:

1. Software as a Service (SaaS): It's typically hosted centrally and accessed by users supporting a subscription. With SaaS, there's no need for a

firm to run applications on their own servers or data centers.

2. Infrastructure as a Service (IaaS): In IaaS model, a third-party supplier hosts hardware, software, servers, storage and different infrastructure parts for its customers and provides the applications to manage it.

3. Platform as a Service (PaaS): Typically, in PaaS the supplier provides the hardware in terms of servers, data centers and applications for development as software.

Companies areopting a cloud based delivery system as a result of most cloud based IT solutions need one to acquire specific resources to be used and not for the complete resource. This considerably reduces the value and conjointly allows easier management. Cloud services facilitate a company to satisfy the apace ever-changing desires of ever growing market, giving them a foothold and ensuring they're in-par with fellow competitors. Cloud computing enhances the market convenience of corporations and likeability among the users of the services. Corporations like Google, Yahoo, Amazon, and Microsoft have sharply been operating towards the development, preparation and providing cloud services that have are the foremost technologically advanced and up to standards. Not solely do they cater to the wants of huge firms but as well for the small and mid-size industries, resulting in a generation of startups that doesn't have to worry regarding the physical aspect of the company, i.e. buyingdata centers, servers and different connected hardware. All this can be taken care of by cloud suppliers and also the startups and individualsonlyhave to worry regarding their own computer code and concepts permitting them to have faith in their business growth and not the physical resources.

Service Models

Cloud Service models are divided into 3 subparts:

1. Software-as-a-Service (SaaS): “SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on their own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support.”[3]All the IT infrastructure like the software package, servers, network, data center, power are the responsibility of the vendor and is to be provided once the user subscribes to the service. The seller ought to conjointly offer upgrades, patches, backups moreover to the buyer. Google apps, Salesforce.com areexamples of SaaS.
2. Platform-as-a-Service(PaaS): “PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users.”[5]PaaS encompasses a high-level integration of cloud infrastructure, chiefly for the aim of testing and implementing cloud services. Management of the infrastructure lies with the seller but the user is entirely to blame for management of the configurations and applications that are deployed. Examples: Google App Engine, Microsoft Azure.
3. Infrastructure-as-a-Service (IaaS):
   Infrastructure as a Service is the sharing of hardware resources by the means of virtualization. Servers, information centers and networks are simply accessible and configurable on-demand. The customer pays for the maximum amount of usage and not for the whole data center or cloud. The suppliers provides solely the hardware and tools to manage the software however the management of application rests with the user.

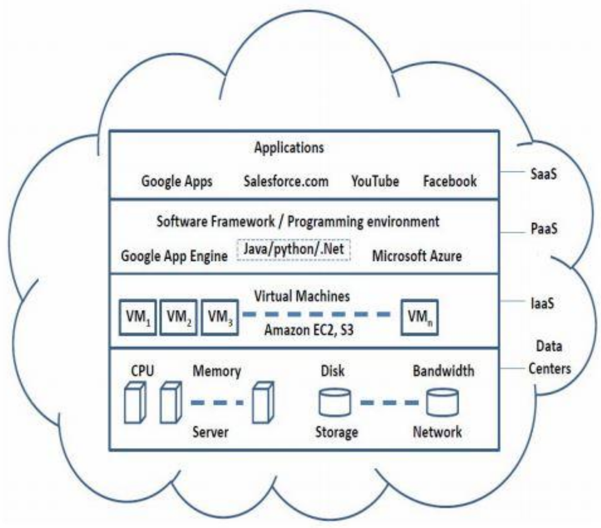

Figure 1. High level view of cloud service models

Security Issues in Cloud Computing

There are numerous parts in cloud computing like applications, platforms and infrastructure. Every one of them contains a completely different functionality and might supply differing types of services and products. A lot of variety of applications of cloud suggests that there would be a lot of security problems. The integration of various parts and technologies makes it difficult to own a secure cloud service. A number of these services are databases, virtualization, operating systems, networks, scheduling, transactions, backups, load balancing, concurrency and memory management. There is also completely different security problems for every of the systems and technologies. For example- The information must be secure because it contains all the sensitive information stored by the user and it may be attacked or infiltrated by a hacker. All information shouldn't solely be encrypted however it ought to be madesure that there are specific protocols and policies once information is shared and retrieved or stored.The primary issues of security are:

1. **Server & Application access:** Unlike traditional data centers where the access to servers is merely on-the-scene, in cloud computing the admin access is through the web. This will increase the chance of a breach. Thus it's necessary to rigorously monitor and manage all administrative access in cloud computing. All security policies ought to be made clear between the vendor and the user.
2. **Data Transmission:** A large quantity of information transmission takes place in cloud computing. These include transmissions between the vendor and the user, user to user transmission and user to third-party transmission. Encryption is probably the simplest way to ensure all data transmissions are secure and also the information reaches the supposed destination without altering and modification maliciously. Any attacker will place themselves between the vendor and user to steal information while not letting either parties comprehend the breach, this is often referred to as man-in-the-middle attack. Auditing and limiting access of information by means of access controls and levels as well as authentication management ensures in security of the data.
3. **Virtual Machine Security:** Virtualization techniques are one of the major advantages of cloud computing. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. [11] This dynamic nature of virtualization and VMs increases the security challenge to making sure total VM security. There are a lot of vulnerabilities and errors. The root access to a Virtual Machine and a Virtual Machine Monitor should be extremely restricted and secure and the guest session should not have the privilege of root access,
4. **Network Security:** Security threats related to networks are DNS attacks, sniffer attacks, reused IP address etc.

Sometimes when a server is called by name, the user is sent to a different server instead of the one asked for. We can use DNSSEC to reduce the effect of DNS threats. Sniffer attacks capture packets which go through networks or routers. Usually these packets are not encrypted, making it easier for attackers to catch them and retrieve any data and information stored.

5. **Data Security:** HTTP is the preferred mode of protocol in cloud computing for exchange of data and information, however HTTP is not a secure link. HTTPS is therefore adopted to make sure a secure connection is taking place. Strong encryption techniques should be adopted to get rid of vulnerabilities and threats. Cryptography should keep on advancing with development of newer and better encryption/decryption techniques as the older ones are constantly cracked and deciphered by attackers.
6. **Data Privacy:** Privacy of data is one of the key concerns of the user. The responsibility of making sure that no data is leaked and is confidential between the user and the vendor is important not only for building trust but for legal reasons as well.
7. **Data Integrity:** Corruption of stored data at any level can occur. Integrity of data should be monitored constantly. There should be backups of data as well in case of corruption so that previous versions can be restored. Multiple storage and backup locations maybe used to make sure consistency and durability of data.
8. **Physical Security:** As much as security of data is important on the software level, physical security is important as well. This includes guarding data centers at the hardware level, preventing insider trading and information sharing, not letting malicious persons enter premises etc.
9. **Shared Technology:** When technology is shared between multiple organizations, cloud providers, users, there is an increased risk of threat and vulnerabilities. A common shared security protocol and policies can ensure that all transactions between organizations is a secure one.

Cloud Security Architecture

There is a constant evolution of cloud computing technologies making it almost impossible to agree upon the same set of guidelines and principals for security. It is important to do so. A base plan should be put in place for treating security as a major concern. A proper architecture to develop specific secure protocols and policies between parties is vital to data security. There should be necessary steps taken for involving all the parties in the decision making process for orchestration of the security policies. Firewalls, encryption, Key management, sign on information, security testing, SSL should all be discussed. Security of the cloud should be an automated process, meaning that the system should itself be able to manage it. The first layer is a protective one where the system has to detect and stop all intrusions, the second would be a preventive one where the system tries to restrict the attacker from gaining complete access, the third and final must be going offline in case of a complete breach. The system should be able to cutoff the connection and prevent any data loss if there is a complete lapse of security and access to all information is acquired by an attacker.

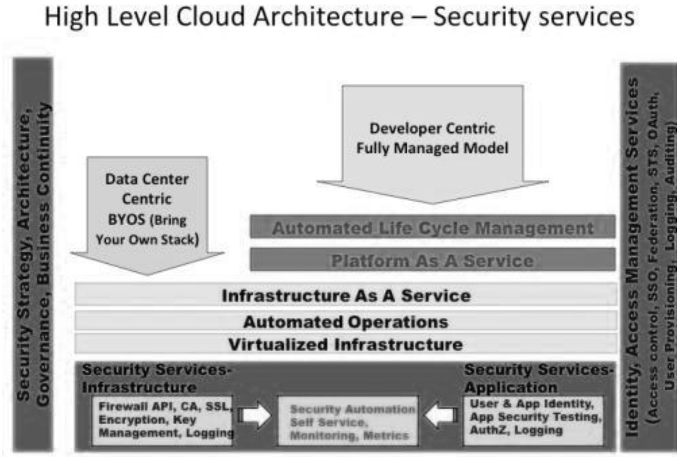
High Level Cloud Architecture – Security services
Security Strategy, Architecture, Governance, Business Continuity
Data Center Centric BYOS (Bring Your Own Stack)
Developer Centric Fully Managed Model
Automated Life Cycle Management
Platform As A Service
Infrastructure As A Service
Automated Operations
Virtualized Infrastructure
Security Services-Infrastructure
Firewall API, CA, SSL, Encryption, Key Management, Logging
Security Automation Self Service, Monitoring, Metrics
Security Services-Application
User & App Identity, App Security Testing, AuthZ, Logging
Identity, Access Management Services
(Access control, SSO, Federation, STS, OAuth, User Provisioning, Logging, Auditing)

Fig. 2 Cloud Security Architecture [24]

Conclusion

Security of cloud services is one of the major challenges in cloud computing and it is of utmost importance to deal with it cautiously. There should be no lapse in the security measures and necessary resources should be allocated for ensuring the enforcement of proper measures and policies. The trust between a user and vendor can only be made concrete if the user fully understands and is aware of the security measures undertaken by the vendor. The vendor should make the user aware of the security policies and should be transparent about how the data is handled in each step of cloud computing, without however revealing too much specific details so as to not compromise and jeopardize the data of the enter user-base of the vendor. In this paper we discussed the major challenges of cloud security like data transmission, virtualization, access control etc. With the progress of time attackers and hackers crack the existing security controls in place so it is important to develop and update existing policies time to time so as to ensure complete security of data.

Acknowledgements

The writers of this paper would like thank VIT University for its constant guidance and help provided in writing this study as well as supporting the unhindered progress in the field of research related to various disciplines.

References

1. A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
2. Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.
3. R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
4. B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.
5. Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.
6. Pring et al., “Forecast: Sizing the cloud; understanding the opportunities in cloud services,” Gartner Inc., Tech. Rep. G00166525, March 2009.
7. AmanBakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.
8. B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE

SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

9. K. Hwang, S Kulkarni and Y. Hu, “Cloud security with virtualized defence and Reputation-based Trust management,” Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Chengdu, China, December, 2009. ISBN: 978-0-7695- 3929 -4.
10. R. Gellman, “Privacy in the clouds: Risks to privacy and confidentiality from cloud computing,” The World Privacy Forum,2009.http://www.worldprivacyforum.org/pdf/WPF_Cloud_ Privacy_Report.pdf.
11. Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009
12. L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.
13. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’ Reilly Media, USA, 2009.
14. Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010
15. K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.
16. Marios D. Dikaiakos, DimitriosKatsaros, Pankaj Mehra, George Pallis, Athena Vakali, “Cloud Computing: Distributed Internet Computing for IT and Scientific Research,” IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.
17. A. Williamson, “Comparing cloud computing providers,” Cloud Comp. J., vol. 2, no. 3, pp. 3–5, 2009.
18. X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, “Information Security Risk Management Framework for the Cloud Computing Environments”, In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.
19. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing,” 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4
20. Hanqian Wu, Yi Ding, Winer, C., Li Yao, “Network Security for Virtual Machines in Cloud Computing,” 5th Int’l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3.
21. S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.
22. V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran “Research Issues in Cloud Computing “ Global Journal of Computer Science and Techn-ology, Volume 11, Issue 11, July 2011.

Website(s)
https://www.infoq.com/articles/cloud-security-architecture-intro