Volume 8, No. 2, March 2017 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Cloud Computing: Issues and Security Challenges

Awwab Mohammad
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
awwab92@hotmail.com

Sanna Mehraj Kak
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
sanah.mehraj@gmail.com

M. Afshar Alam
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
aalam@jamiahamdard.ac.in

Abstract: Cloud computing is a model that provides computing services through internet on demand and pay per use access to a varied number of shared resources such as storage, services, servers, networksetc. without accessing them physically. It is cost effective. As cloud computing has increased the standard of digital life, it has however increased the security risk as all the information is presented over an open source which can be breached. Cloud computing influences many technologies but it also pulls in the security issues which withstand with these technologies and helps to identify the vulnerabilities in any system and most importantly the threats that are included in cloud computing environment as well as to identify the possible solutions which is the point of discussion in this paper.

Keywords: cloud computing; security; data integrity; authentication; CSP(cloud service provider).

INTRODUCTION

The widest representation for Internet is cloud. Cloud computing is a new and advanced technology that is being used forbusiness purpose. Cloud computing [1] is accessing data over the internet and storing it instead of any available harddrives. No need for large investments in hardware or spending money or time on hardware is necessary while usingcloud. Instead we can provide the accurate size and type of computing resources that we need to get our project running and in shape [2]. We can access unnumbered resources and pay for only those resources. Cloud providing centres such as Microsoft Azure, Amazon etc. play a vitalrole. These centres provide utility computing service to software centres which can further provide application service to the end user through the internet. For the users' privacy protection, the sensitive data needs to be encrypted before being uploaded over the cloud. Some available data is shared within the trusted partners to the organization with the users'consent. In a cloud computing infrastructure, the available resources are in someone else's network and can be accessed remotely by the users [3]. Security always has been the core issue of computing practices. It is likely for any unwanted party to peek into anyone's private computer by adopting different hacking techniques thus increasing the securityconcerns [4]. Cloud computing cannot change or stop this nature of security breach but few measures can be been taken to secure the data over cloud.

Cloud Computing Building Blocks

Cloud services can be divided into: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service(IaaS).

*Software-as-a Service(SaaS): I*t is the biggest market. The provider allows the user to only use the applications. The software networks with the user through a user interface[5].

Platform-as-a Service(PaaS): It is a set of software and cloud development tools staged on the provider's server. Anyone can provide the hardware and the software application into programming functions upon which an application can be developed. Platform as a Service is an application development as well as a deployment platform delivered as a service to developers over the internet.

Infrastructure-as-a Service(IaaS): It offers virtual servers with unique IP addresses and storage blocks on demand. The user pays for the service they use which is called as utility computing.

There are four deployment models: Private cloud, Public cloud, Hybrid cloud and Community clouds.

- *Private cloud:* The private cloud lets systems and services to be accessible inside an organization. It provides more security due to its private nature.
- *Public cloud:* The public cloud lets systems and services to be accessible to the public. It provides less security due to its openness.
- *Hybrid Cloud:*The hybrid cloud is a combination of public and private cloud, in which the critical performances are handled using private cloud while the non-critical performances are handled using public cloud. A company outlines the goals and needs of services in this model[6].
- *Community Cloud:* The structure may be managed by a third party service provider. They are mainly based on settlements between business organizations. A cloud environment functioning under this model may exist remotely or locally.

The paper is organized as follows:

Section II, explaining authentication in cloud. In Section III, security issues in cloud computing including a bar graph is explained that represents respondents that see cloud security as a significant challenge. In Section IV, various solutions for the security issues are explained. And in section V, conclusion of the paper is stated.

I. Authentication In Cloud

Security is the most highlighted feature for any computing form making it obvious that security issue is critical in cloud environment. As cloud computing involves storing users' data at clients' as well as servers end, authentication is crucial in cloud environment. Verification of authentic user and protecting authorization are main security issues in cloud where disruption to any of these areas could lead to undetected security breach to some limited period [7].

II. Security In Cloud Computing

Cloud computing is the delivery of on demand computing resources as pay per use for on demand services. Thus security is a big issue as everything is controlled by a third party.

Security issues:Cloud computing has to be done at at provider level and at user level. Cloud computing service provider should guarantee security from the external threats that may come along theway. Better the service provider better is the security [8][9]. Security of a service provider can be checked whenever an attacker tries to breach in by acting like a legitimate user thus infecting the entire cloud. This affects the users that are using the shared infected cloud. Certain issues are raised as cloud security is being discussed.

1. Privacy issue
2. Data issue
3. Infected applications

Privacy Issues:Confidentiality is an important aspect of cloud computing. Since everything is handled by a third party, CSP make sure that the users' personal data is secured from being accessed by other users or CSP. The provider can encrypt the data that is to be stored on the cloud to ensure privacy which is not possible completely. As most of the servers are external, CSP keeps a check on who accesses and maintains the data so that the provider can protect the sensitive data [9][10].

Data Issues: Sensitive data over the cloud calls out to be the major issue concerned with security. Whenever data is uploaded on the cloud, anyone can access the data from anywhere and at any time depending on the type of cloud model used [8][9]. A number of users access and make changes to their data on the cloud at the same time. So there is no way to tell if the user is authentic or malicious. Data integrity is a standalone system with a one-on-one database [10]. In such systems, data integrity is maintained through database constraints and transactions. To ensure data integrity, transactions should follow ACID (atomicity, consistency, isolation and durability) properties.

Second issue to be deal with is *data location* [11][12].Physical location of data being stored is very important. It should be transparent to user and customer. Most well-known cloud service providers have data centres around the world. Provider does not expose where all the data is stored.

Third issue to be deal with is *data theft*. Cloud service provider does not install its own server but steals and acquires server from other CSP which makes it adaptable and cost effective for processes. So there is a possibility of data being stolen from the external server [11].

Fourth issue to be deal with is *data loss* [11]. If the CSP shuts down his services due to some crisis like legal or commercial, then the user would lose the data. Data loss can also be caused due to file corruption or damage due to natural causes like fire etc. Thus the above stated reasons may lead to the data being vulnerable to attacks and misuse thus making it inaccessible to users.

Infected Issues:CSP should have complete access to the server for maintaining and monitoring the server. This willcomparatively prevent the attacker from infecting the cloud which strictly affects both the user and the provider [11].

In 2014, Rightscale conducted its third annual state of the cloud survey, asking 1,068 skillfulness professionals across a wide cross-section of organization about their acceptance of cloud computing[12].

In compiling the state of the cloud survey, Rightscale Maturity model is used to analyze the organization based on different levels of cloud adoption.

Cloud Beginner: They work on initial cloud projects.

Cloud Explorer: They have multiple projects deployed over the cloud.

Cloud Focused: They include businesses that densely use cloud infrastructures.

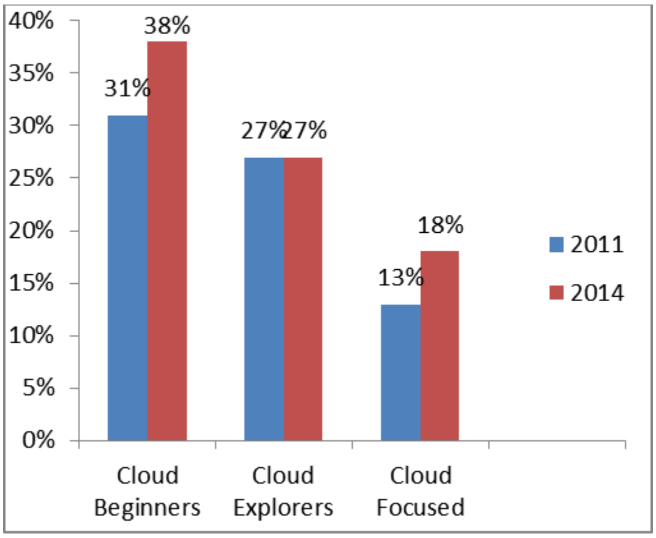

Figure 1: The above graph represents the respondents that see cloud security as important situation.

III. Solution To Security Issues

- ***Find The Right Cloud Provider:***Different providers have different security and management systems. So the first thing to actually do is to find the key cloud provider [13]. The CSP should be experienced, recognized, standard and by laws. Thus if we have the right CSP, we have a better chance of secure data storage.
- ***Use of Data Encryption:***It provides encrypted data for the development of the application to the security developer [8]. Thus additional security is not required and thus all the concerns related to security is taken under control by the provider. The developer must state the point at which data encryption strategy is to be used.
- ***Recovery Services:*** CSP must provide the user with the option of recovery that can be used in

case of data loss. So if the data is lost or tampered or disjoint, it can be recovered and used in the original form [13].

- ***Systematic knowledge of data flow:***Thereshould be a systematic knowledge of the data being stored and updated on a cloud [13]. Thus the provider would have all the knowledge about any data modification or data share so there should be complete analysis of data.
- ***Better Organizational Infrastructure:***Organizations should have structures which provide hardware modules like servers, routers etc. thus preventing malicious attacks [13].

IV. CONCLUSION

There are many rising technologies each with improvements and with the potential of making life easier but one must be careful considering the security risks while using these technologies. Similar is the case with cloud computing. It has great visions but the security threats included in the computing approach are directly proportional to the benefits provided byit. Both the attacker and the providers find great opportunities of getting access to the shared data on the cloud and can get whatever they want. Knowing the security issues and challenges that cloud-based computing faces, authenticity of the data is the among the main concern. To know if the data that is dealt with is tamper free or not is among the core issues which is the future work that is to be done regarding cloud. However, knowing the vulnerabilities of cloud would help the organization to make cloud secure. Moreover, we have discussed some important solutions that can help in making the cloud more secure by addressing the various issues and preventing the possible attacks.

V. REFERENCES

[1] K. Hashizume, D.G Rosado, E. F. Medina and E. B. Fernandez “An analysis of security issues for cloud computing”. *Journal of Internet ServicesandApplications,* 2013.

[2] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, *International Journal of Digital Content Technology and its Applications, AICIT,* Vol. 4, No. 5, pp. 143-152, 2010.

[3] D. Chen, and H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”. *International Conference on Computer Science and Electronics Engineering*, 647-651.doi: 10.1109/ICCSEE.2012.193.

[4] R. L Grossman, “The Case for Cloud Computing,” IT Professional, Vol. 11(2), pp. 23-27, 2009, No. 1520-9202.

[5] M. Jensen, J. Schwenk, N. Gruschka, L. L Iacon, “On technical Security Issues in Cloud Computing,” *Proc. of* IEEE *International Conference on Cloud Computing* (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] M. Ahmed, M. A Hossain “Cloud Computing and Security Issues in the Cloud”, *International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.1, January 2014.

[7] Available at: http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf

[8] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion Detection Techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[9] S. Pearsonand A. Benameur, ―Privacy, Security and Trust Issues Arising from Cloud Computing‖ in 2010 IEEE Second *International Conference Cloud Computing Technology and Science (CloudCom),*Nov 30-Dec 3,2010, pp: 693-702.

[10] A. B.Angadi, A. B.Angadi, K. C.Gull, “Security Issues with Possible Solutions in Cloud Computing-A Survey”, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* Vol. 2,No. 2278 – 1323 February 2013,

[11] P. K. Tiwari, Dr. B. Mishra, “Cloud Computing Security Issues, Challenges and Solution”, *International Journal of Emerging Technology and Advanced Engineering(IJETAC)*Vol. 2,No. 2250-2459, Issue 8, August 2012.

[12] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions", *Procedia Computer Science*, Vol. 37, pp. 357-362, 2014.

[13] M. A. Vouk, “Cloud Computing – Issues, Research and Implementations”, Journal of Computing and Information Technology- CIT 16, 2008, 4, 235–246, doi:10.2498/cit.1001391.

[14] H.Fayaz, A. Khalique, “A Review on Sociological Impact of Social Networking”. *International Journal of Engineering Applied Science and Technology*, Vol. 1, pp.612,2016.

[15] T.Bazaz, A. Khalique,“ A Review on Single Sign On Enabling Technologies and Protocols”. *International Journal of Computer Applications*, Vol. 151, No. 11,2016.

[16] B.Bashir, A. Khalique “A Review on Security versus ethics”. *International Journal of Computer Applications*, Vol. 151, No. 11,2016.