RCES REVIEW OF COMPUTER ENGINEERING STUDIES

A publication of IIETA

IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

http://www.iieta.org/Journals/RCES

ISSN: 2369-0755 (Print), 2369-0763 (Online)
Vol. 4, No. 2, June 2017, pp. 62-66
DOI: 10.18280/rces.040204
Licensed under CC BY-NC 4.0

Security and privacy issues for cloud computing and its challenges

Moumita Sen*, Sasmita S. Choudhury

Department of Computer Science & Engineering, MCKV Institute of Engineering, Liluah 711204, India

Email: moumita02314@gmail.com

ABSTRACT

In Today’s world with the engineering development, Internet connectivity has become a commodity product. With the rapid adoption of Web technologies such as blogging, online media sharing, social networking, it generates enormous quantities of data onto Internet servers. Like traditional infrastructure utilities, such as gas and electricity, “cloud” computing provide computing services via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. It saves managing cost and time for organizations and due to its flexible infrastructure, net centric approach and ease of access, the cloud computing has become prevalent. Today, security issue is the biggest hazards to moving services to external clouds. With cloud computing, data is stored and delivered over the Internet. The owner of the data does not have the control over the data even, does not know the location of the data and limited control over the data may incur various security issues and threats. Hence we discusses different security issues, its privacy and risk in a cloud and also suggests how to reduce the risk in cloud.

Keywords: Cloud Security, Risk Handling, Security Framework, CIA.

1. INTRODUCTION

Cloud Computing has been seen as the next-generation information technology (IT) architecture for enterprises. On-demand self-service, everywhere network access, location independent resource pooling, rapid resource flexibility, usage-based pricing and transmission of risk are the major advances of cloud computing. High quality computing services with reduced cost and improved performance have made cloud computing a popular paradigm [7]. It’s a claim that Cloud computing providers are responding to customer demands for guarantees on the security of the services they provide, even they know their customers place high priority on the security of the data they own. The security of the cloud services they offer is often significantly better than that of the customer’s own IT systems.

The security issues with cloud computing do not vary enormously from those users facing in any other computing environment. The classic problem can be epitomized by the acronym CIA which representing, Confidentiality of data, Integrity of data, and Availability of data [2][11]. Once data is out in the cloud, only authenticated and authorized users should be able to see the company data, ensuring confidentiality. For every piece of information that is considered confidential or sensitive in some way, it is necessary to know where it is stored, who has been looking at it, under what conditions they have been accessing it, and can be provided with an audit trail, so that if something unplanned happens, the owner can track its cause. Security is one key requirement to enable privacy. This principle specifies that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, use, modification, destruction, or disclosure of data [8]. Cloud computing changes the way we think about computing by changing the relationship of location with resources. Because cloud computing represents a new computing model, there is much uncertainty about how to achieve security at all levels (e.g., network, host, application, and data levels).

2. CLOUD COMPUTING SECURITY FUNDAMENTALS

Network security has become an integral part of any network service. With the rapidly increasing number of transactions on the Internet, security has become an essential part of everyday life. For dynamic and demanding environment like cloud computing, network security becomes much more difficult to control. We know the cloud computing is used to reduce operational and support costs but this reduction is not only in terms of computing resources, but also in terms of helping its users to focus on the business instead of the information technology enabling this business. Cloud computing has evolved from many different technologies such as virtualization, autonomic-computing, grid-computing, and many other technologies [1]. With every new technology, new challenges arise. The most important challenge is to provide adequate security to cloud for performing well. Control of security in cloud computing is not fundamentally different from security control in any IT environment. However, because of the cloud service models employed, their operational models, and the technologies used to enable cloud services, cloud computing may introduce different risks to an organization than traditional IT solutions.

In general, computer security identifies three main objectives:

Confidentiality

Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in a cloud system is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference.

Integrity

Guarding against destruction of information and improper modification from unauthorized personnel and also assuring that data has not been altered while transport over the network.

Availability

Availability ensures the reliable and timely access to cloud data. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. A denial-of-service attack is an example of a threat against availability.

However, with the emergence of new technologies and threats, two more objectives can be added to the previous list:

Authentication

Assuring the identity of the entity involved in the communication process.

Auditing

To control operational assurance, organizations use two basic methods, system audits and monitoring. These methods can be employed by the cloud customer, the cloud service provider or both, depending on asset architecture and deployment. Firstly, a system audit is a one-time or recurrent event to evaluate security. Secondly, monitoring refers to progressive activity that examines either the system or the users, such as attack detection.

3. ABOUT CLOUD SECURITY

The Internet was designed primarily to be resilient, but not to be secure. Any distributed application has much greater attack surface than an application that is closely held on a Local Area Network. Cloud computing has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from pooled, virtualized, and outsourced resources. Different types of cloud computing service models provide different levels of security services [7]. We will get the least amount of built in security with an Infrastructure as a Service provider, and the most with a Software as a Service provider. So, risks in any cloud deployment are dependent upon the particular cloud service model chosen and the type of cloud on which we deploy our applications.

In order to evaluate the risks, we need to perform the following analysis [9]:

i. To determine the resources (data, services, or applications), we can plan to move to the cloud.

ii. Determine the sensitivity of the resource to risk.

Risks which need to be evaluated are loss of privacy, unauthorized access by others, loss of data, and interruptions in availability.

iii. Determine the risk depend on particular cloud type for a resource.

Cloud types include public, private (both external and internal), hybrid, and community types. With each type, we need to consider where data and functionality will be maintained.

iv. It is important to know the particular cloud service model that we will be in use.

Different models such as IaaS, SaaS, and PaaS require their customers to be responsible for security at different levels of the service stack.

v. If we will select a particular cloud service provider, we need to evaluate its system to understand the process of data transferring and data location, means where it is stored and how to move data both in and out of the cloud. We require to build a flowchart that shows the overall mechanism of the system for using.

Many cloud providers offer a snapshot feature that can create a copy of the client's entire environment. This includes not only machine images, but applications and data, network interfaces, firewalls, and switch access. If we feel that there is a problem in system, we can replace that image with a known good version. Many vendors maintain a security page where they list their various resources, certifications, and Credentials.

4. SECURITY FRAMEWORK IN CLOUD

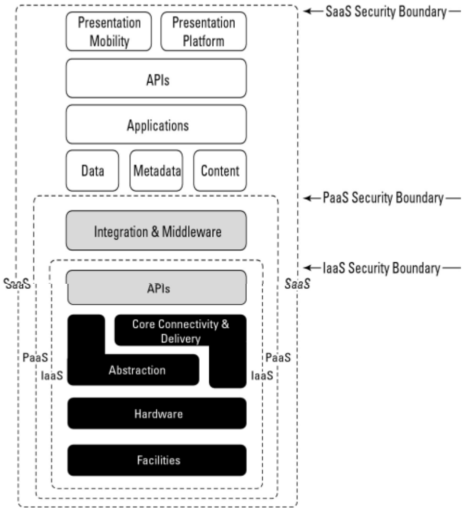

Figure 1. Cloud security framework

Cloud computing security must be done on two levels, provider level and user level. Responsibility of Cloud computing service provider is to secure the server from all the external threats, it may come across. The cloud computing service provider has provided a good security layer for the customer as well as the user. The user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

The Cloud Reference Model architecture describes each different type of cloud service delivery model and its security boundary at which the cloud service provider's responsibilities end and the customer's responsibilities begin [9] [11]. Any security mechanism below the security boundary must be built into the system, and any security mechanism above must be maintained by the customer. As we move up the stack, it becomes more important to make sure that the type and level of security is part of our Service Level Agreement.

Each service model inherits the capabilities of the model within it, as well as all the inherent security concerns and risk factors. IaaS supplies the infrastructure, PaaS adds application development frameworks, transactions, and control structures and SaaS is an operating environment with applications, management, and the user interface. As we move in the stack, IaaS has the least levels of integrated functionality and the lowest levels of integrated security, and SaaS has the most.

In the SaaS model, the vendor provides security as part of the Service Level Agreement, with the compliance, governance, and liability levels stipulated under the contract for the entire stack. For the PaaS model, the security boundary may be defined for the vendor to include the software framework and middleware layer. In the PaaS model, the customer would be responsible for the security of the application and user interface at the top of the stack. The model with the least built-in security is IaaS, where everything that involves software of any kind is the customer's problem.

4.1 Levels of cloud security

Software as a service (SaaS)model

- May be customized by the user.
- Places most of the responsibility for security management on the cloud provider.
- Provides ways to control access to the Web portal, such as the management of user identities, application level modification, and the ability to constrain access to specific IP address ranges or geographies.

Platform as a service (PaaS) model

- Refers to application development platforms where the development tool itself is hosted in the cloud and accessed and deployed through the Internet.
- Allows clients to assume more responsibility for managing the configuration and security for middleware, database software, and application runtime environments.

Infrastructure as a service (IaaS) model

- Provides fully scalable computing resources such as CPU, and storage infrastructure.
- Transfers responsibility for security is from the cloud provider to the client.
- Provides full access to the operating system that maintains virtual images, networking, and storage.

5. SECURITY ISSUE IN CLOUD COMPUTING

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs differentoperations and offers different products for businesses and individuals around the world. There are numerous security issues 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 [6]. Security issues for many of these systems and technologies are applicable to cloud computing [4] [5]. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data location is a crucial factor and Location transparency is a prominent flexibilities for cloud computing. Without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Hence cloud user’s personal data security iscrucial concern in a cloud computing environment. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The following are the various security and privacy concerns in a cloud computing environment.

5.1 Different security issues

Data location: depending on contracts, some clients do not know in which country or where data is stored.

Restoration: every cloud provider should have a disaster restoration protocol to protect user data.

Inquisitive support: if a client suspects faulty actions by the provider, it may have few legal ways to continue an enquiry.

Data isolation: encrypted information from multiple companies may be saved on the same hard disk, so a mechanism to isolate data should be deployed by the provider.

Privileged user access: Transferring client’s information over the Internet presents certain degree of risk, because of data ownership enterprises spend time to know their providers and their regulations as much as possible, basically assigning some trivial applications first.

Regulatory compliance: clients are responsible for the security of their solution, as they can select between providers that allow audits by third party organizations that test levels of security which providers do not.

5.2 Privacy in cloud computing

Today most visible cloud applications are consumer services such as e-mail, social networks, and virtual worlds. The companies maintaining these services collect terabytes of data, sensitive informationwhich is then located in data centers in countries around the world.

Privacy is a fundamental human right. There are various forms of privacy, including “the right to be left alone” and “control of information about our-selves” [10]. Taxonomy of privacy has been produced which focuses on the harms that arise from privacy violations and this can provide a helpful basis on which to develop a risk/benefit analysis.

- Cloud users need a guarantee that their private information, saved, processed and communicated in the cloud, will not be used by the cloud provider in unenforceable ways.
- Cloud providers should create privacy rules that are appropriate for the particular cloud service as they provide and employ business model. They should disclose such policies and should give reasonable advance notification to their customers of any changes in those policies. When

appropriate, they should provide customers with the opportunity to opt out of such changes.

5.3 Risk for cloud privacy

The different types of risk factors which influenece the cloud privacy are following.

Cloud service user: The user will not be forced to give personal information against their will, or in a way in which they feel uncomfortable.

The organization using the cloud service: The non compliance with enterprise policies and legislation and loss of reputation.

Implementers of cloud platforms: The exposure of sensitive information stored on the platforms, legal liability, loss of reputation and credibility and lack of user trust.

Providers of applications on top of cloud platforms: The legal non-compliance, loss of reputation, abuse of personal information stored on the cloud.

The different Vendor issues are -

i. Organizations may be unaware they are even using cloud-based products.

ii. Due diligence is still required as in any vendor relationship.

iii. Data security is the responsibility of the customer.

iv. Service level agreements need to account for access, correction and privacy rights.

To Manage Privacy in the Cloud, policies and procedures must explicitly address cloud privacy risks. Information governance must be put in place that provides tools and procedures for classifying information and assessing risk. It establishes policies for cloud-based processing based upon risk and value of assets and it evaluate third party security and privacy capabilities before sharing confidential or sensitive information. Privacy can be managed thorough review and audit of providers, independent third party verification.

6. HOW TO HANDLE CLOUD SECURITY CHALLENGES

First, we have to secure any device connected to the open Internet from unauthorized access from a common risk and is faced equally by any company and customers. Secondly, we have to secure any data in transit over the network and finally we have the important task of ensuring dependable high-quality networking to the cloud [4].

6.1 Prevent physical access to server and application

“Self-service” is one of the most important characteristics of cloud computing. It offers access to computing power via the Internet. In traditional data centers, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data.

6.2 Securing data within the cloud

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system.

(1). Whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. At the same time, many cloud computing service consumer and provider accesses and modify data. Thus, there is a need of some data integrity method in cloud computing.

(2). Data stealing is a one of serious issue in a cloud computing environment.

(3). Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accessible to users.

(4). Data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. The key challenge for the cloud is keeping “data in transit” secures. It is important that one user is unable to view the Internet traffic of another user. This is the networking risk in a multi-tenant environment. With open networking, it is possible for users of the cloud to create secure encrypted VPN connections among their cluster in the cloud and corporate infrastructure. This solution is used by some large clients and allows end-to- end encryption of data. 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.

6.3 Virtual machine security

Virtualization is one of the main components of a cloud. 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. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

6.4 Maintaining network security

In a traditional enterprise environment, the infrastructure and the network used can be well defined in terms of usage. Traffic is predictable and this allows a relatively static network configuration that allows the sort of traffic expected and blocks everything else. Likewise, in such a single tenant environment, the opportunity to be affected by malicious attacks by other tenants (or against them) is of course zero. Everything changes when we move to a multi-tenant public cloud environment; we now have diverse, unforeseeable networking traffic that can change significantly in nature from hour to hour. Consequently, it is important to manage a high-quality networking environment for a number of very different uses. The first thing to acknowledge is that such a general-purpose network will never perform as predictably and in such an optimized way as a specialized dedicated network.

7. EXISTING ALGORITHMS FOR CLOUD SECURITY

Many organizations and people store their important data on cloud and it is also accessed by many persons, so it is very important to secure the data from intruders. To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data or plaintext message into cipher text by using "the key" and only the user has the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption [12].

We are presenting some popular security algorithms used for data security in cloud computing.

RSA algorithm- The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm which involves both public and private key. The public key can be known to everyone and is used for encrypting messages which can only be decrypted using the private key. So, in our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

DES algorithm- Data Encryption Standard (DES) is very commonly used symmetric key algorithm. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It divides the whole message into blocks of 64 bits which encrypts and produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption. The key length of this algorithm is 56 bits; however, a 64 bits key is the actual input. The drawback of DES is that the key used in DES is very small and its security can be broken easily and DES works fast on hardware only and woks slowly on software.

AES algorithm - Advanced Encryption Standard (AES) is the new symmetric key encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. Each of these ciphers has 128-bits of block with key sizes of 128, 192 and 256 bits respectively. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

8. STEPS TO ENSURE OUR CLOUD IS SECURED

- Use certificates and encrypt all sensitive information.
- Deploy strong authentication for all remote users and do not use vendor supplied defaults passwords and other security parameters.
- Ensure isolation by using private IP address spaces and (virtual) networks.
- Provide location independence through virtual machines and networks that can be physically allocated in any data center.
- Use anti-virus software on every device.
- Install and maintain a firewall configuration and use firewall technology at every point and block unused services, ports and protocols [3].
- Teach all users "safe Internet skills."

9. CONCLUSIONS

With the rapid increase in the adoption of cloud computing by many organizations, security issues arise. One of the biggest security worries with the cloud computing model is the sharing of resources and data security. In this paper, we have discussed in details the different security and privacy issues and research challenges in cloud computing. The paper also included suggestions to mitigate these issues. The paper provided general cloud security recommendations as well.

REFERENCES

[1] Buyya R., Broberg J., Goscinski A. (2010). *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, Vol. 87.

[2] Mohammed M. (2014). Alani: securing the cloud: threats, attacks and mitigation techniques, *Journal of Advanced Computer Science and Technology*, Vol. 3, No. 2, pp. 202-213.

[3] Buecker A., Lodewijkx K., Moss H., Skapinetz K., Waidne M. (2009). Cloud security guidance, *IBM Red Paper 2009*, p. 12.

[4] Padhy R.P., Patra M.R., Satapathy S.C. (2011). Cloud computing: security issues and research challenges, *IRACST- International Journal of Computer Science and Information Technology & Security(IJCSITS)*, Vol. 11.

[5] Tiwari P.K., Mishra B. Cloud computing security issues, challenges and solution, *International Journal of Emerging Technology and Advanced Engineering*. Vol. 2.

[6] Prince Jain: security issues and their solution in cloud computing, *International Journal of Computing & Business Research*.

[7] Anantwar R.G., Chatur P.N., Anantwar S.G. (2012). Cloud computing and security model: a survey, *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 1.

[8] Tim M., Subra K., Shahed L. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance, *O' Reilly Media*, USA.

[9] Barrie S. (2011). *Cloud Computing Bible*, Wiley Publishing Inc.

[10] Pearson S., Azzedine B. (2010). Privacy, security and trust issues arising from cloud computing, *2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom)*, pp. 693-702.

[11] Hamouda S.K., Glauert J. *Security, Privacy and Trust Management Issues for Cloud Computing*, Taylor & Francis Group.

[12] Shakeeba S.K., Tuteja R.R. (year). Security in cloud computin using cryptographic algorithms, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3.