Addressing Cloud Computing Security Issues and its Solution

Nirmal Kumar Gupta

Dept. of CSE, Jaypee University Anoopshahr, Anoopshahr, Uttar Pradesh, India

Abstract

The advent of cloud computing has had a major impact on software organization and software architecture design. In recent years, cloud computing has shifted from promising business concepts to one of the fastest-growing sectors in the IT industry. Cloud computing has revolutionized the way companies use information technology internally and externally. Cloud computing has many advantages, such as cost-effectiveness, convenience, availability, scalability, performance, flexibility and greater storage capacity. Despite the potential benefits of cloud computing, organizations are slow to accept due to security issues and challenges. This article discusses the various issues and challenges of cloud computing security and discusses its solutions from a cloud computing perspective.

Keywords

Cloud Computing, Cloud Security, Privacy, Data Security, Challenges

I. Introduction

Cloud computing has become a new computing model that provides virtual hardware and hosted software resources and provides on-demand service. Cloud computing provides the ability to access shared resources and common infrastructure to deliver on-demand services over the network to perform operations that meet the needs of business change. Software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) have become the basic service models for cloud computing [1]. Cloud computing has also introduced a variety of new concepts, such as resource sharing, centralized data sharing, etc., bringing new security challenges. Direct or indirect access to the cloud infrastructure adds vulnerabilities and threats in the cloud [2]. As the cloud becomes more and more popular, security issues have emerged. Due to the availability of resources and the elasticity of the architecture, the cloud is more vulnerable to Distributed Denial of Service (DDoS) attacks. Fig. 1 shows the cloud implementation model, its internal infrastructure (IaaS, PaaS and SaaS) and its basic features [3]. Cloud Community defines four cloud deployment models, namely Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud [4].

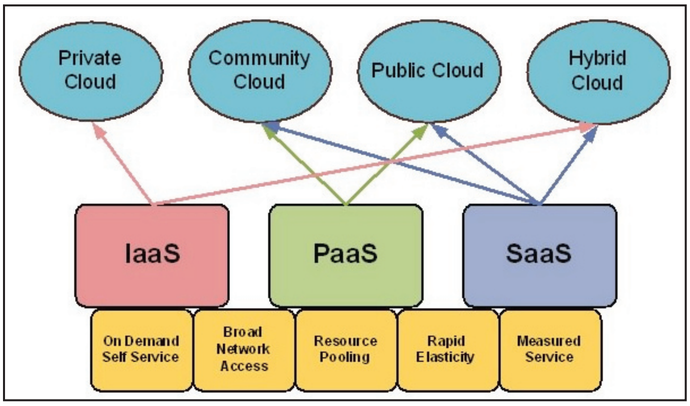

Fig. 1: Cloud Deployment Models and Infrastructure

A. Computing as a Service

One of the foundational principles of cloud computing is the “As a Service” that cloud service providers provide “specific services” to users (customers) for their use. Such services are usually classified according to their scope of application [5]. Here are some examples of application delivery services: Finance, Management, or Analytics. The agreed terms of use indicate that the actions to be taken by service providers and consumers are described in the contract before the service is provided. Failure to comply with this Agreement may result in the Customer denying service or assuming legal liability to the Service Provider. This contract is often described as an agreement regarding the terms of use or service level agreement. In addition, as part of this agreement, service providers also provide a privacy policy that describes how the user’s data will be stored, managed, used and protected.

B. Service Levels

The services offered are often classified using the SPI service model (SaaS, PaaS, IaaS). This model represents the different layers/levels of service that the service providers offer to users across the different application domains and types of clouds available [6]. Clouds can be used to provide a service such as: software to use, development platform or infrastructure to use.

1. Software as a Service

The first and the highest layer is known as software as a service (SaaS). SaaS is a software distribution model in which applications are hosted by a service provider and made available to the customers over a network, usually the Internet. SaaS is becoming an increasingly common delivery model as the underlying technologies that support Web Services and Service Oriented Architecture (SOA) becoming mature and new development approaches become available. SaaS is also often associated with a pay-per-use subscription license model.

2. Platform as a Service

The next layer is known as: Platform as a service (PaaS). This is a development platform that developers can use to write, implement, and manage applications running in the cloud. This can include aspects such as development tools, administration and administration, data management engines and execution, as well as security services and user administration.

3. Infrastructure as a Service

The final and lower layer is known as Infrastructure as a Service (IaaS). IaaS is a single-tenant cloud layer in which cloud provider dedicated resources are only shared with contracted customers at a user-charge rate. This greatly minimizes the need for a large initial investment in hardware such as servers, network devices, and processing power. They also allow for varying degrees of financial and functional flexibility that do not exist in internal data centers or placement services, because IT resources can be added or launched much more quickly and economically than in an internal data center or data center.

II. Security in the Cloud Computing

Wikipedia [7] defines Cloud Computing Security as "Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing."

A. Security Issues Associated with the Cloud

Various security issues are involved for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Security risks in the cloud may differ from traditional IT infrastructure risks, either in nature or intensity or both [8]. The various c cloud computing are shown in fig. 2.

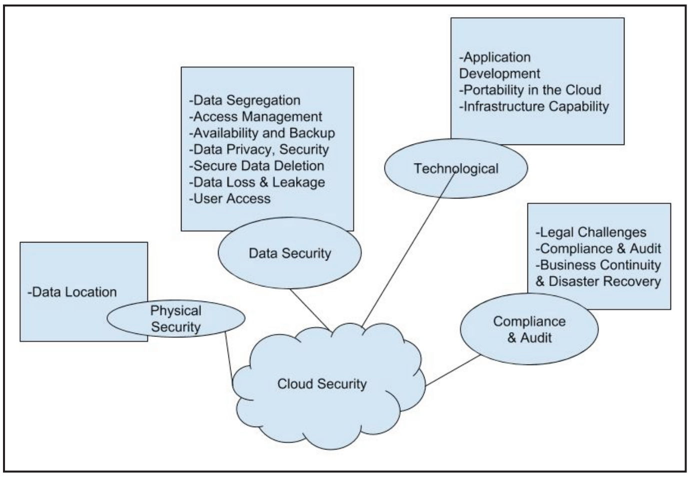

Fig. 2. Various Cloud Security Issues [17]

The pooling of resources allows savings on equipment and therefore indirectly a reduction in electricity consumption thanks to virtualization and multi-lease technologies, but these technologies introduce some risks into the system. Sharing infrastructure between multiple clients leads to the risks of data visibility by other users. In addition, cloud users want to ensure that critical data is not accessible and utilized illegally, even by cloud providers. The on-demand service is provided to clients through web-based interfaces that causes the probability of unauthorized access to the interface which might be higher than the traditional systems. According to Gartner [9], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. According to [10], there are two types of communication, namely, external "customer-to-cloud" communication and internal "cloud-to-cloud" communication. In the first case the cloud services are accessible via the internet using standard internet mechanisms and protocols to transmit data or applications between clients and the cloud. This type of communication is similar to any other communication on the Internet. Indeed, data in transit can be the target of several malicious attacks [9-10]. These attacks include denial of service (DoS), eavesdropping, identity theft, altered environment etc. The second type is related to the communication between the VMs. This communication is targeted for malicious attacks because of the various factors which includes the shared communication infrastructure, the virtual network, and the bad security configuration. The level of security of the public cloud is not optimized for professional use, but its flexibility and value can make it attractive to many small organizations. The Private Cloud is based on the same principle as the public cloud, but it is of course owned by a company and intended for a smaller number of users, customers or partners of the company owner. Finally, the hybrid cloud is a mix of private and public clouds. It is made up of several internal and external partners. Regardless of its type, cloud solution providers rely on a mix of proprietary and open source code to ensure the security and integrity of the data they host and protect. According to [11], whatever the form of the Cloud Computing contract is, this contract must absolutely include these five key points, namely, data localization, law and Jurisdiction, service levels provided by the Cloud Computing provider, reversibility and access to data and data security. In addition, the order of importance of these five key points will vary according to the service used (IaaS, PaaS, SaaS) and its purpose (storage space, development environment, billing tool). According to [12], cloud security challenges are the dispersion of international data and privacy laws, the need to be addressed for various issues like local management, multi-tenancy, logging challenges, data ownership issues, and Guaranteed quality of service, dependence of secure H-viewers, interest for hackers, security of virtual OS in the Cloud, possibility of massive interruptions of service, encryption needs for security in the Cloud, public cloud security versus private cloud security etc. According to [13], there are nine main risks, namely Data Breaches, Data Loss, Account Hijacking, Insecure APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence and Shared Technology Issues. Regarding the legal responsibilities for data security and privacy in the cloud, according to [13], they find that the customer is legally responsible for its data and usage, including anything concerning their compliance with legal obligations, while, the provider is subject to technical and organizational obligations. It is committed to preserving data integrity and confidentiality, protecting and recovering data, encrypting data etc.

III. Cloud Computing Security Concerns

Some of the security concerns discussed below:

A. Loss of Control Over Data

The paradigm of cloud computing is changing the way information is managed, especially with respect to the processing of personal data. Storing personal data on a server somewhere in cyberspace could pose a great threat to privacy. Because tenants and users lose physical control over their data and applications, this raises a number of issues.

B. Data Security and Privacy

With public or community clouds, the data may not remain in the same system, which poses multiple legal problems. The biggest concern that everyone seems to agree with the cloud is security. Data security and privacy are at the forefront of almost all the concerns. The main challenge for cloud computing is how it addresses the security and privacy concerns of the companies that are considering adopting it. The fact that the company's valuable data resides outside the company's firewall raises serious concerns. Piracy and various attacks on the cloud infrastructure would affect multiple clients, even if only one site is attacked. These risks can be mitigated through the use of security applications, encrypted file systems, data loss software and purchase of security hardware to track unusual server behavior.

C. Data Control

Data can reach the provider in several ways with some data belonging to others. A host administrator has a limited scope of control and accountability within a public infrastructure implementation as a service (IaaS), not to mention a platform as a service (PaaS). Hosts must have confidence that their provider will provide adequate control, while recognizing the need to tailor their expectations to the amount of reasonable control in these models.

D. Disaster Recovery and Business Continuity

Hosts and users need the confidence that their operations and services will continue if the cloud provider's production environment is subject to disaster [14].

E. Quality of Service

Quality of service is one of the most important factors that companies consider a reason not to move their commercial applications to the cloud. They consider that SLAs (Service Level Agreements) provided by cloud providers are not currently sufficient to guarantee the requirements to run cloud-based development applications, particularly in terms of availability, performance, reliability and scalability. In most cases, companies are reimbursed for the duration of the non-availability of the service, thus most current SLAs reduce commercial losses [15]. Without a guarantee of service quality, companies will not host their critical infrastructure in the cloud.

F. Transparency

When a cloud provider does not expose the details of its own internal policy or technology, hosts or users must rely on vendor security claims. Hosts and users may still require some transparency from providers as to how they handle security, privacy, and security incidents in the cloud.

G. Legal and Regulatory Compliance

It may be difficult or unrealistic to use public clouds if your data is subject to legal restrictions or regulatory compliance. You can expect vendors to create and certify cloud infrastructures to meet the needs of regulated markets. Achieving certification can be a challenge because of the many non-technical factors, including the current state of general knowledge of the cloud. As best practices for cloud computing encompass a broader scope, this concern should disappear.

H. Incompatibility Issue

The storage services provided by a cloud service provider may be incompatible with the services of another provider in case some user decides to switch from one to the other. Providers are known for creating what the world of hosting calls "persistent services," services that an end user may have difficulty moving from one cloud provider to another.

I. Performance and Cost of Bandwidth

Companies can save money on hardware, but they have to spend more on bandwidth. This can be a low cost for a smaller application, but it can be high for an application that requires a large amount of data. Providing intensive and complex data through the network requires sufficient bandwidth. For this reason, many companies expect a reduced cost before moving to the cloud.

J. New Risks and Vulnerabilities

It is feared that cloud computing will generate new types of risks and vulnerabilities. There are new hypothetical risks, but their true nature will largely depend on the setting up of a supplier. All software, hardware and network equipment are vulnerable to discovering new vulnerabilities. By applying layer security and well-designed business processes, you can protect a cloud against common attacks, even if some of its components are inherently vulnerable.

K. Low Performance of the Network

The provision of complex services through the network is clearly impossible if the bandwidth of the network is not enough. Many companies expect improved bandwidth and lower costs before considering switching to the cloud. Many applications in the cloud still consume too much bandwidth.

L. Integration

Many applications have complex integration needs to connect to other applications in the cloud, as well as other local applications. This includes the integration of existing cloud applications with enterprise applications and existing data structures. It is necessary to connect the application in the cloud to the rest of the company in a simple, fast and profitable way.

IV. Some Solutions to Security Problems in the Cloud

The correct implementation of security measures is mandatory in cloud computing to provide a secure infrastructure that can only ensure and increase confidence that the stored data is safe with the service provider. This can be achieved by the following means:

A. Data Encryption

In the public cloud, resources are shared by multiple users in the cloud and, as a result, the responsibility of their providers is to entrust the separation of data to their customers. Data encryption is a common approach that providers follow to protect their customers' data, but the question is whether the data is stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store critical data, organizations can think of a private or hybrid cloud where the data will be in a secure corporate firewall. An important way to increase data protection, privacy and integrity is to ensure that data is protected in transit and when stored in the cloud by using file-level encryption. As CSA (Cloud Security Alliance) [16] Guidance notes, "Encryption offers the benefits of minimal use of the cloud service provider and dependence on operational failure detection." Encrypted data-centric protection means that data cannot be used by anyone without the key to decrypt it. It does not matter if the data transmits or is stored, it remains protected. The owner of the decryption keys maintains the security of this data and can decide whom to allow access to what data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an administrator could encrypt all data in the backup before sending them to the storage cloud. One of the best security solutions for cloud and virtualized environments is portable encryption at the file level, focused on data on all computer platforms and operating systems, and operates in a private, community, public or hybrid cloud.

B. Restricted Access

Restricted user access can range from simple username/password protection to some challenge-response test in login forms. When an employee no longer needs to access the data center, their access privileges to the data center must be immediately revoked. Cloud providers can also consider password authentication at a time when customers will get a temporary password from the SSN/mobile device, which contributes to data security even if the password is compromised.

C. Installation and Maintenance of the Firewall

Firewalls are an essential component of cloud computing security. Firewall installation and maintenance is required to ensure protection. A firewall must be present on all external interfaces. The evaluation of firewall policies and rule sets and the reconfiguration of the router should be done at regular intervals. Create and implement a firewall that denies access from untrusted sources or applications and correctly records these events. Create and implement a firewall that restricts access to systems with a direct external connection and those that contain sensitive data or configuration data. To accelerate cloud-based applications, we need scalable management to be effective and maximize the benefits of modern firewall capabilities.

D. Backup and Recovery

In cloud computing, the data is stored in a distributed location. Cloud clients will never be able to determine the exact storage location of their records and the importance of data backup and recovery appears. The backup software must include cloud-based APIs, which allows simple backup and recovery in the main cloud storage providers. The backup and restoration services guarantee that one can always recover the data. A questionable question is whether to back up all the data or make a backup of critical and vital data. If the provider agrees to save crucial data, the question is how to determine the priority of the data. The simplest and least complicated way is to protect the entire workstation or server. It is essential that the backup application encrypts confidential data before sending it to the cloud off-site, protecting data in transit through a WAN to a storage location in the cloud and data storage on the site as cloud storage.

E. Access Control

Access control and management of user profiles become more complex with cloud services because information sources can be hosted somewhere other than the cloud service that needs them. Clients must identify reliable sources for this information and ensure mechanisms to transmit information from the reliable source to the cloud service. It is also important to periodically reconcile the information between the cloud service and the source. Customers must confirm that cloud providers support their access control requirements appropriately for cloud resources.

V. Conclusion

Cloud computing has emerged as an important technology for providing Internet services in a simple and efficient way. The main reason for the possible success of cloud computing and the great interest of organizations around the world are due to broad category of services provided with the cloud. But the current technology does not provide all the requirements that cloud computing needs. Researchers face many challenges to make cloud computing work in reality. Besides the various benefits provided through cloud computing some security issues need to be addressed to ensure that it is a safe and reliable services have been provided.

References

[1] Luo, J. Z., Jin J., Song A., Dong F.,“Cloud computing: architecture and key technologies”, Journal of China Institute of Communications 32, No. 7, pp. 3-21, 2011.

[2] Chou T.,“Security threats on cloud computing vulnerabilities”, International Journal of Computer Science & Information Technology 5, No. 3, pp. 79, 2013.

[3] Gong C., Liu J., Zhang Q., Chen H., Gong, Z.,"The characteristics of cloud computing", In Parallel Processing Workshops (ICPPW), 2010 39th International Conference on (pp. 275-279). IEEE, 2010.

[4] Dillon T., Chen W., Chang E.,“Cloud computing: issues and challenges”, In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pp. 27-33. IEEE, 2010.

[5] Krutz, R. L., Vines R.D.,“Cloud security: A comprehensive guide to secure cloud computing”, Wiley Publishing, 2010.

[6] Peter M., Grance T.,“Effectively and securely using the cloud computing paradigm”, NIST, Information Technology Laboratory 2, No. 8, pp. 304-311, 2009.

[7] Wikipedia contributors,“Cloud computing security”, Wikipedia, The Free Encyclopedia, [Online] Available: https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&oldid=811015689 (accessed December 6, 2017).

[8] Mazhar A., Khan S.U., Vasilakos A.V.,“Security in cloud computing: Opportunities and challenges”, Information Sciences 305 (2015): pp. 357-383.

[9] Gartner: Seven cloud-computing security risks. InfoWorld. 2008. [Online] Available: http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

[10] Chen, S., Surya N., Liu R.,“Secure connectivity for intra-cloud and inter-cloud communication”, In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on, pp. 154-159. IEEE, 2011.

[11] Carlos A R., Sousa Rocha Cunha, Juliana Falci,“Some legal aspects of cloud computing contracts”, J. Int’t Com. L. & Tech. 10 (2015): 37.

[12] Nir K.,“Privacy and security issues in cloud computing: The role of institutions and institutional evolution”, Telecommunications Policy 37, no. 4: pp. 372-386, 2013.

[13] Rafal R., Shackleford D., Sullivan B.,“The notorious nine cloud computing top threats in 2013”, Cloud Security Alliance 2013.

[14] Alabdulwahab M,“Disaster Recovery and Business Continuity”, In International Journal of Scientific & Engineering Research, Vol. 7, Issue 3, 2016.

[15] Sujal D., Kagan M., Crupnicoff D.,“Faster and efficient VM migrations for improving SLA and ROI in cloud infrastructures”, DC CAVES (2010).

[16] Catherine E.,“Cloud computing–A question of trust”, Computer Fraud & Security, No. 6, pp. 5-7, 2009.

[17] Latif, R., Abbas H., Assar S., Ali Q.,“Cloud computing risk assessment: A systematic literature review”, In Future Information Technology, pp. 285-295. Springer, Berlin, Heidelberg, 2014.

Nirmal Kumar Gupta, Department of CSE, Jaypee University Anoopshahr, Uttar Pradesh, India