IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Cloud Computing and its Techniques to Improve Data Security and Storage Utilization

Eng. Jasim M. A. Albazzaz[1], Anwar J. Alzaid[2]

The Public Authority for Applied Education and Training, Higher Institute for Communication and Navigation

Computer Department, Kuwait[1, 2]

Abstract: Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing IT services over the Internet that enable convenient, on demand and pay for use access to a pool of shared resources. It is a new technology that can support a broad-spectrum of applications without physically acquiring them. Like other IT services, there are bound of fears and concerns about cloud technology. In this paper, we identify the major security issues and security threats. This paper provides techniques to improve data security by discussing the cryptography and authentication concepts. Additionally deduplication technique is discussed to improve storage utilization in the cloud environment. Finally, we provide some cloud security recommendations.

Keywords: Cloud Computing, SaaS, PaaS, IaaS, Cloud drivers, Security issues, Security threats, Cryptography, Authentication, Deduplication.

I. INTRODUCTION

Cloud computing is the 6th phase of computing paradigms. Figure (1) shows the 6 phases from mainframe using dummy terminals, Personal Computer, network computing (client-server computing), Internet computing, to grid computing through distributed systems and cloud computing. The cloud itself is a set of hardware, networks, storage, services, and interfaces that enable the delivery of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand. [1]

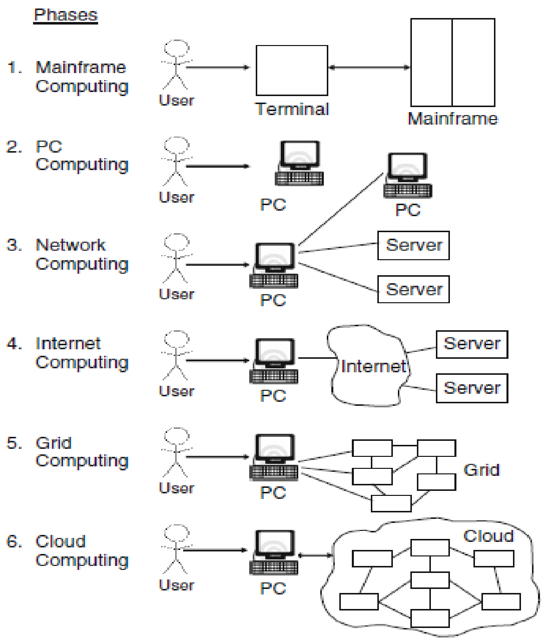

Figure 1 Computing paradigms

The world of the cloud has lots of participants:

- The **end user** doesn't really have to know anything about the underlying technology. In small businesses, for example, the cloud provider becomes the de facto data center. In larger organizations, the IT organization oversees the inner workings of both internal resources and external cloud resources.
- **Business management** needs to take responsibility for overall governance of data or services living in a cloud. Cloud service providers must provide a predictable and guaranteed service level and security to all their constituents.
- The **cloud service provider** is responsible for IT assets and maintenance.

As with many other technical choices, security is a two-sided coin in the world of cloud computing—there are pros and there are cons. So it is necessary to examine security in the cloud and consider about what's good, and where you need to take extra care.

In order to be successful, vendors will have to take data like this into consideration as they offer up their clouds.[2] Many customers must take a leap of faith to trust that the cloud service is safe.
Turning over critical data or application infrastructure to a cloud-based service provider requires making sure that the information can't be accidentally accessed by another company.

II. WHAT IS CLOUD COMPUTING?

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.51122

configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3].
By comparing Cloud Providers with Traditional IT Service Providers; Traditional IT service providers operate the hardware, software, networks, and storage for its clients. While the customer pays the licensing fees for the software, the IT service provider manages the overall environment. The service provider operates the infrastructure in its own facilities. With the traditional IT service provider, the customer signs a long-term contract that specifies mutually agreed-upon service levels. These IT providers typically customize an environment to meet the needs of one customer. [1]

In the cloud model, the service provider might still operate the infrastructure in its own facilities (except in the case of a private cloud). However, the infrastructure might be virtualized across the globe, meaning that you may not know where your computing resources, applications, or even data actually reside. Additionally, these service providers are designing their infrastructure for scale, meaning that there isn't necessarily a lot of customization going on.

Essential characteristics of Cloud Computing

❖ Broad network access.
❖ Rapid elasticity.
❖ Measured service.
❖ On-demand self-service.
❖ Resource pooling.

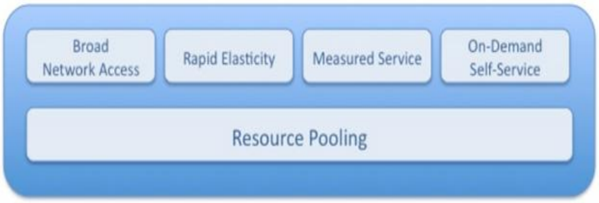

Figure 2. Essential characteristics

Cloud Service Models

❖ Software As a Service (SaaS)
• Use provider's applications over a network. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management. The cloud provider hosts a single application which offers complete application functionality. In brief, with SaaS you no longer have to purchase, install, update and maintain the software.

❖ Platform As a Service (PaaS)
• Deploy customer-created applications to a cloud. Users create and run their own applications while relying on the cloud provider for software development tools. In brief, with PaaS you can deploy and migrate applications to the cloud without complexity.

❖ Infrastructure As a Service (IaaS)
• Rather than purchasing servers, software, data center and network equipment, Users rent computing power – either actual hardware or virtualized machines – to deploy and run their own operating systems and software applications. In brief, with IaaS users running more quickly while cutting hardware costs.

Cloud Deployment Models

❖ Public Cloud.
❖ Private Cloud.
❖ Community Cloud.
❖ Hybrid Cloud.

III. IMPACTS AND BENEFITS OF CLOUD COMPUTING

The Cloud Computing will continue to expand because it offers many advantages. There are many impacts that must be factored:

❖ **Reduction of cost** – Cloud system provided low cost and free technology. It reduced the implementation and maintenance costs and could help with growing resources requirements.
❖ **Increased mobility for a global workforce** – Cloud system is free from the location. From any where you can login to the system and access your applications and data.

❖ **Elasticity of service** – The amount of stored data is growing at an exponential rate; the best part is that there is no limitation of space.

❖ **Greening the environment** – Cloud surely reduced the carbon footprint and not requiring large data centers that consumes a lot of power.

❖ **Availability** – Increased availability of high performance services and applications. 24 hours/7 days is the availability that is needed without failure.

Drivers of Cloud Computing

Cloud Computing is becoming a popular technology for many organizations in the world of Information Technology (IT). The major cloud services providers are Microsoft, Amazon, Google, Oracle, IBM, VMware and Citrix. Figure (3) shows the major cloud services providers.

❖ Microsoft
• It provides collaboration services, communication tools, mobile, desktop, and web-based applications and it has the features of data storage capabilities.

❖ Amazon
• It provides the cloud services in categories of Compute, Software, Database, Storage, Deployment & Management, Application services and Workforce.

DOI 10.17148/IJARCCE.2016.51122

❖ Google

• It supports application programming interfaces for the data store, image manipulation, Google accounts, and e-mail services.

Figure 3. Major cloud services providers

IV. THIRD-PARTY CONTROL

Cloud computing solutions provide users with many capabilities to store and process their data in third-party data centres. Third-party web services components combine more than one source element into a single integrated unit. It inherits security issues related to data and network security. Also users have to depend on both the security of web-hosted development tools and third-party services. Cloud computing providers must adopt the most sophisticated and up-to-date tools and procedures to provide better security.

V. CLOUD CONCERNS AND SECURITY ISSUES

There are many security concerns associated with cloud computing. Cloud Computing is tackled by several issues that a cloud environment need to resolve. The cloud security is a big concern on the cloud based technologies and computing to make them admirable among the corporate environment.

This part is very complex and need to be understood very well by cloud computing users.

These main issues include Security, Privacy, Confidentially, Integrity, Availability, Performance, Quality of service, Cost and Reliability.

❖ Security: The security is a major concern for any technology, but it becomes a major challenge for cloud users to rely on their providers for proper security. It includes both the security issues faced by cloud providers and the security issues faced by their customers.

❖ Privacy: Clients trust that a cloud provider will protect the privacy of their data. Privacy is exactly the ultimately desired for cloud services and applications. Privacy refers to the right to self-determination, that is, the right of users to be aware of stored information about them, control how that information is communicated and prevent its abuse. Thus, every user has the right to control his own data.

❖ Confidentially: Data confidentiality means only authorized users should be able to access the data while others should not. To ensure confidentiality, it must include file permissions and access control list.

❖ Integrity: Data integrity demands ensuring the accuracy and completeness of data. It means to protect the data from modification by unauthorized users.

❖ Availability: It means that services should be available all the time (24 hours a day, 7 days a week, and 365 days a year) without failure and avoiding cloud provider outages.

❖ Performance: Cloud providers should provide cloud services ensuring that the performance remains the same all the time. Many users understand that for cloud services to be effective they must measure and monitor performance. In fact, performance monitoring will become increasingly important as companies rely more on third-party services.

❖ Quality of service: Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance avoiding the delay in the processing of cloud services and loss of data.

❖ Cost: All IT organizations monitor costs, but few monitor them in terms of performance. The requirement to optimize the return on investments for both hardware and software. Unlike traditional licensing models, cloud propositions are based on rental arrangements. And because a cloud requires a self-service capability, it must be designed to manage billing services.

❖ Reliability: Failure of a cloud provider which owns data centers can a serious concern for cloud users who trusted their data with their provider. It means the probability of failure-free software operation for a specified period of time in a specified environment. So reliability has been equated with preventing failure. Cloud services are complex and have dependencies, so they become more reliable when they are designed to quickly recover from unavoidable failures; particularly those are out of an organization's control.

Cloud security is an important issue for IT organizations. A survey was conducted by the IDC (International Data Corporation) regarding the challenges and issues which mainly affect the performance of Cloud Computing. And the result shows security at the top of the list with 74.6% as the biggest cloud challenge. [14]

VI. CLOUD COMPUTING SECURITY THREATS

The environment of cloud computing creates some security threats. Cloud computing is a target for many attacks that result to system failure. Cloud threats result from internal attackers or external attackers. Internal attackers can be customers, cloud provider employees, or other third party provider organization supporting the operation of a cloud service. Internal attackers may have authorized access and use privileges to gain further access in executing attacks. While external attackers are not customers, not cloud provider employees, or other third

party provider organization supporting the operation of a cloud service. External attackers have no authorized access to cloud services and customer data. They exploit technical operational process and vulnerabilities to attack.
Some threats to cloud computing security include Data Breaches, Data Loss, Service Traffic Hijacking, Insecure Interfaces and APIs and Malicious Insiders.

❖ Data Breaches: A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and publish data to an unsecured or illegal location. A way of eliminating data breaches is to encrypt all of the client data.

❖ Data Loss: Data loss is any process or event that results in data being corrupted, deleted or became unreadable by the data owner or requesting application. Data loss is also known as data leakage. Data loss can occur due to many reasons, including Data corruption, Data being accidentally deleted or overwritten by a user or an attacker, Data storage device physically damaged and Virus infection. Data loss is usually prevented by implementing data backup solutions.

❖ Cloud Account Hijacking: Cloud account hijacking is a process in which a user or organization’s cloud account is stolen or hijacked by an attacker. The mitigation technique for this threat can be done by keeping all systems and protection software up-to-date. And prohibiting account sharing between users and services.

❖ Insecure Interfaces and APIs: Cloud APIs are Application Programming Interfaces used to build applications in the cloud computing Environment. Customers interact with cloud services through interfaces or APIs. Providers must ensure that security is integrated into their service models, while users must be aware of security risks in the use, implementation, management, and monitoring of such services.

❖ Malicious Insiders: A malicious insider is an employee of the Cloud Service Provider who abuses his position for other nefarious purposes. Encrypting the client data will not completely mitigate this threat. If the encryption keys are not stored with the client and are only available at data-usage time. Thus, it is advisable that all client data is encrypted and the keys should be kept only with the client.

VII. TECHNIQUES TO IMPROVE DATA SECURITY

❖ Cryptography: Cryptography is a technique of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is used to prevent unauthorized access to information, protect data in the cloud and enhanced security. With Cryptography techniques; users encrypt and decrypt data by using cryptography algorithms using secret key or password. Encryption is the process of converting plain text into cipher text. Decryption is the converting of cipher text back to plain text form. By using private key cryptography algorithm (Symmetric-key algorithm); the encryption and decryption both share the same key as shown in Figure (4). And using Public key cryptography algorithm (Asymmetric-key algorithm), a key is used for encryption, while another secret key is used for decryption as shown in Figure (5).

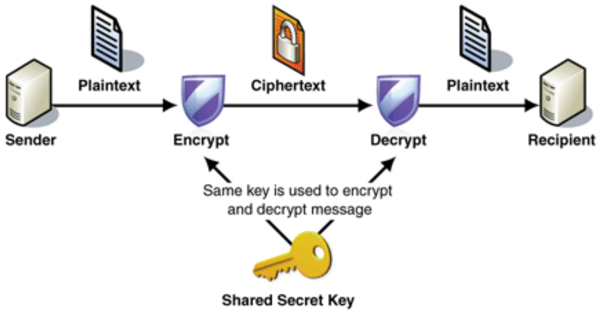

Figure 4. Symmetric key algorithm

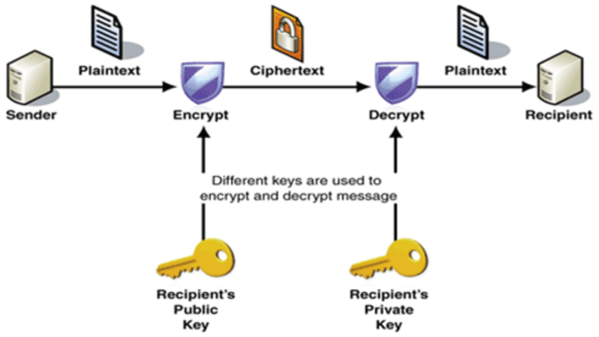

Figure 5. Asymmetric key algorithm

❖ Authentication: Authentication is a process that ensures and confirms a user's identity. The identifying of an individual usually based on a username and password. Authentication ensures that the individual is who he claims to be.

3D Security Technique is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data. It is a multi-level authentication system. The system makes the confidential data secure using highly secure graphical passwords.

VIII. TECHNIQUES TO IMPROVE STORAGE UTILIZATION

❖ Deduplication: It is a technique of keeping only one unique instance of data copy by detecting identical data copies and eliminating redundant data, so that could improve storage utilization and system performance. Only one unique data is retained on storage media and redundant data is replaced with a pointer to the unique data copy. Data deduplication is a great technique for cloud providers because it enables to save money on storage cost. The major benefits of data deduplication include:

DOI 10.17148/IJARCCE.2016.51122

- Reduced hardware costs.
- Reduced backup costs.
- Reduced costs for disaster recovery.
- Increased storage efficiency.
- Increased network efficiency.

IX. CLOUD SECURITY RECOMMENDATIONS

❖ Understand the internal control environment and analyze the security model of cloud provider interfaces.
❖ Install and maintain a firewall configuration. A firewall should be placed at each external network interface and between each security zone within the cloud.
❖ Ensure strong authentication and access controls are implemented and do not use vendor defaults for passwords and other security parameters.
❖ Ensure that no unnecessary functions or processes are active.
❖ Protect encryption keys from disclosure.
❖ Revoke access for terminated users.
❖ Prohibit the sharing of account between user and services.

X. CONCLUSION

Cloud computing is the best solution for IT organizations. We have looked at the concept of cloud computing and its benefits with discussing the major security issues and threats. In short, we discussed techniques to improve data security and storage utilization on cloud environment. In this paper, we provided important recommendations to use the cloud feeling secure and safe.

REFERENCES

[1] Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Dr. Fern Halper, "Cloud computing for dummies", 2010.
[2] Anthony T. Velte, Toby J. Velte, Ph.D. Robert Elsenpeter, "Cloud computing A practical Approach", 2010, ISBN: 978-0-07-162695-8.
[3] P. Mell and T. Grance, “The NIST Definition of Cloud Computing”, September 2011.
[4] Cloud computing basics, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 2, Issue 5, July 2012.
[5] Adoption of Cloud computing In Education and Learning, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 2, Issue 10, October 2013.
[6] Cloud computing for Academic Environment, International Journal of Information and Communication Technology Research, Vol. 2, No. 2, February 2012.
[7] Cloud computing Technology in Education system, International Journal of Advanced Technology & Engineering Research (IJATER, Vol. 2, Issue. 2, March 2012.
[8] 3D Security Cloud Computing using Graphical Password, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 2, Issue 1, January 2013.
[9] Cloud Computing Security with VPN, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 4, Issue 8, August 2015.
[10] Enhanced Security as a Service to Protect Data in Public Cloud Storage, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 4, April 2016.
[11] Secured Data Transmission in Cloud Using Trapdoor Encryption, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 4, April 2016.
[12] An analysis of security issues for cloud computing, Journal of Advanced of Internet Services and Applications, 2013, 4:5.
[13] A Survey on Cloud Computing Security, Challenges and Threats, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 3, Mar 2011.
[14] Cloud Computing Concepts, Securities issues, and its techniques, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 6, June 2014.
[15] Enhancing Cloud Data Security Using Elliptical Curve Cryptography, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 3, March 2016.
[16] Deduplication Techniques in Storage System, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 4, Issue 11, November 2015.
[17] Data Partitioning Techniques to Improve Cloud Data Storage Security, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 3, March 2016.
[18] Securing the Cloud: Threats, Attacks and Mitigation Techniques, Journal of Advanced Computer Science and Technology (JACST), 3, Feb 2014.

BIOGRAPHIES

Eng. Jasim M. A. Albazzaz: Computer Engineer from Kuwait University, Experience 3 years in the Information center in the Kuwait University, 16 years in the public Authority for Applied Education & Training in The Higher Institute for Telecommunication and Navigation-Computer Department.

Eng. Anwar. J. Alzaid: Computer Engineer from Kuwait University, 20 years in the public Authority for Applied Education & Training in The Higher Institute for Telecommunication and Navigation- Computer Department.

DOI 10.17148/IJARCCE.2016.51122