Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 2, February-2019, ISSN 2230-7540

Cloud Computing: A Study on Security Issues and Their Impact on Cloud Computing Environment

Nisha Rani*

Computer Science

Abstract – Cloud computing enables users to use a Web browser only to receive computing services over the Internet. Users just have to pay for the services they are actually using. The present study shows that there is a large gap in the existing system's security issue. Confidentiality, authentication, access control, and integrity are the main security ideology and one of the most important requirements for any software. This paper investigates existing cloud computing solution for the SaaS model, and explores the various security flaws. The work concludes here with the comparative study of the various existing solutions and addresses the common problems and excuses.

Keywords: Cloud computing, Security Issues, Cloud Computing Impact

----------X----------

INTRODUCTION

Cloud is a feature of dispersed computing advancement and a general variety of Service-Oriented Architecture (SOA) and virtualisation. (1) Cloud computing is a model for drawing up advantageous, on-demand courses of action to access an ordinary pool of configurable computing assets which can be quickly furnished and discharged with insignificant communication between associations or specialists (2).Cloud computing has become widespread among organizations seeking a cheaper way to access the infrastructure, service, and/or applications needed (3). This has changed the perception of organizations about software, infrastructures, and platforms for development (4). This essay aims to give an overview of cloud computing and various management issues faced by organizations during the implementation of cloud computing and to make possible suggestions that might help to solve these problems.

Platform-as-SaaS allows users to use cloud infrastructure applications from a provider without having to worry about managing or controlling cloud infrastructures such as servers, storage, network, etc. PaaS provides the customer with the ability to create their own administrations and applications with the help of administrations, programming dialects and devices upheld and supplied by the stage supplier (4-6). IaaS uses virtual machines to furnish customers with capacity, systems, handling power and other important computing assets that enable the shopper to send and run their applications and software.

CLOUD COMPUTING

Cloud computing offers points of interest such as adaptability, versatility, versatility of the frameworks, unwavering quality, wide system access, conveyance on-demand administration, economies of scale, cost-effectiveness and time-to-advertise expansion (4). While cloud computing offers many advantages for the organization, cloud computing management can be challenging, as it poses many problems for organizations (7). The following section will discuss issues related to information systems management with cloud computing, and the directions that the issues may take in the next five years. Recommendations are also made regarding possible ways by which cloud computing can explain these issues to ensure that associations receive the most extreme reward.

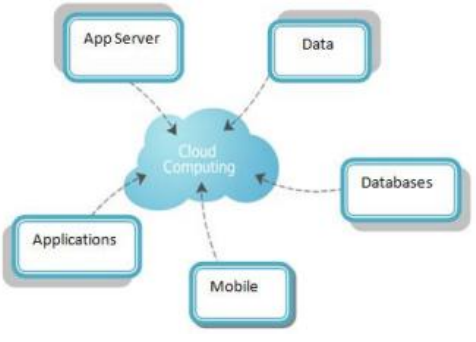

Figure 1.1: Cloud Computing

Similarly these cloud administrations may be in the three classifications.

PaaS-A platform where users can build their

- application using provider-supported languages, libraries, tools, and services.

SaaS-Application transmitted over a

- Organize, commonly the web, through a program or program interface; alluded to as programming on request.

IaaS-Capacity for processing and storage,

- networking and computing resources where the user controls the operating system and deploys the application; sometimes referred to as computing utilities.

Cloud computing deployment models: Cloud services are typically made available through a private, public, community, hybrid cloud to their customers.

Private Cloud-One organization owns, maintains and uses it, and its internal users use the services. Users within the organization may use the data, services available, and other applications.

Public Cloud: A single organization owns and maintains it but its services and applications are available for general public use. All services are available in this and any user can receive those services by paying the appropriate amount.

Community Cloud: An organization owns and maintains it for a given community. For any particular reason, many organizations could share this cloud; possibly it could be managed internally or externally. Hybrid Cloud-This cloud type is a combination of two or more clouds (for example, combining clouds from the public and the community).

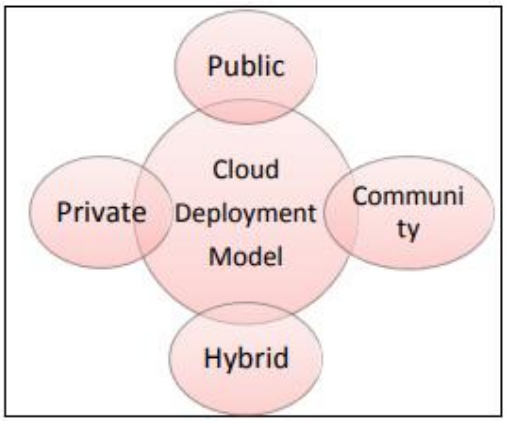

Figure 1.2: Cloud Computing Deployment Model.

Information systems management issues with cloud computing

Cloud computing management raises a number of issues related to the management of information systems, including ethical (security, availability, confidentiality and privacy), legal and legal issues, data lock-in, lack of standardized service level agreements (SLAs), customization, technology bottlenecks, strategic issues, implementation issues, sharing of reputation, dependency on the int Each of these issues will be discussed in more detail below.

Security

Security includes confidentiality, integrity and availability which helps to develop secure systems. Inside the cloud computing environment there is so much concern about security(4) Literature has revealed that security in cloud computing is the biggest management issue. Applications and data that service providers are hosting are prone to vulnerabilities from unauthorized parties(8) Security efforts should be made to prevent unauthorized access to information, applications, programming and equipment Ethical Issues Cloud computing presents important moral issues, such as security, secrecy, protection, respect and accessibility, since specialist cooperatives have a moral obligation to ensure that information and data are stored in their information for the client association.

Performance measurement

Measuring the level of service providers is a serious management issue for organizations to determine if the service provider meets the agreed level of service as set out in the SLA(8) This issue can be resolved in the next five years if the SLA defines clear measurement goals.

Risk management

cloud computing exposes organizations to a wide variety of risks, most of which were discussed in this paper earlier. Dealing with these dangers is a significant issue in light of the fact that cloud computing usage accomplishment relies on legitimate management, decrease and moderation of cloud-related risks(9) Within the next five years, this issue can be resolved by implementing available risk management practices such as disaster recovery planning.

Legal and judicial legislative and jurisdictional issues are very important issues related to the management of cloud computing information systems, given the possibility that data centers may be located in locations with different jurisdictions. In cases where data is in various jurisdictions. There is an urgent need for

lawmakers to come up with useful regulations which will help determine the legislation in force.

Architecture of cloud computing

Present a top-level cloud computing engineering right now that portrays various models of cloud conveyance administration. Cloud computing enhances coordinated effort, dexterity, scale, accessibility, and transmits cost-cutting potential through upgraded, competent computing. In particular, cloud portrays the use of a variety of conveyed administrations, applications, data, and foundations that include PC pools, system, data, and capacity assets

Those parts can be coordinated, provided, updated, and decommissioned immediately using a utility-like allotment and utilization model on request. Cloud administrations are used most of the time, but not constantly, in connection with a powerful mix, provisioning, arrangement, versatility, and scale enhanced by innovations in virtualization. While the very meaning of cloud suggests the decoupling of assets from the physical liking to and area of the framework that transmits them, many cloud depictions go to some outrageous by either misrepresenting or falsely restricting the numerous traits of the cloud. This is regularly done intentionally in an offer to blow up or minimize its extension. A few models incorporate recommendations that for a support of be cloud-based, that the Internet ought to be utilized as a transportation, an internet browser ought to be utilized as a methodology of access, or that the assets ought to consistently be shared outside the "edge" in a multi-inhabitant condition. From a structural perspective, given this unique development of innovation, there is a great deal of disarray encompassing how cloud is comparable and not quite the same as existing models, and how these likenesses and contrasts could influence cloud selection authoritative, operational and mechanical methodologies as it identifies with conventional system and data security rehearses. There are individuals who say cloud is a novel ocean change and specialized transformation, while others advocate it as a characteristic advance of innovation, economy, and culture. Today, there are numerous models available that attempt to address cloud from the point of view of scholars, modellers, engineers, designers, supervisors and even shopper. The engineering that we will focus on this part is explicitly tailored to the novel viewpoints of organizing sending the IT and offering support. Cloud administrations rely on five main highlights displaying their relationship to and contrasts with customary computing approaches (CSA Security Guidance, 2009).

These qualities include: I reflection framework, (ii) democratization of assets, (iii) located design administration, (iv) flexibility / dynamism, and (v) utility model of buyers and allotments.

Cloud computing security issues:

Cloud computing presents many unique challenges and security challenges. Data is stored in the cloud with a third party provider and accessed over the internet. That means there is limited visibility and control over that data. It also raises the question of how to safeguard it properly. It is imperative that everyone understands their respective roles and the security issues that cloud computing entails.

Providers of the cloud services treat the risks of cloud security as shared responsibility. The cloud service provider in this model covers cloud security itself, and the customer covers security of what they put in it. Cloud computing customers are always responsible for protecting their data from security threats and controlling access in every cloud service — from software-as - a-service (SaaS) like Microsoft Office 365 to infrastructure-as - a-service (IaaS) like Amazon's Web Services (AWS).

REVIEW OF LITERATURE

Hussain Aljafer et al. describe a portion of the important ways in which secure information sharing in the cloud computing condition can be handled and explicitly highlights the use of encryption plans and also gives a similar investigation of important plans by updating some agent structures. The survey is to show how encryption is used in each of the techniques covered, and discuss the corresponding open issues The objective is to provide a concise survey of existing solutions, discuss their advantages, and point out any shortcomings for future research.(10)

Mrudula Sarvabhatla et al. introduced an improved mutual authentication scheme that is secure and contrary to all major cryptoggs. The proposed authentication scheme prevents expensive operations that consume resources. With negligible computational overload on the client and server side and the ability to resist all major cryptographic attacks, our scheme becomes more practical. Also in resource fewer environments can be deployed. This scheme is based primarily on less expensive operations such as one-way hash computations and insignificant resource consuming XOR operations. Improved mutual authentication scheme is divided into three stages: stage of registration, stage of login, stage of mutual authentication.(11)

Inside a cloud domain, Dimitrios Zissis et al. acquaint a Trusted Third Party with explicit guarantee of security. This paper investigates cloud security by identifying security needs and attempts to display a potential response to kill these potential dangers. Plan standards for a cloud domain that come from the need to control

important vulnerabilities and hazards have been distinguished right now. A mix of PKI, LDAP and SSO can focus on most distinguished risks to cloud computing's uprightness, classification, validity, and accessibility of information and correspondence. Security requires a systemic point of view from which security will be built on trust and mitigate protection for a trusted third party in a cloud computing environment. Security is still a problem in cloud computing, but research shows that this is taking a positive turn and is greatly improving with the development of cloud technology and adoption. The survey results show that cloud technology is popular. The survey findings will inform Cloud-based e-learning tool development and deployment with the required security features.(9)

Jayant, D. Using the AES and RSA algorithm to provide a secure environment for the public cloud environment, et al. proposed role-base access control mechanism. Here, they use the RSA and AES model for the purpose of encryption and decryption where RBAC is used for access control. It gives different user rights and upload rights as per RBAC model.(13)

K. Nasrin, y. Al. Address that cloud storage frameworks are one of cloud computing's key research areas. Security is one of the major research preoccupations. They derived a mechanism which uses RSA and AES algorithms to combine asymmetric and symmetric key method. AES is useful for key sharing and in addition low overhead cryptographic component, RSA is useful for aggressors making complex marvels. The attackers ' focus was on proving secure communication of files from vulnerable network.(14)

Cindhamani. J et. Al. proposed enhancing the data security design. In order to achieve integrity, confidentiality and authentication in a single architecture it proposed a concept. They use 128 bit key for authentication purposes for RSA and third party auditor. Here, the solution proposed consists of two main parts, one of which is the storage of data and another of which is the retrieval of data from storage. This paper ensures security goals and guarantees about valid authentication and access during storage operations.

Chen, D. (15) Et al. addresses that data security greatly affects cloud services performance. They do not help maintain the privacy and originality of the content, but also help maintain confidence and reliability in service providers as well.

The mechanism for providing privacy protection concises all round analyzes. They compare their solution to airawet and aim to avoid leakage of information from the cloud environment. They are using MapReduce framework to deploy proposed solution. Tumpe Moyo et al discusses the various (8)

Kawser Wazed Nafi et al[10] have also introduced a similar improved security framework with the researchers above. OTP mechanism and security services have also been proposed for secure communication.(16)

CONCLUSION

Cloud computing is the new paradigm where computing is on demand. When the organization opts to cloud computing, it loses power over the information. The major problem is therefore providing security of its data during transmission and that is stored in the cloud. Any application which relies on an emerging technology should consider the various possible threats. Cloud users would definitely benefit from the various security issues presented in this paper to suggest a proper choice and cloud service providers to handle such threats effectively. Thus, a study of the cloud security environment and cloud security requirement was explored in our survey paper, and problem observations were addressed. As with cloud now, a user's way of working over the network is changing. In terms of cost and complexity it continually reduces the load on users. It also lets the association feel safe from security breaks and interferes with their information. It provides a sturdy way to serve users through a service-based model.

REFERENCES:

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. . A. Patterson, A. Rabkin, I. Stoica and M. Zaharia (2009). “Electrical Engineering and Computer Sciences, University of California at Berkeley," 10 February 2009. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS2009-28.pdf. [Accessed 12 July 2013].

2. S. Paquette, P. . T. Jaeger and S. C. Wilson (2010). “Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, vol. 27, no. 1, pp. 245 - 253.

3. E. D. Canedo, R. T. de Sousa Junior and R. de Oliveira (2012). "Trust model for reliable file exchange in Cloud Computing," International Journal of Computer Science & Information Technology (IJCSIT), vol. 4, no. 1, pp. 1-18.

4. D. Zissis and D. Lekkas (2012). “Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 1, pp. 583 - 592.

5. S. C. Misra and A. Mondal (2011). “Identification of a company’s suitability for the adoption of cloud computing and modelling its corresponding Return on Investment," Mathematical and Computer Modelling, vol. 53, no. 1, pp. 504 - 521.

6. M. Maurer, V. C. Emeakaroha, I. Brandic and J. Altmann (2012). “Cost–benefit analysis of an SLA mapping approach for defining standardized Cloud computing goods," Future Generation Computer Systems, vol. 28, no. 1, pp. 39 - 47.

7. X. Wang, Z. Du and Y. Chen (2012). "An adaptive model-free resource and power management approach for multi-tier cloud environments," The Journal of Systems and Software, vol. 85, no. 2, pp. 1135 - 1146.

8. Deyan Chen and Hong Zhao (2012). “Data Security and Privacy Protection Issues in Cloud Computing” IEEE International Conference on Computer Science and Electronics Engineering.

9. Tumpe Moyo, Jagdev Bhogal (2014). “Investigating Security Issues in Cloud Computing” 2014 IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems.

10. Hussain Aljafer, Zaki Malik, Mohammed Alodib, Abdelmounaam Rezgui (2014). “A brief overview and an experimental evaluation of data confidentiality measures on the cloud” journal of innovation in digital ecosystems 1, 1 – 11, Elesvior.

11. Mrudula Sarvabhatla, Chandra Sekhar Vorugunti (2015). “A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture” IEEE Future Information Security Workshop, COMSNETS.

12. Dimitrios Zissis, Dimitrios Lekkas (2012). “Addressing cloud computing security issues” Future Generation Computer System Volume 28, Issue 3, March 2012, (pp. 583–592), Elesvior.

13. Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S. (2015). “Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model” International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015.

14. Nasrin Khanezaei, Zurina Mohd Hanapi (2014). “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services” IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia.

15. Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh Babu (2014). “An enhanced data security and trust management enabled framework for cloud computing systems” IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China.

16. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem (2012). “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10.

Corresponding Author

Nisha Rani*

Computer Science