International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Study on Security Controversies and Techniques in Cloud Computing

[1]Cholleti Jyothi, [2]Paladi Bhavani

[1,2] Assistant Professor, Department of Computer Science and Engineering,
TKR College of Engineering and Technology, Hyderabad, Telangana.

Abstract— *Cloud computing have turn out to be a popular slogan in IT industry as area of computer technology. On behalf of growing the infrastructure at low-cost cost, universally the organizations are moving to cloud based system. Cloud computing decreases the client organization having the complete physical infrastructure of software and hardware. However, with all strength and flexibility provided by cloud there are some concerns regarding security which may turn out to be a resilient obstruction. Service providers have been geographically dispersed due to enhanced migration of organization from traditional system to the cloud. Hence the data are usually stored in the servers that are remotely located at various places and unauthorized parties may have access to those data which directs to various security issues like data availability, data leakage, resource pooling, diffident interface, cloning, allocation of data and some attacks in the interior. This paper presents a review on the security issues in security standards followed in cloud, infrastructure, access control, third party privacy, confidentiality, reliability and integrity of data. It portrays the techniques employed in addressing cloud security issues and its challenges.*

Index Terms *—Cloud computing, Service provider, Cloning, Infrastructure. Cloud Security.*

I.INTRODUCTION

Cloud computing bestows hosted services by sharing the processing resources, data for computing, virtual machines, storage and other services on demand basis and it is internet dependent computing technology. The cloud user does not require more knowledge to use cloud they need to pay based on their consumption of resources. It is in the form of abstraction, let clients to make use of services similar to internet with qualities such as increased scalability, maximum output, service reliability and great computing power. Cloud is characterized by on-demand self-services, wide network access, reduced maintenance, speedy elasticity, enhanced productivity, precise services, etc. Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the three types of services in cloud namely. Cloud computing offers a comfortable way to obtain high quality applications with hosting and storage services through the internet [7].

II. PRIMITIVE CLOUD SERVICES

A. Software As A Service (SAAS)

SAAS offers customers towards develop software applications on demand over the Internet which running on cloud infrastructure and accessible to client machine in the course of lines such as web browser. Services such as software for operating system, databases, servers, network access, power, and data center space, etc. are contracted by the Cloud service provider [3].

B. Platform As A Service (PAAS)

PAAS provides a layer of application buildup or an environment to develop software which is encapsulated and offered as a service. The user has the freedom to build his applications and it runs on the provider's high level infrastructure. Various features of PAAS are auto scaling, supports multiple hosting, extensibility, etc.

C. Infrastructures As A Service (IAAS)

IAAS specifies to the distribution of computing resources, basic storage and computing capabilities for executing services using virtualization technology. IAAS provides fundamental computing resources such as servers, storage system, network,etc.

III. CLOUD DEPLOYMENT MODELS

A. Public Cloud

Public cloud is managed, operated and hosted usually by third party providers and they are out of scope of firewall. The physical infrastructure is generally possessed by service providers and directed by the assigned service provider and located within the provider's data centers [7].

B. Private Cloud

Private cloud infrastructures are generally handled through an organization and made available to specific set of users. The private cloud can also managed by third party. In this deployment model, it makes sure that no additional security policy, official necessities or bandwidth obstructions since it offers greater control and configurability of the infrastructure and security.

C. Hybrid Cloud

Hybrid cloud is the blending of both two previous cloud models which lets greater flexibility for business and more data deployment models. It helps to perform diverse functions within same organization. Hybrid cloud provides secure services such as receiving customer payments, secondary business processes such as employee payroll processing. [4]

D. Community Cloud

Community cloud has mutual analyze include security, strategies, etc, among organization and communities in the Cloud infrastructure. Third party service provider manages the shared scheme of infrastructure which is allotted by several organizations.

IV. SECURITY CONTROVERSIES IN CLOUD

A. Access

Hijacking is done by unauthorized users which deal with hackers gaining access to your account. It comes under the category of phishing, fraud, software victimization, manipulation of software vulnerabilities like buffer overflow attacks, etc. The major concern in hijacking is illegal control of user account through that account be able to eavesdrop during transactions, influence of data, providing false and business harming responses to clients, and transmit customers to a wrong sites [1].

1) Malicious insiders:

A present or former employee, supplier, or other contractual partner considered as a malicious insider to an organization, that one misuse their position for information outbreak that harmfully influenced the privacy, uprightness, or accessibility of the company's data either statistics systems. In that way, for cloud computing insider is measured to be an unit who works for the cloud host, having privileged access to the cloud resources, malicious insider threat detection in cloud computing environment and who uses the cloud services [2].

2) Authentication mechanism:

Authentication for the valid user or the system is the primary factor which is concerned in both the old and current standards. Cloud Service Provider request clients to accumulate their account details in the cloud and infinitely Cloud service provider have access to those data this leads to privacy issues. There are many copies of account will point to multiple authentication processes for all cloud service, the customer needs to switch their authentication mechanism which redundant actions ahead to abuse of the authentication mechanism[3].

3) Privileged user access:

When vulnerable data is handled outside the enterprise, or by non-employees, it imply that organizational managers are less instantaneous aware of the nature and level of risk and that they have no direct facility to control these risks. It is exactly the case that reliable companies employees are capable of create mistakes. Privileged users cannot access all information at any time or anywhere. Conventional methods for securing networks are inadequate for privileged users due to that powerful claim are lacking, it require rigid access control and management [4].

4) Browser security:

The client and server in the cloud accomplished by a client sending request to the server and wait for the result where server performs the computational process. A connection medially client and cloud service provider is Web browser which relates to the cloud system. As discussed before client proceed a request and needs to validate by its own to check the authority of the user on the cloud system. Client credentials are signed using Extensible Markup Language signature to authenticate and XML encryption to encrypt the SOAP messages [5].

B. Security Standards

1. Inadequacy in auditing: Information Technology security audits focuses to figure out whether an information maintenance system and its managers meet up both the constitutional hope of users data protection and the company's rules of achieving financial growth against various security threats. Organizations still uses traditional IT audits to find issues.

*2. Compliance risks :*Internal controls protect the integrity of the company's properties and the accuracy of its financial reporting. Information security controls are a important part of the frameworks. It helps internal controls to be effective. Businesses that export their data processing to a cloud vendor are not responsible for internal control of the data[6].

3. Inadequacy of legal aspects (service level agreement): Service level agreement is a bond among the client and service provider in the cloud environment which allows copying of one to many servers when call appear based on priority scheme, the cloud may diminish less performing softwares.Cloud vendors should assess the Service Level Agreement to cloud customers is a major issue. SLAs gives assurance in offering resources to make security dealing with the customers

4) Trust: Trust is crucial factor in cloud computing environment in current practice it depends mostly on Observation of characteristics, and own evaluation vendors of cloud service vendors. Existing trust mechanisms in the cloud are characteristics based trust, SLA confirmation based trust, Cloud transparency techniques, Trust as a service, Formal endorsement, audit, and standards. In order to attain the service, it requires to be used in blend with social and technological mechanisms for providing persistent trust.

5) *Inadequacy of standards:* The lack of cloud standards, rules and interoperability has made it hard to move their data between private, public and hybrid clouds. This problem can reduce the cloud adoption. As there are no proper universally approved or recognized cloud standards to establish powerful security, many groups of standards bodies are working to enhance these specifications

C. Cloud Infrastructure

1. Multi-tendency: One of the crucial securities between the client and service provider in cloud computing environment is Multi-tenancy. In a separate server, details of the sharing resources and data used by numerous connected systems are maintained at the same time security of those virtual machines should be guaranteed by the cloud service provider. It is complex task to overcome this issue of multitenancy, the following things to be concentrated such as isolation of virtually connected machines, communication over network, execution of data and memory resources [8].

2. Quality of service: Another threat in cloud application is quality of service (QOS) management as it is responsible for allocation of the resources for services. The cloud service platform is provided by the vendors and they usually adopt single renting scheme because of which the service request are not acknowledged instantly. This issue is due to lack of servers and thus the response time is comparatively high[9]..

3. Insecure interface of API : API is used by developers which act as a interface between the cloud service providers and to the client. It allows the users to manage and get the information from the service providers. API and the related software need to be highly secured as it is used by the cloud users to access their data. API are the public front door entry to the data and accessible externally thus they incorporate many threats in it [10].

V.TECHNIQUES IN CLOUD SECURITY – A REVIEW

The following Existing work deals out various research contributions in addressing cloud data security

Manivannan et al [12], have proposed a secured mechanism for encryption of database known as transposition, substitution, folding, and shifting (TSFS) algorithm with three key. When the number of keys increased, then the processing and computation may also increase. Encryption of database particularly the data stored in the database need to be encrypted which helps to enhance the privacy and security of data stored in cloud. For mutual transmission, synchronizer used to gather all the keys and the client system receives the key from the synchronizer which decrypt the distributed data that is already encrypted. A three-layer system structure is proposed by Navia Jose et al [18] in which each layer performs its own duty to ensure the data security of cloud layers. Authentication of user is done in first layer and the data encryption by using AES algorithm is done in second layer. First layer uses access control tools to check for authorized user and to restrict unauthorized access to users data. The third layer supports the faster user data recovery by using Byzantine fault tolerance algorithm methods.

In these model, a encryption and decryption technique for provide security to that data is implemented by Goikar Vandana et al[13],. Also provide a extra security layer we use the user location and geographical position. To provide this, we need Anti-spoof GPS which is gives very accurate location of the user for accessing data and it can give us the latitude, longitude and altitude accurately This method can be useful for many applications such as banks, big companies, institutions, etc.

As reported by Ahmed E. Youssef et al[15], proposed a security model for cloud computing which improves the privacy issues in cloud and it can also protect cloud from vulnerabilities. It consists of various units such as verification and validation, privilege control, data protection, attack detection/prevention unit. The working of first layer is to validate the data accuracy, integrity and shared resources in the cloud though it performs authentication of cloud users. Privilege control security unit is necessary to control cloud usage by Different individuals and organizations. It protects user's privacy and ensures data integrity and confidentiality by applying a collection of rules and policies that control that has the authority to do what on the cloud. The last most layers in this model is detection and prevention unit which detect attacks and malicious insiders for data access and also prevent unwanted modules being installed without the knowledge of service provider. It increases the security system within the cloud environment.

VI. CONCLUSION

In this paper we examine the sharing of resources with measurement of security level that they provide on their cloud should be informed to the customers by the cloud service providers. This article understands different models of cloud computing, numerous security issues in securing cloud. Data security is one of the key issues in cloud computing. There are countless other security threats that include some of the security aspects of trust, infrastructure, access, network, virtualization, etc.

REFERENCES

[1]A.Annie Christina, "Proactive Measures on Account Hijacking in Cloud Computing Network," Asian Journal of Computer Science and Technology, Vol. 4 No. 2, 2015.

[2] Atulay Mahajan, "The Malicious Insiders Threat in the Cloud," in International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April,2015.

[3] Monjur Ahmed1 and Mohammad Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud," International Journal of Network Security & its Applications , Vol.6, No.1,January 2014.

[4] Ch Gowthami, " Control Cloud Data Access Privilege using Attribute based Encryption," International Journal of Computer Science and Information Technology & Security,Vol.6, No.2, Mar-April 2016.

[5] Ms. Disha H. Parekh, " An Analysis of Security Challenges in Cloud Computing," International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013.

[6]K.Samunnisa,Maloth Bhavsingh, "Privacy-Preserving Scalar Product Computation over Personal Health Records International Journal of Computer Engineering in Research Trends,vol.3,no.12, pp. 42-47,2016.

[7] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges," International Journal of Computer Science and Information Technology & Security Vol. 1, No. 2, December 2011.

[8] M.Saraswathi "Multitenancy in Cloud Software as a Service Application," International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 11, November 2013.

[9] Danilo Ardagna, "Quality of Service in Cloud Computing: Modeling Techniques and their Application," Journal of Internet Services Applications, December 2014.

[10] Muhammad Kazim, "A Survey on Top Security Threats in Cloud Computing," in International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, 2015.

[11] Bhavani B H "Resource Provisioning Techniques in Cloud Computing Environment: A Survey," International Journal of Research in Computer and Communication Technology, Vol 3, Issue 3, March-2014.

[12] D. Manivannan and R. Sujarani, "Light Weight and Secure Database Encryption using Tsfs Algorithm," Proceedings of the International Conference on Computing Communication and Networking Technologies, Ieee,2010.

[13] Goikar Vandana T. et al, " Improve Security of Data Access in Cloud Computing using Location," International Journal of Computer Science and Mobile Computing, Vol.4 Issue.2,February-2015.

[14] Jahangeer Qadiree, Mohd Ilyas Maqbool, " Solutions of Cloud Computing Security Issues," International Journal of Computer Science Trends and Technology – Volume 4 Issue 2, Mar - Apr 2016.

[15] Ahmed E. Youssef and Manal Alageel , "A Framework for Secure Cloud Computing," International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.

[16] Nidal M. Turab , Anas Abu Taleb Shadi R. Masadeh, "Cloud Computing Challenges and Solutions," International Journal of Computer Networks & Communications Vol.5, No.5,September 2013.