Cloud Computing: Security Issues

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : September

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:
Manigandan, R. (2018). Cloud Computing: Security Issues. *Shanlax International Journal of Arts, Science and Humanities*, 6(S1), pp.115–123

DOI:
https://doi.org/10.5281/zenodo.1411009

R.Manigandan
M.Phil.,Research Scholar, Department of Computer Science
Morappur Kongu College of Arts and Science

Abstract

Cloud computing is an architecture which provides computing service through the internet on demand and pays per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied, etc. Cloud computing is an internet dependent technology where client data is stored and maintained in the data center of a cloud. Example Google, Amazon, Salesforce.som and Microsoft, etc. Limited control over the data may occur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. Various research also challenges there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper describes the security issues of cloud computing.

Keywords: Security Issues, Cloud Security, Data Protection.

Introduction

Cloud Computing is a distributed architecture that has centralized server resources on a scalable platform. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services. It is same as internet service with high-speed broadband to access the internet. CSPs and Internet Service Providers both offer services. Cloud activates on-demand network access to a shared pool of configurable computing resources with minimal management effort or service provider's interaction. In general cloud providers offer three types of services.T hey are Software as a Service, Platform as a Service and Infrastructure as a Service. There are various reasons for organizations to move towards IT solutions because that includes cloud computing as they are just required to pay for the resources on a consumption basis. Also, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [1].

Cloud computing appeared to satisfy the business necessity, being animated by the idea of just using the infrastructure without managing it. Although initially, this idea was present only in

the academic area, recently, it was transposed into an industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via a lightweight, portable devices such as mobile phones, PCs and PDAs.

Clouds are the new trend in the evolution of the distributed systems, the predecessor of the cloud being the grid. The user does not require knowledge to control the infrastructure of clouds; it provides the only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through a web browser [2].

Building Blocks of Cloud Computing

Models of Cloud Computing

Cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software as a Service: It can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer get rid of installing and operating the application on own computer and also eliminates a tremendous load of software maintenance; continuing operation, safeguarding and support [3]. SaaS vendors take the responsibility for deploying and managing the IT infrastructure and processes required to run and manage the full solution. SaaS features a complete application offered as a service on demand.

Platform as a Service: It provides the runtime environment for applications. It also provides development and deployment tools required to develop applications. PaaS consist of point and click tools that enable non-developers to create web applications.

Infrastructure as a Service: It refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. It provides basic infrastructure on-demand services using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. The user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service providers own the equipment and responsible for housing, running and maintaining it and the client has to pay-per-use.

Deployment Models of Cloud Computing

Private cloud: It can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security. Examples of a private cloud are Eucalyptus Systems [4].

Public Cloud: Cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider. Customers are only charged for the resources they

use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Examples of a public cloud include Microsoft Azure, Google App Engine.

Hybrid Cloud: It is a combination of two or more cloud deployment models, linked each other and data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [5]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments and employee payroll processing. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. Example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by several organizations based on an agreement between related business organizations and operates according to this model may exist locally or remotely. May be managed by them or a third party service provider and rarely offered cloud model. Example of a Community Cloud includes Face book.

Cloud Computing Entities

Cloud providers and consumers are the two main entities in the business market and service brokers and resellers are the two service level entities in the Cloud world. These are discussed as below.

Cloud Providers: It consists of Internet service providers, telecommunications companies, and large business process outsourcers that provide either the media or infrastructure that enable consumers to access cloud services. Service providers may also include systems integrators that build and support data centers hosting private clouds and they offer different services to the consumers, the service brokers or resellers [6].

Cloud Service Brokers: It consists of technology consultants, business professional service organizations, registered brokers and agents, and influencers that help guide consumers in the selection of cloud computing solutions. Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure and they add extra services on top of a Cloud provider's infrastructure to make up the user Cloud environment.

Cloud Resellers: If the Cloud providers want to expand their business across continents then may choose local IT consultancy firms or resellers for their Cloud-based products in a particular region.

Cloud Consumers: End users are called Cloud consumers. Cloud service brokers and resellers are also customers of another Cloud provider, broker or reseller.

Security Issues in Cloud Computing

Cloud computing consists of applications, platforms and infrastructure. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service, Utility Computing, Web Services, Platform as a Service, Managed Service Providers (MSP), Service Commerce and Internet Integration. Cloud computing includes several security issues and technologies like networks, databases, operating systems, virtualization, etc.,

Example: The network that interconnects the systems using cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data and ensuring the appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers and Applications: cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is related to security policies. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its security policies based on which each employee can have access to a particular set of data. Some of the employees are not given access to a certain amount of data by security policies. These security policies must be adhered to by the cloud to avoid intrusion of data by unauthorized users [9].

Most companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest cloud application adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With cloud application, the software is hosted outside of the corporate firewall. Many times user credentials are stored in the cloud application provider's databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to disable accounts as employees leave the company.

Data Transmission: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment to process data, for any application that data must be unencrypted. In a full homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. For providing confidentiality and integrity of data cloud provider uses the access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at the cloud provider. Man-in-the-middle attacks are the cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

Virtual Machine Security: Virtualization is the main component in a cloud. Virtual machines are dynamic. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization and they can be readily cloned and effortlessly moved between physical servers. Vulnerabilities or configuration errors may be unknowingly propagated and it is difficult to maintain an auditable record. Full Virtualization and Para Virtualization are two

kinds of virtualization in a cloud computing paradigm. In full virtualization, the entire hardware architecture is replicated virtually. In para virtualization, an operating system is modified to run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Xen can be exploited by root users of a guest domain to execute arbitrary commands. The other issue is the control of the administrator on the host and guest operating systems. Current VMMs do not offer perfect isolation. Virtual machine monitor should be root secure, meaning that no privilege within the virtualized guest environment permits interference with the host system.

Network Security: Networks are classified into shared and non-shared, public or private, small area or large area networks and each of them has a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server performs the translation of a domain name to an IP address. The user has been routed to some other evil cloud instead of the one he asked for and using IP address is not always feasible. DNS security measures like Domain Name System Security Extensions reduces the effects of DNS threats but inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems. Sniffer attacks are launched by applications and it captures packets flowing in a network, if the data that is being transferred through these packets are not encrypted, it can be read and vital information is flowing across the network can be traced or captured. A sniffer program, through the Network Interface Card, ensures that the data/traffic linked to other systems on the network also gets recorded. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [11].

When a particular user moves out of a network, then the IP-address associated with him is assigned to a new user. Sometimes old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user [12].

Data security: In cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure and Secure Shell (SSH) is the most common adoption. In cloud computing, the enterprise data is stored outside the enterprise boundary so the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon. Elastic Compute Cloud Administrators use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. The data at rest in Simple Storage Service is not encrypted, users can encrypt their data before it is uploaded to Amazon Storage Service.

Data Privacy: The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns

about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its potential risks [14].

Data Integrity: Data corruption can happen at any level of storage, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database and maintained via database constraints and transactions. Transactions should follow atomicity, consistency, isolation and durability properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

Data Location: cloud service providers have data centers around the globe. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In a distributed system, there are multiple databases and multiple applications [15].

In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail-safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

Data Availability: data at remote systems owned by others, data owners may suffer from system failures of the service provider and If the Cloud goes out of operation, data will become unavailable for that single service provider. So the Cloud application involves making architectural changes at the application and infrastructural levels to add scalability and high availability for that a multitier architecture needs to be adopted and supported by a balanced load farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to the denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies. Data Segregation: The cloud data is in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems because some customers may not want to encrypt data because sometimes encryption accident can destroy the data. So make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals [16].

Security Policy and Compliance: A cloud service provider does not adhere to security audits; then it leads to a decrease in customer trust. Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, GLBA and auditing practices such as SAS70 and ISO.So they need to prove compliance with security standards, regardless of the location of the systems required to be in the scope of regulation, on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources. An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail.

Securing Data Storage: The service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in

transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS, i.e., data stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks, so the cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self-encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact [17].

Patch Management: Once an enterprise subscribes to a cloud computing resource by creating a Web server from templates offered by the cloud computing service provider then the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor-supplied patches. If patching is unmanageable, then compensating controls such as "virtual patching" need to be considered.

Conclusion and Feature Work

The biggest security issue with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues in cloud computing. Due to the complexity of the cloud, it will be difficult to achieve end-to-end security. So new security techniques need to be developed and older security techniques needed to be improved to work with the clouds.

References

Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in V*irtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conferen*ce on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

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

Gellman, R, "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.

Grossman, R.L., "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

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.

Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

K. Hwang, S Kulkarni and Y. Hu, (2009), "Cloud security with virtualized defense 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.

K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, (2010), "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43.

Kandukuri, B. R., Paturi, R. V., & Rakshit, A, "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.

Kandukuri, B. R., Paturi R, V, A. Rakshit, (2009), "Cloud Security Issues," In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

Krishna Reddy, V, Thirumal Rao, B, Reddy, L.S.S., & Sai Kiran, P, (2011), "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11.

Kundu, A, Banerjee, C. D., & Saha, P, (2010), "Introducing New Services in Cloud Computing Environment," International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152.

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.

Marios D. Dikaiakos, Dimitrios Katsaros, 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.

Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, (2009), "On Technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India.

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

Pring et al., (2009) "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525.

Ronald L. Krutz, Russell Dean Vines, (2010), "Cloud Security A Comprehensive Guide to Secure Cloud Computing," Wiley Publishing, Inc.,.

Subashini, S, & Kavitha, V, "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.

Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

Williamson, A, (2010), "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.

Zhang,L.J. & Qun Zhou, (2009), "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616.

Web Sources

http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf
https://www.oracle.com/assets/paas-iaas-public-cloud-2140609.pdf
http://ijarcsms.com/docs/paper/volume3/issue7/V3I7-0079.pdf
http://www.ijcsit.com/docs/Volume%207/vol7issue2/ijcsit2016070231.pdf
https://www.coursehero.com/file/p7jr8oa/Consequently-the-service-provider-must-adopt-additional-security-checks-to/
http://ijcsits.org/papers/Vol1no22011/13vol1no2.pdf
https://www.coursehero.com/file/pp1lgs/customer-contracts-laws-and-regulations-driven-by-business-objectives-internal/