A Review on Cloud Computing Technology Threats and Security

Basweshwar B. Swami[1] Hemant A.Tirmare[2] Gajanan K.Mangnale[3] Rajesh R. Kshirsagar[4]
[1]UG Student [2,3]Assistant Professor [4]PG Student
[1,2,4]Department of Technology [3]Department of Computer Engineering
[1,2,4]Shivaji University, Vidya Nagar Kolhapur, Maharashtra India [3]Government Polytechnic, Limbala Hingoli, Maharashtra India

Abstract— this paper presents the issues of the cloud computing threats and security mechanisms. The paper presents comprehensive assessment of the architecture and various platforms of cloud computing technology. The paper also describes the major & minor challenges of cloud computing technology in detail. In accordance with several limitations and today's requirements for improvement mechanisms of security processes. Cloud computing technology is becoming most attractive especially for large organizations and business. Cloud Computing technology may affect the enterprises within next few years as it has the potential power to change current technologies. The paper also focuses on the data recovery issues occurred in cloud computing. The paper comprehensively discusses about types of the cloud computing in short. Cloud computing security key issues are discussed in short.

Key words: Security, Social Awareness, Sniffer Attack, Cloud Security, Data Abstraction, Patch Management, Cloud Computing Platforms

I. INTRODUCTION

As innovations in technology are increased rapidly, the attacks on the computer systems and data are increased in a proportion more than security enhancement. The attacker selects the system with low security and by using the various techniques he can play with user's confidential data and information.

Many authors had pointed the necessity of the strong security mechanisms to be implemented for the safe transactions in real world. (Ross and Tyler, Anderson, etc.) [1].

The cloud computing definition may be different for various users depending upon their requirement for the enterprise. The government sector companies and agencies uses their platform as the internal database can be shared among them. Each category of usage of cloud may have different levels of risks and advantages. The main key issue is to provide the security to the public and private clouds, for avoidance of theft of data. The goal to provide security based on integrity, availability, isolation and confidentiality. The confidentiality refers to the data abstraction. The data is only accessible to authorized person. The confidentiality can be implemented by the encryption and access control, also by enforcement of law. The integrity means the cloud must be protected and the data should not be altered by the unauthorized person, such alteration of data flow is done by attacker with the help of the man-in-middle attack. Integrity is enhanced by using robustness feature of control framework and maintaining regular audit of data flow across network. Availability means the system must be always available to the client. The availability can be extended by using the internet access for all internet enabled devices.

II. SECURITY THREAT ISSUES

As per survey of IBM the IT professional's concerns regarding the security are of only 42%, cloud based projects are back to the home. [7]

A. Authentication of data

The data stored on cloud server via internet is available to all unauthorized people. Therefore, only authorized user and assistance cloud must have access permissions.

B. Control over data usage

To validate and promote only legal users, cloud must have strong access control policies and mechanisms. Such services must be flexible, well organized, and consistent.

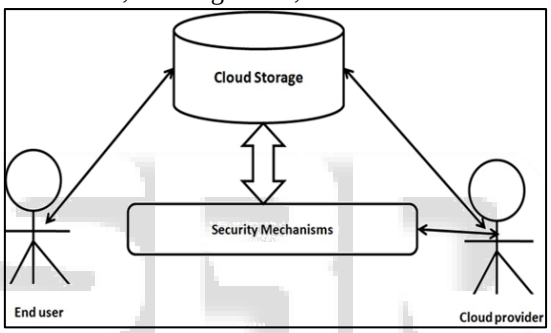

Fig. 1: Control over data usage

C. Methodology merging

Now-a-days several cloud providers provides the service to clients such as Amazon, Google. So each cloud provider having different policies and terms for data management over the cloud.

1) Service facilities:

In this various cloud providers such as Amazon, Google, get together for building a new converged service to fulfill needs of clients.

D. Assurance policy

The cloud provider management approach must be to develop a cloud platform that establishes the assurance of data security between both such as user and cloud provider.

1) Data Recovery

The cloud provider must define a method or procedure of restoring the data had lost, damaged or misplaced.

E. Malware Injection

In this type of attack, a malware-injection attempts to inject malicious code into the system. This attack may be in any form, in the form of code, scripts, and any free software.

To avoid this type of attacks the cloud provider server is required to constantly for exploit iFrame codes through the network media. Many web browsers provide the

All rights reserved by *www.ijsrd.com*

plug in and extensions for the same. The security mechanisms are handled by the cloud provider as shown in fig.1

III. CLOUD ARCHITECTURAL DESIGNS

A. Software as a Service (SaaS)

Cloud computing users release their data in a hosting platform, which can be accessed through internet by client. Cloud users not having any control over the cloud architecture, they have the only authority to access and store the data on cloud platform.

Examples of SaaS include Google Mail, Google Docs, etc.

B. Platform as a Service (PaaS)

This is the second type of architecture which supports for development of applications by the clients. The client directly develops his own service and can access it from cloud platform. An example of PaaS is Google AppEngine by which client can host his own apps and use the cloud platform.

C. Infrastructure as a Service (IaaS)

This system uses the virtualization that is mostly used in cloud to combine or separate physical resources from the logical resources. The main goal is to set up a independent virtual machine that is isolated from the hardware and other virtual machines. e.g. Amazon's EC2.

D. Data as a Service (DaaS)

This service is a special type in which the service is provided to the user on demand basis. It provides the facility to consumers and takes the charges from them for the service. e. g. Google BigTable.

IV. TYPES OF CLOUD

A. Private Cloud

Private cloud can be purchased and managed by the organization or an individual .It is expensive and most secure than public cloud. In private cloud service providers and the clients have the authority to set optimized control of the framework and security. Private clouds are dedicated to individual or any one organization e.g. Eucalyptus Systems

B. Public Cloud

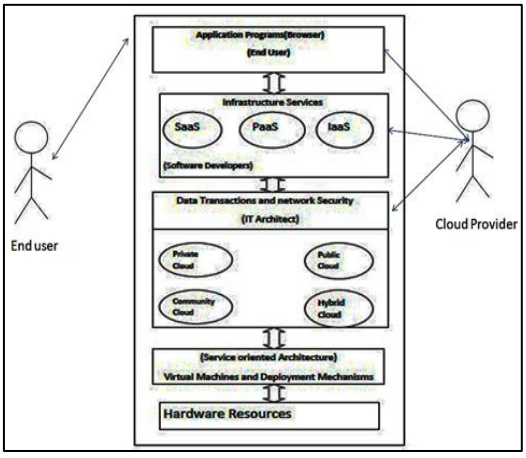

Fig. 2: Cloud types

A public cloud is shared by multiple clients and managed by a third party and exist in the company firewall. Multiple business organizations can work on the provided platform simultaneously. In this type of cloud consumers have no control over the framework, processes requiring powerful security. e.g. Google App Engine.

The above figure well describes the cloud computing types and architecture in detail.

C. Hybrid Cloud

In this type of cloud the merging of two or more clouds are linked in a way that data transfer takes place between them. These clouds created by the organization itself as per their strategy but management is split between the organization that developed it and the cloud service provider.

V. ENTITIES INVOLVED IN CLOUD COMPUTING TECHNOLOGY

A. Cloud Service Providers

This includes Internet service providers and telecommunication enterprises. The cloud service providers provide the facility to the user to access the cloud services and provide security mechanisms.

B. Cloud Service Brokers

This includes technology consultants, professional engineers and service enterprises, registered agents. Service brokers mostly emphasizes on the negotiation between clients and service providers without managing the whole Cloud platform. Also as per their need they can insert extra services on top of a Cloud platform to enhance the service set of cloud.

C. Cloud Resellers

Resellers are the important factor of the Cloud market for expanding the cloud business over the world. The cloud reseller may be any local agency which works for any large cloud data provider.

D. Cloud Consumers

The end user belongs to the Cloud consumers. We can also include Cloud service brokers and resellers in this category, as they are customers of another Cloud provider, broker or reseller.

VI. POPULAR CLOUD COMPUTING PLATFORMS

A. AbiCloud

Abicloud is a famous cloud computing platform; it can be used to develop, merge and manage public and private clouds. With the help of this platform user can easily host and manage the server, storage system, and virtual machines and applications and so on. The main difference between Abicloud and other cloud computing platforms is Abicloud is most powerful due to it is web-based platform. Using the Abicloud, user can create a new service by just drag and drop method with mouse. This is too easier than other cloud computing platform that helps in creating new services through command prompt. This reduces the number of lines code for development of virtual machine services.

B. Eucalyptus

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) is the platform used for development of open source cloud development mechanism. The Eucalyptus can be used for both public and private cloud development.

All rights reserved by www.ijsrd.com

C. Nimbus

Nimbus is an open set of tools which is a cloud computing solution providing IaaS. It permits users to purchase remote resources and to develop the required computing platforms through the development of virtual machines concept.

D. OpenNebula

OpenNebula is also open source cloud service Environment which allows client development and management of virtual machines on physical resources such as memory and files and it can set user's data centers or clusters.

VII. Applications of Cloud Computing

Following are applications of cloud computing technology:

- Cloud computing technology facilitates secure data storage.
- Cloud computing technology provides data sharing among different devices over internet at anytime and anywhere.
- The cloud computing technology provides big data access for users over the internet.
- Cloud computing technology requires less storage than individual as the data is shared among users.

VIII. Discussion

Based on our comprehensive discussion it was found that cloud computing security includes different security issues. Many security algorithms have been developed for avoidance of attacks and protection of cloud computing systems from threats. There are several advantages of using cloud computing technology such as cost benefits, fast deployment, improvement in accessibility etc. The data confidentiality, integrity and availability must be maintained properly.

IX. Conclusion and Summary

As per our opinion, cloud computing is the implementation of parallel computing, distributed computing and grid computing technologies defines a new era. Cloud computing technology is an emerged model of enterprise computing. We also discussed about the key security issues for cloud computing and applications of popular cloud computing platforms.

In this paper, we discussed the challenges and issues of cloud computing security. We also identified several challenges for cloud interoperability issue that is taking into consideration for further research and development. In this paper, we discussed about several cloud computing system providers and their security and privacy issues. Many researchers contributed their best efforts for minimization of data security issues in this domain with several solutions that described in this work.

A literature review of their works in the area of cloud computing technology and data security is carried out and the results of review are presented in this paper. The results describe that maximum invented approaches are based on encryption method. These results show the real fact that most of the research persons show their interest in encryption technique for ensuring the security on cloud computing platform.

Our review has explored the issues in cloud computing technology, further research and development is required to confirm the results. Future work in this paper includes the extension of this review by including more sources.

A future planning is to explore the remaining all security issues in the cloud computing platform and to build the strong security techniques for data security in cloud computing technology.

Acknowledgement

Our thanks to Department of Technology, Shivaji University, Kolhapur for allowing us to go ahead with this system.

My thanks to all people who directly and indirectly helped me to complete this work.

References

[1] Anderson, Ross and Tyler Moore. "The Economics of Information Security", Science 314, October 27,2006
[2] Bellovin, Steve "On the Brittleness of software and the infeasibility of security metrics", IEEE Security and Privacy, July 2006.
[3] Benioff, Marc, "behind the cloud", Jossey-bass 2009.
[4] Goodman, Peter," Yahoo says it gave china internet data", Washington Post, Sept.11, 2005.
[5] Allan A. Friedman and Darrell M.West, "Privacy and security in cloud computing", issues in technology innovation No.3, October 2010.
[6] Aized Amin Soofi, M.Irfan Khan and Fazal E Amin,"A review on data security in cloud computing", International Journal of Computer Applications Vol.94 ,no.5,May 2014.
[7] IBM, "What is cloud computing?"[online], http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html
[8] Rabi Prasad pandhy,Manas Ranjan Patra,Suresh Chandra Satpathy, "Cloud computing: Security issues and research challenges", International Journal of computer science and information technology and security, vol 1, No.2, Dec-2011.
[9] B.P. Kandukuri, R.Paturi V., A.Rakshit,"Cloud security issues", IEEE International conference on services, computing, Banglore, India pp.517-520.
[10] Tout, Sverdlik and Lawver,"Cloud computing and as security in higher education", in proceedings of the proc, ISECON-2009.
[11] Santosh Kumar and R.H.Gouder, "Cloud computing: Research issues, challenges, architecture, platforms and applications: a survey", International Journal of future computer and communication, vol.1,No.4,Dec-2012.
[12] R.L.Grossman,"The case for cloud computing", IT professional, vol.11 (2), pp.23-27, 2009, ISSN-1520-9202.
[13] A.Williamson,"Comparing cloud computing providers", cloud computing journal, vol.2, No.3, pp.3-5, 2009.
[14] Manpreet Kaur, Hardeep Singh, "A review of cloud computing security issues", Journal of advances in engineering and technology, June 2015, ISSN-22311963.
[15] P.Mell and T.Grance,"Draftnist working definition of cloud computing ", vol.21, Aug-2009.

All rights reserved by www.ijsrd.com

[16] Manjur Ahmad and Mohammad Ashraf Hossain,"Cloud computing and security issues in the cloud", IJNSA, vol.6, No.1, Jan-2014.
[17] Kim.w"Cloud computing today and tommarrow" Journal of object technology, pp.65-72.
[18] Mosher R."Cloud computing risks", ISSA journal, july issue, pp.34-38.
[19] Vishal Vijaykumar Parkar, H.A.Tirmare,"Aggregating static and dynamic methodologies for PHP application security assessment", vol.2, issue 3, June 2015 pp.253-256.

All rights reserved by *www.ijsrd.com*