Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.796 – 801

RESEARCH ARTICLE

EMPLOYING SECURITY TECHNIQUES IN THE CURRENT WORLD OF CLOUD COMPUTING ENVIRONMENT: A STUDY

Mrs. Snehal A.Narale[1], Dr. P.K.Butey[2]

[1]Deptt of Computer Science, Dharampeth M.P.Deo Memorial Science College, Nagpur, India

[2]Asso.Prof, Head, Dept of Computer Science Kamla Nehru College, Nagpur, India

[1] Snehal.narale2012@gmail.com; [2] buteypradeep@yahoo.co.in

Abstract: ***Cloud computing is a fastest mounting technology which is based on internet. It assists the users to operate services by making use of large poll of resources without installation of any software. Implementation of this technology in different areas is increasing hastily because of its many advantages like cost reduction, reliability, elasticity, flexibility and many more. In spite of the popularity of cloud computing, it has to appear for many complexities such as security that is one of the major inhibitors in the growth of cloud computing. Cloud Computing transfer users application software and databases to the large data centers, data and services offered by cloud providers may not be manage reliably. Security is to save users data from hazard and openness. For cloud computing environment the top of the list of security is Data confidentiality which is concern to this technology. Encryption is one of them and widely used method to ensure the data confidentiality in cloud environment. In this research paper we discuss security techniques that will be used for data confidentiality .In addition for providing the enhanced security in cloud computing technology, lots of authentication and authorization techniques are being used. In our research paper we are make a glance on some of them.***

Keywords— Cloud computing, Security techniques, Cloud deployment model, Service model, IaaS, PaaS, SaaS

I. INTRODUCTION

Now a day cloud computing working as a utility computing which is nothing but the transformation of computing to services which are customaries and delivered like traditional utilities like water, gas and electricity. Cloud computing provides different services through different service providers. Because of the outstanding features of cloud computing it is frequently used for fastest development in the field of IT . Cloud computing is defined as the delivery of application as services over internet using the software and hardware facility of the service providers which can be either called as Software as a Service (SaaS), Infrastructure as a service (IaaS) or Platform as a Service (PAS) .Cloud computing offer Business applications to the customer. These services are accessed over a network with the help of cloud service provider for that the customers are being paid. Cloud computing technology delivers all the IT functionalities and dramatically reduces the upfront costs of computing which may give the cutting edge to the companies [1]. As a part of Total Quality Management (TQM), redundancy and reliability; providers

especially Amazon, Google, Sales force, International Business Management (IBM)& Microsoft have launched data centers for cloud computing around the globe.

Cloud computing support the three main technologies such as virtualization which hides the physical characteristics of computing platform, multitenancy allows instances of application software for multiple clients and web services which provides a software system designed to support interoperable machine to machine interaction over a network which is being rapidly emerging. A web service provides the stakeholders in cloud computing which is totally different from the traditional computing and involves consumers, providers, enablers and regulators. According to International Data Corporation (IDC) Security is ranked first as the greatest challenge or issue of cloud computing[2]. Experience shows that attacks may never be completely prevented or detected accurately and on time.

For sustaining security in the cloud we have to consider some of the issues addressed and its solution. There are some standards and agreements that should allow clouds to interoperate and communicate with each other no matter which vendor provides cloud services. For storing secure data on cloud, cloud computing used an encryption technique .Concern among big cooperate companies about handling their operations through another firm and bankruptcy of cloud providers especially in a reducing economy. Security also a serious concern among IT executives followed by performance and reliability [2]. Lack of standards especially International Organizations for Standards are still missing in cloud services which may reduce its acceptability. The launch of Euro Cloud is a typical example were standards are implemented and being checked for the safeguarding the interest of clients throughout European Union (EU). In our research paper we were discussing security techniques that will help to try to reduce the problem of data security.

II. CLOUD COMPUTING

Cloud computing is the use of computing resources (hardware and software) that are shared as services over the internet. It is called "Cloud" computing because a cloud shaped symbol is often used to represent bulky networks especially the internet. Cloud Computing is one of the form of distributed computing which can be virtualized and managed pool of resources like computing power, storage, platform and network over the internet. According to the NIST definition, cloud computing can be defined as a model for enabling useful, on-demand network access to a shared pool of configurable computing possessions [1]. According to Gartner [2] cloud computing can be defined as a technique of computing that delivered IT facilities 'as a service' to end users through internet. Foreign large companies such as Google, IBM, Amazon, Microsoft and Yahoo are leading the way in cloud computing. Many other companies like MySpace, Facebook, Salesforce and YouTube, also make an achievement in cloud computing [3].

1. Advantages Of Cloud Computing

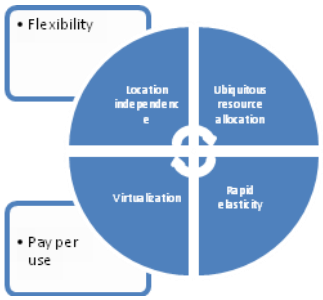

Fig : Advantages of Cloud Computing

Table I .Challenges In Cloud Computing

Cloud computing faces five major challenges that need to be addressed:

Challenges
Security
Interoperability
Availability & Performance
Data migration

TABLE II. Cloud Service Model & Deployment Model(Iaas & Paas)

Service model	Deployment model
IaaS: ➢ It offers virtualized computing resources. ➢ It offers different resources on demand on behalf of users ➢ It is multitasker. ➢ Pay on a per use basis.	Public cloud ➢ Scalability. ➢ Elasticity ➢ Accountability ➢ Low-cost, pay-as-you-go model ➢ Greatest efficiency in case of shared resources
PaaS: ➢ It allows for higher-level programming. ➢ It will help to reduced complexity. ➢ Easy to maintain &enhance application. . ➢ Multiple users work on single site with location independence..	Private cloud ➢ Greater control ➢ More security ➢ High performance ➢ Customizable ➢ Deeper compliance

TABLE III. Cloud Service Model & Deployment Model(Saas , Hybrid,Community Cloud)

Service model	Deployment model
SaaS: ➢ Ease in administration. ➢ Automatic updates and patch management. ➢ Compatibility. ➢ Global accessibility.	Hybrid Cloud ➢ Cost effective ➢ Increased flexibility ➢ Better security and control ➢ More scalability of resources.
	Community Cloud ➢ Cost of setting up a communal cloud is cheaper as compare to private cloud ➢ Management of the community cloud is easy. ➢ Results in time

III. SECURITY ISSUES IN PUBLIC, PRIVATE AND HYBRID CLOUD

In a public cloud, security management day-to-day operations are transferred to the third party vendor, who is responsible for the public cloud service offering .Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (*i.e.*, the cloud is dedicated to a single organizational tenant)[3]. The security management and day-to-day operation of hosts are relegated to internal IT or to a third party with contractual SLAs. By virtue of this direct governance model, a customer of a private cloud should have a high degree of control and oversight of the physical and logical security aspects of the private cloud infrastructure.

A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud .Providing security in a private cloud and a public cloud is easier, comparing with a hybrid cloud since commonly a private cloud or a public cloud only has one service provider in the cloud[3]. Providing security in a hybrid cloud consisting of multiple service providers is much more difficult especially for key distribution and mutual authentication. Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While in the whole cloud, there are many different kinds of clouds and each of them has its own identity management system. Thus a user who wants to access services from different clouds needs to have multiple digital identities from different clouds, which will lead to inconvenience for users. Using federated identity management, each user will have his unique digital identity and with this identity, he/she can access different services from different clouds.

IV. SECURITY TECHNIQUES IN CLOUD COMPUTING

From the work done on security in cloud computing we conclude that encryption is the most widely used method to ensure the security of data in cloud. One of the best ways to ensure confidentiality of secret data in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage [3,4]. Encryption plays a big role in fulfilment as many policies need specific data components to be encrypted. To protect a user‘s secret data in the cloud, encryption is considered as influential tool that can be used efficiently. User can confidently utilize cloud services by knowing that their confidential data is protected by encryption.

Security goals of data include three points which are Confidentiality, Availability and Integrity. Confidentiality of data in the cloud can be achieved by cryptography. Data cryptography is the shuffling of the content of the data, such as text, image, audio, video to make the data meaningless, unreadable or invisible during transmission or storage is termed Encryption. The main role of encryption is to take care of data secure from attackers. The process of getting back the original data from encrypted data is Decryption, which refurbish the original data[4]. Both symmetric-key and asymmetric-key algorithms can be used to encrypt data in cloud storage.

1. Raid Technique:

The first goal of security of data on cloud is integrity While accessing information from cloud computing the issue is whether our uploaded information is secure or not . For preserving the deployed information on the cloud the Data integrity is used in the cloud system .In data integrity concept , the data should not be lost or modified by unauthorized users. The main aim of using Data integrity in cloud computing g is to provide cloud computing service such as SaaS, PaaS, and IaaS[5]. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

The RAID technique is try to used to reduce the security problems in cloud computing. This is a serious threat for critical data such as medical records, as cloud provider staff has physical access to the hosted data. We tackle the problem by encrypting and encoding the original data and later by distributing the fragments transparently across multiple providers. This way, none of the storage vendors is in an absolute possession of the client’s data. Moreover, the usage of enhanced erasure algorithms enables us to improve the storage efficiency and thus also to reduce the total costs of the solution.

Due to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers.

2. Encryption Technique

The Data confidentiality is another important goal of security of data in cloud system. It will help for users to store their private or confidential data in the cloud. In cloud computing there are some strategies are used for Authentication and access control to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness ,as users do not trust the cloud providers it is very difficult to remove the threat insider because it is very difficult to eliminate the threat[4,5]. To solve this problem in some extent we were proposed to use encryption technique to solve the management problem occurred in cloud computing while performing different operations Encryption is usually used to ensure the confidentiality of data.

One of the types of the encryption technique is Homomorphic encryption. It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results, while using this technique there is no need to decrypt the whole data. The implementation of this technique could well solve the confidentiality of data and data operations in the cloud. Cryptographic encryption is used in many countries including U.S. The commandment of cryptographic encryption is for securing data at rest at the cloud provider. Encryption techniques should also be used for data in transit.

3. Hybrid Technique

For more flexibility and enhanced security, a hybrid technique that combines multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed .RSA is useful for establishing secure communication connection through digital signature based authentication while 3DES is particularly useful for encryption of block data. Besides, several encryption algorithms for ensuring the security of user data in the cloud computing are discussed.

This technique proposed for data confidentiality and integrity in cloud system, which uses both key sharing and authentication techniques. The key sharing and authentication processes help to provide the connectivity between the user and the cloud service provider to make it more secure [6]. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

4. User Authentication

User authentication technology is used in cloud computing for security purpose. The first user authentication method used is Id/Password. It is very easy to use but have some complications at some level as there is need to renew the key to enhance the security. The second technology is PKI (public key infrastructure), while using this technology the authentication is given using public key cryptography [7]. It enables to authenticate the other party based on certificate without sharing secretes information. In cloud computing environment misuse of access authority to resources and leak of personal information which should be used to authenticate the user could affect faster and powerful. For effective user authentication in cloud computing environment there is a need to use such type of authentication technologies.

5. Data Concealment

To keep the data confidential the Data concealment could also be used. For database security [8] introduced a concealment concept. Data concealment approaches merge real data with the visual fake data to fix the real data's volume. Data concealment technique will help the authorized users to easily differentiate between the fake data and real data. Data concealment techniques increase on the whole volume of real data but provide enhanced security for the private data. As Data concealment technique enhanced the security of private data so it will help in cloud computing for private cloud, because in private cloud the data is restricted to particular organization it is not accessible to all the users[9]. The main purpose of data concealment is to make the real data protected and secure from nasty users and attackers. Watermarking method can serve as a key for the real data. Only the authorized users have key of watermarking, so the authentication of users is the key to ensure the true data to be accessible for right users.

6. Management of Identity of Data

Cloud computing provides a platform podium to use ample collection of services which are based on internet Connection. But moreover its advantages, as we know that the coin has two sides cloud computing has to face lots of challenges & amongst that one is security[10]. In cloud computing paradigm when third party is involved (private cloud) it increases the security threat. A possible solution to this problem is that the third party could use identity of data on unexpectational host means it make its own independent party identity and its management[11].

Cloud security infrastructure and the trust reputation management play a vital role to upgrade the cloud services. The Internet access security, server access security, program access security, and database security are the main security issues in the cloud.

As we study lots of security techniques in our research paper now we make a glance on some of the authentication techniques [12].

7. Authentication Technique

Authentication can be done in various ways:

7.1 **Authentication using Kerberos**: Kerberos is the authentication technique which is used to authenticate the clients to the server in Client-Server architecture. Cloud Computing can also be viewed as distributed Client-Server architecture, where Cloud Provider is the Server and Cloud User is the Client., which communicates by the inter mediator , named as Cloud Broker[13].

7.2 **Authentication using Public Key Infrastructure**: The component of PKI includes end entity which is used to denote the end user, devices or any other entity which can be identified second component is certification authority which is the issuer the certificate and third is registration authority support the administrative functions and last one is repository which denote any method for storing certificate.[14]

CONCLUSIONS

Even a fundamental step towards a wide acceptance towards interoperability is the necessity. Customers and cloud providers should map use cases where the lacks of standards turn the process critical. Even though there are various proposals related to interoperability and standards in the area of cloud computing, there is no widely acceptance on neither a common cloud definition nor standards. Moreover, the peculiarity of core and proprietary functionalities appear to be the key for the adoption of cloud standards. Not only customers will benefit from this distinction, but also cloud providers which would have the possibility to provide basic standards and provide proprietary solutions on the top of core functionalities/resources. The cloud provider can offer an optimized way (with a proprietary algorithm) to a better traffic management on virtual machine instances. However, some parameters have to be set. The manner of how to express these parameters must be standardized, and the relation between them should also be standardized. A separation of core and proprietary categories may require some heavy effort from both industry and academia. Moreover, PaaS and SaaS don't have related cloud computing standards yet.

REFERENCES

1. Squicciarini, et.al "Preventing information leakage from indexing in the cloud," in Proceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD '10), pp. 188–195, July 2010NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012.
2. Gartner, "What you need to know about cloud computing security and compliance", (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013.
3. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11,2011.
4. A. Soofi and M. I. K Fazal-e-Amin, "A Review on Data Security in Cloud Computing", International Journal of Computer Applications, vol. 94, no. 5, pp. 12-20,2014
5. Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 2010.
6. A comparison between traditional Public Key Infrastructures and Identity-Based Cryptography by Kenneth G. Paterson Geraint Price.
7. N. Kshetri, "Privacy and security issues in cloud computing: the role of institutions and institutional evolution," Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386, 2013.
8. R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.
9. M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.
10. S. Kardaş, S. Çelik, M. A. Bingöl, and A. Levi, "A new security and privacy framework for RFID in cloud computing," in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol , UK, 2013.
11. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation," in Proceedings of the World Congress on Information and Communication Technologies (WICT '11), pp. 217–222, IEEE, December 2011.
12. S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," inProceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom '10), pp. 693–702, IEEE, December 2010.
13. Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.
14. Farhana S. Munnee, Anirudh Jonnavitula "Kerberos using public key cryptography" by in GMU-ECE 646 Fall 2007.

