Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 5(A), pp. 26497-26500, May, 2018

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

A SURVEY ON CLOUD COMPUTING: DATA SECURITY CHALLENGES AND THEIR DEFENSIVE MECHANISMS

Shanthni KK., Kaviya K and Sujithra M

Department of Computing, Coimbatore Institute of Technology Coimbatore

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2070

ARTICLE INFO

Article History:

Received 16th February, 2018
Received in revised form 12th March, 2018
Accepted 20th April, 2018
Published online 28th May, 2018

Key Words:

Cloud, security, encryption, cloud Service, threats, vulnerability, mechanisms.

ABSTRACT

Saving data in cloud has become the most important evolving process in past few years. By tremendous growth in the analysis field, cloud has become a way to store data in large number and the users are allowed to try to test various ideas in low or even in free of cost. Cloud computing plays a major role by storing the data and it can be arranged by a third party. The major drawback in the cloud field is privacy and security issues. One of the main issue is the data security and privacy of information stored and processed at the cloud service provider's systems. Despite of all these services provided by cloud, it lags in the major side of security. The main idea of this paper is to identify the security challenges and issues faced in cloud and to provide appropriate solution to make the service process more efficient and secure.

INTRODUCTION

Cloud computing can be defined as a method of delivering the trending technology to the consumer by using Internet servers for processing and data storage, while the client system uses the data. Cloud computing aims to provide scalable and inexpensive on –demand computing infrastructures with good quality of service levels. Today cloud is used in every sector even in small scale industries, vendors and start-up companies to big organisations. It also enables the organisations to focus on their main domain and to maintain their infrastructures and proponent says that they adjust the resources more frequently in order to meet the oscillation and customer's demands that cannot be predictable. Main goal of cloud computing is to provide a trying and testing at minimum cost or in other words customers can pay only for the resources what they use. This provides scalable and minimum cost on-demand computing infrastructures with good quality of service levels. [1].

Characteristics of Cloud Computing

NIST further specifies that cloud computing exhibits the following five characteristics in its operation

- On-Demand Self Service
- Broad Network Access
- Measured Service
- Rapid Elasticity
- Resource Pooling

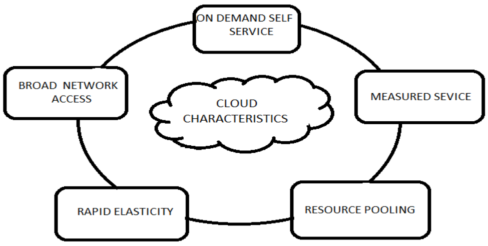

Fig 1 Characteristics of Cloud Computing

Ondemand Self Service

On demand self-service means that customers can access the functionalities and services without dependency. Consumer can provide capabilities of computing such as server time, network storage, automatic Information Technology (IT) resources that require no human interactions. The user can also modify or trim the functionalities and provision its facilities based on the customer's needs.

Corresponding author:* **Shanthni KK.,
Department of Computing, Coimbatore Institute of Technology Coimbatore

Broad Network Access

This means that resources can be accessed in any type of platforms like mobile phones, laptop, and desktop from any far (remote) location over the network. Companies prefer private cloud service because they will be relevant about their information leaks in outer area. I

Measured Service

The important need of cloud computing is the measured service. This is reference to services where the cloud provider notifies the provision of services for many types of reason including billing, effective use of resources, or planning prediction throughout the system. Here, both the customer and service provider must be aware of the level of software being used so that it can be used for predictive planning of understanding the overall performance and to view the effectiveness of the resource.

Rapid Elasticity

Rapid elasticity is one of the main key characteristics of cloud computing, where the capabilities can be elastically arranged and released automatically based on the inward and outward on corresponding demand. In other words, the customer can increase or decrease the software requirements according to his need which will be cost efficient for him.

Resouce Pooling

The resources of cloud are pooled and presented to more than one user suing the Multi-Tenant Model. They can be assigned and reassigned dynamically and it can be offered based on the customer's needs. This Multi-Tenant model made the user to share the same corporal hardware to more persons so that the user can use the software with less financial costs. Multiple mirror copies are stored and mirroring process is done to decrease the loss of data. [2].

Cloud Service Models

Since cloud computing can fulfil virtually any IT needs in many ways, these classifications are necessary to indicate how that service accomplishes its role. In other words, SaaS, PaaS, and IaaS are the three main paradigms of cloud computing.[3].

- Platform as a service (PaaS)
- Software as a service (SaaS)
- Infrastructure as a service (IaaS)

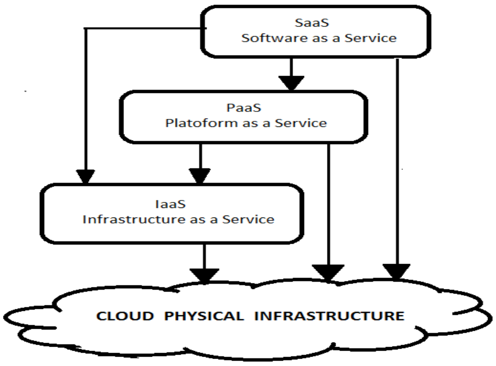

Fig 2 Cloud Computing Service Models

Platforms as a Service (PaaS)

A PaaS model is that the ability of a seller to move into the cloud and use the hardware over the internet for customers. It is one-step above the IaaS model where the user can manage the runtime and middle ware devices. PaaS provides many services and that facilities must also be available up-to-date. It can save money developing new services and applications and it can be released more quickly to get user response.

Examples of PaaS market player are Google AppEngine, Windows Azure Platform, and force.com.

Software as a Service (SaaS)

SaaS patterns are predictable by companies that want to profit from application custom without the need to maintain and update substructure and components. It has a complete operating system with a claim management and a user interface. It is only the service which arises along with Platform as a service (PaaS) and Infrastructure as a service (IaaS). The consumer does not manage the fundamental SaaS model that provides the great flexibility and elasticity.

Example

Mail, ERP, collaboration and office apps are the most accepted by SaaS.

Infrastructure as A Service (IaaS)

IaaS provides a virtual machine, virtual storage, virtual substructure, and other hardware properties as resources that to the customer. Compared to the SaaS and PaaS models, the IaaS level has a major contribution since it is the platform for placement and services. Many IaaS now provide database services, message queues, and other such services which are assessed according to the priority of the consumers. Several use cases can benefit from this pattern. Companies that lack a maintained data centre look to IaaS as a quick, cheap infrastructure for their business inventiveness that can be extended or ended as needed.

Cloud Deployment Models

Public Cloud

These are virtualized infrastructure that can be easily accessed by any user. They can enter the cloud and access their essential set of data for free. The free access is offered for limited resources. They can be easily accessed and managed from a self-servicing portal.

Private Cloud

An organisation with a group of people can access the cloud. They are provided with a limited set of resources within a third party, or some grouping of them, and it may exist on or off premises.

Community Cloud

The cloud is allocated for a specific sector of users, like those in politics, military or police. Here, the cloud can be obtained and managed by one or more organisations in that community.

Hybrid Cloud

As of cloud infrastructure hybrid is a combination of 2 or more community of people that remain as a unique entity but are managed by a standard technology that enables data and application portability.[4].

Security Challenges

Despite all these sources in the field of technology over the past few years cloud has developed as one of the significant factor that we use in day-to-day process. Security is one among the cloud that need to be changed i.e. progress should be made in security level in order to make the cloud platform more efficient. The malware assaults cannot be prevented without making a change in the infrastructure of the cloud security level.[5].

LAYER	CLOUD COMPUTING COMPONENTS
Five Characteristics	On-demand self service Broad network access Resource Pooling Rapid Elasticity Measured Service
Three Delivery models	SaaS PaaS IaaS
Four Deployment Models	Public Private Community Hybrid

Fig 3 Cloud Environment Architecture

The security level varies across the cloud service models where the IaaS has the least level security while the SaaS has the highest level of security. Data leak avoidance is considered as the most important factor to be resolved. These are the main areas where security field is concerned as follows.

Confidentiality

This is linked to data secrecy since this is the property confirming that the data that belongs to a CSC is not visible to any illegal parties. In open clouds, the CSP is mainly responsible for safeguarding the CSC's data. These two methods allow intruders to have full access to the host and cross- VM side channel attacks to abstract data from a target VM on the same device.[6].

Integrity

The integrity of data refers to the sureness that the data stored in the cloud is not altered in any way by unauthorised parties when it's being retrieved, i.e. you get out what you put in. To confirm this, CSPs must make sure that no third party has access to data in transfer or data in storage. Only official CSCs should be able to change their data.

Availability

This property ensures that the CSC has access to their data, and is not denied access mistakenly or due to mischievous attacks by any entity. Attacks like denial-of service are typically used to deny accessibility of data

Privacy

It is one of the more significant problems to deal with in the cloud and in network safety in general. Privacy confirms that the personal data and identity of a CSC are not exposed to illegal users. This property is most vital to the CSC, particularly when they deal with complex data.[7].

Mechanisms-High Sensitive Data

These mechanisms are used for extremely sensitive data. The cloud security system can be improved in the following ways.[8].[9].[10].

- For securing data both at rest and in transit, cryptographic encryption mechanisms are definitely the best options to confirm data security against popular threats and data storage security. Data Encryption: Encryption is the key policy used to protect data. It is better if cloud servers automatically encrypt data when user uploads data.
- The Service Providers should be given limited access to the data, just to manage it without being able to see what exactly the data is.
- Data backup and redundant data storage to make data retrieval easy due to any type of loss unlike the recent breakdown issues with the Amazon cloud.
- Distributed identity management and user security is to be maintained by using either Lightweight Directory Access Protocol (LDAP), or published APIs (Application Programming Interfaces) to connect into identity systems.
- Authentication in the Cloud - cloud computing is associated with having users' sensitive data stored both with a CPC and a CSP, identity and access management (IAM), a form of access control, is very crucial.
- Access Mechanism: Strong verification procedure must be used. To reset or alter authentication attributes like password secure method must use.
- Digital Signature: Use of digital signature for exchange of data ensures security as only intended user can access data [11].[12].

CONCLUSION

Both the cloud service provider and the client should make sure that the cloud-data stored is free from all external threats. In order to keep the data secured these threats must be controlled because data residing in the cloud will also cause numerous number of threats and there may arise some security issues, accessibility issues, lack in privacy and reliability of data. In this paper various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed. The classification and mechanism proposed in the above work would definitely make the cloud-data stored free from threats and makes a choice to provide more security and privacy. The proposed work also contains the data security challenges and solutions to overcome the threat involved in cloud. To provide a secure data access in cloud, advanced encryption methods can be used for storing and recovering data from cloud.

References

1. L. Badger, T. Grance, R. Patt-Corner and J. Voas, “Cloud computing synopsis and recommendations (draft), nist special publication 800-146”, Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).
2. U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, “Cloud based secure and privacy enhanced authentication & authorization protocol”, Procedia Computer Science, 22, (2013), 680-688.
3. T. Acar, M. Belenkiy and A. Küpçü, “Single password authentication”, Computer Networks, 57(13), (2013), 2597-2614.
4. G. Wang, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, Computers & Security, 30(5), (2011), 32331.
5. C. I. Fan and S. Y. Huang, “Controllable privacy preserving search based on symmetric predicate encryption in cloud storage”, Future Generation Computer Systems, 29(7), (2013), 1716-1724.
6. D. W. Chadwick and K. Fatema, “A privacy preserving authorisation system for the cloud”, *Journal of Computer and System Sciences*, 78(5), (2012), 1359-1373. *International Journal of Grid and Distributed Computing* Vol. 9, No. 1 (2016) 56 Copyright ⓒ 2016 SERSC
7. M. Hange, “Security Recommendations for Cloud Computing Providers”, Federal Office for Information Security (2011).
8. G. Brunette and R. Mogull, “Security guidance for critical areas of focus in cloud computing v2”, Cloud Security Alliance, (2009), 1-76.
9. M. Sujithra, and G. Padmavathi, “Ensuring Security on mobile device data with two phase RSA algorithm over cloud storage”, *Journal of Theoretical and Applied Information Technology*, Vol.80. No.2 ISSN: 1992-8645, October 2015.
10. DeCandia, G., Hastorun, D., Jampani, M., Kakulapati, G., Lakshman, A., Pilchin, A., Sivasubramanian, S., Vosshall, P., and Vogels, W. (2007). “Dynamo: Amazon’s Highly Available Key-Value Store. “In Proceedings of the 21st ACM SIGOPS Symposium on Operating Systems Principles (SOSP’07), pp. 205-220, Stevenson, WA, USA, October 2007.
11. Heritage, T. (2009).” Hosted Informatics: Bringing Cloud Computing Down to Earth with Bottom-Line Benefits for Pharma”. Next Generation Pharmaceutical, Issue 17, October 2009.
12. Itani, W., Kayssi, A., and Chehab, A. (2009). “Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures”. In Proceedings of the 8th IEEE International Conference on Dependable, Automatic and Secure Computing (DASC’09), pp. 711-716, Chengdu, China, December 2009
13. Kaufman, L. M. (2009).” Data Security in the World of Cloud Computing.” IEEE Security & Privacy, Vol 7, Issue 4, pp. 61-64, July-August 2009.

How to cite this article:

Shanthni KK., Kaviya K and Sujithra M.2018, A Survey on Cloud Computing: Data Security Challenges and Their Defensive Mechanisms. *Int J Recent Sci Res.* 9(5), pp. 26497-26500. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2070

****