ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

A Survey of Security and Privacy Challenges in Cloud Computing

Sakshi Nema

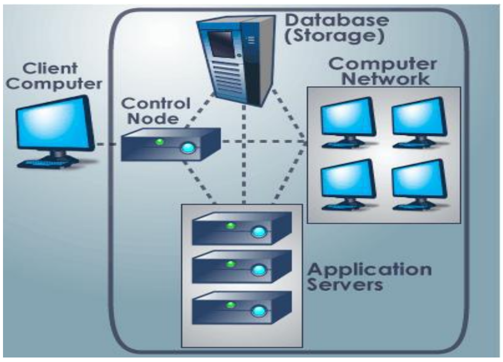
M. Tech (Computer technology and application), Dept of CSE, Gyan Ganga College of Technology, Jabalpur, India

Abstract: While cloud computing is gaining popularity, diverse security and privacy issues are emerging that hinder the rapid adoption of this new computing paradigm. And the development of defensive solutions is lagging behind. To ensure a secure and trustworthy cloud environment it is essential to identify the limitations of existing solutions and envision directions for future research. In this paper, we have surveyed critical security and privacy challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions.

Keywords: Cloud, Security, Privacy, Survey

1. INTRODUCTION

Enables convenient, on-demand network access to a large shared pool of configurable computing resources (e.g., networks, Cloud computing is defined as a service model thatservers, storage, applications, and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. This innovative information system architecture, which is fundamentally changing the way that computing, storage and networking resources are allocated and managed, brings numerous advantages to users, including but not limited to reduced capital costs, easy access to information, improved flexibility, automatic service integration and quick deployment[2]. Cloud computing has some attributes that are shared, standard service, solution packaged, self service, elastic scaling and usagebased pricing.



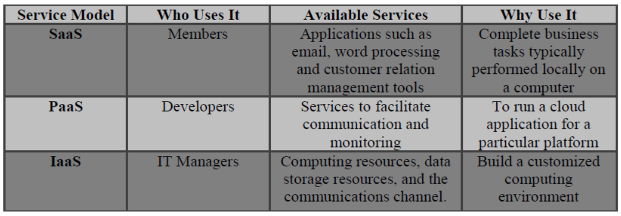
.Fig 1: Cloud Computing

A. Different Service Models

1 .software as a service (SaaS) - model SaaS is software that is developed over internet. It is a delivery model where the software and the associated data are hosted in a cloud environment by a third party such as Cloud Service Provider (CSP). It provides an application to customers either as a service on demand. It is mainly accessed through web portal and service oriented architecture based on some of the web service technologies.

2. platform as a service (PaaS)- Is a computing platform that allows creation of web applications easily without the complexity of maintaining the software. Is a delivery model where a CSP provides an online software development platform for an organization. It comprises the environment for developing and provisioning cloud applications. Cloud platform tend to represent a compromise between complexity and flexibility that allows applications to be implemented quickly and loaded in the cloud without much configuration.

3. Infrastructure as a service (IaaS)- This model is used to access essential IT resources. These essential IT resources include services that are linked to resources of computing, data storage and the communications channel. It is a delivery model where CSP provide the necessary hardware and software upon which a customer can build a customized computing environment. This service model, manages an applications, data operating system, middleware and runtime. The service provider manages the virtualization, servers, networking and storage.



Service Model	Who Uses It	Available Services	Why Use It
SaaS	Members	Applications such as email, word processing and customer relation management tools	Complete business tasks typically performed locally on a computer
PaaS	Developers	Services to facilitate communication and monitoring	To run a cloud application for a particular platform
IaaS	IT Managers	Computing resources, data storage resources, and the communications channel.	Build a customized computing environment

Table 1: Cloud computing service models geared for different purpose

2. CLOUD DEPLOYMENT MODEL

Depending on the organizational structure, the provisional location and also based on their specific business, operational, and technical requirements the cloud services can be deployed in different ways. Mainly there are four primary cloud deployment models they are:
1. Public Cloud
2. Private Cloud
3. Community Cloud
4. Hybrid Cloud

1. Public Cloud -The public cloud deployment model represents true cloud hosting. In this model services are rendered over a network that is open for public use. Here service can be provided by a vendor free of charge or on the basis of a pay-per-user license policy. In this model cloud infrastructure is available to the general public and is owned by a third party cloud service provider (CSP). This model is best suited for business requirements, utilize interim infrastructure for developing and testing applications. It reduces capital expenditure and brings down operational IT costs

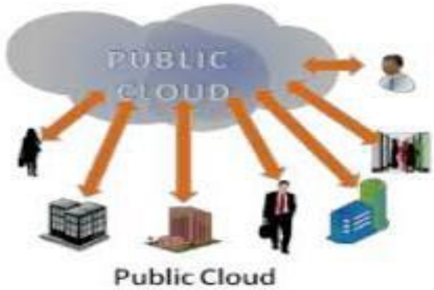


Fig 2: Public Cloud Deployment Model

2. Private Cloud- A private cloud deployment model is owned by a single organization. In this model cloud infrastructure operated solely for a single organization, managed internally or by a third-party, and is hosted either internally or externally. Private cloud makes use of virtualization solutions and focus on consolidating distributed IT services often within data centers belonging to the company. In this model the enterprise retains full control over corporate data, security guidelines and system performance.

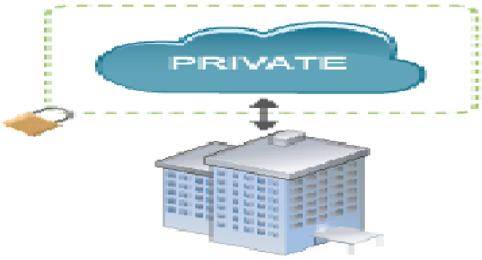


Fig 3: Private Cloud Deployment Model

3. Community Cloud- In this model organizations with similar requirements share a cloud infrastructure. In this model cloud infrastructure is procured jointly by several agencies or programs that share specific needs such as security,compliance, or jurisdiction. It is a generalization of a private cloud, as private cloud is being accessible by one certain organization. The CSP manage community cloud. This model helps to reduce costs as compared to a private cloud

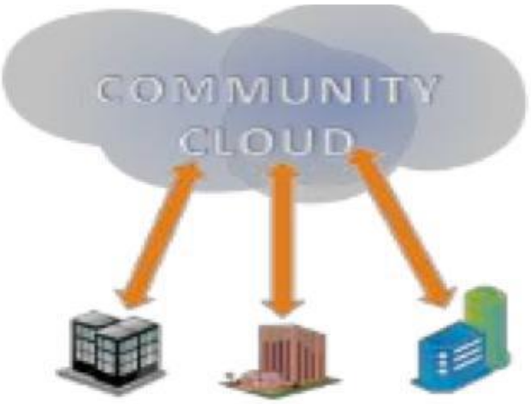


Fig 4: Community Cloud Deployment Model

4. Hybrid Cloud -Hybrid cloud is a composition of two or more clouds that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, manage dedicated services with cloud resources. Hybrid deployment models are complex and require careful planning to execute and manage especially when communication between two different cloud deployments is necessary.

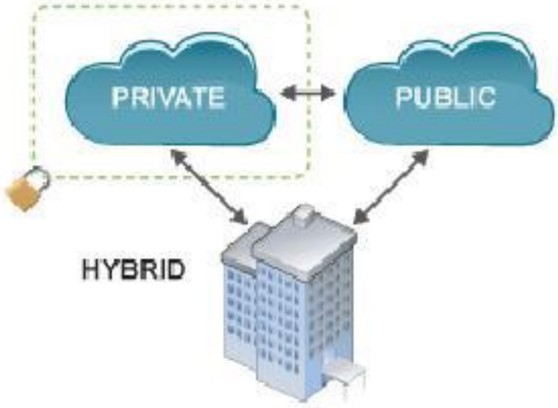


Fig 5: Hybrid Cloud Deployment Model

3. SECURITY AND PRIVACY CHALLENGES

In this section, we investigate the specific security and privacy challenges in cloud computing which require the development of advanced security technologies.

A. Loss of Control

In cloud computing, loss of control refers to the situation that cloud users' control over their data is diminished when they move the data from their own local servers to remote cloud servers. A great number of concerns about data protection are raised, since giving up direct control has to be one of the hardest things enterprises have to do [3].

1**). Data Loss and Data Breach-**Data loss and data breaches were recognized as the top threats in cloud computing environments in 2013 [4]. A recent survey shows that 63% of customers would be less likely to purchase a cloud service if the cloud vendor reported a material data breach involving the loss or thef to f sensitive or confidential personal information [5].Whether a CSP can securely maintain customers' data has become the major concern of cloud users. The frequent outages occurring on reputable CSPs [6], including Amazon, Drop box, Microsoft, Google Drive, etc., further exacerbate such concerns.

2). **Data Storage and Transmission under Multiple Regional Regulations-**

Due to the distributed infrastructure of the cloud, cloud users' data may be stored on data centers geographically located in multiple legal jurisdictions, leading to cloud users' concerns about the legal reach of local regulations on data stored out of region [7]. Furthermore, the local laws may be violated since the dynamic nature of the cloud makes it extremely difficult to designate a specific server or device to be used for transponder data transmission [8].

B. Lack of Transparency

In the context of cloud computing security, transparency refers to the willingness of a CSP to disclose various details on its security readiness. Some of these relevant details include policies on security, privacy, service level, etc. [9]. In addition to the willingness, when measuring transparency, it is important to observe how accessible the security readiness data and information are. No matter how much security facts about an organization are available, if they are not presented in an organized and easily understandable manner for CSUs and auditors, the transparency of the organization should still be rated relatively low. CSUs and auditors need to know the types of security controls put in place by CSPs for their cloud infrastructure, but CSPs are often not willing to share this information.

This is partially due to the fact that some of this information can be considered to consist of trade secret.

For example, a lot of technical knowhow is involved in effectively storing and securing customer data, and it takes significant time and resources to reach the acceptable level of technical sophistication. Therefore, CSUs and CSPs should negotiate on the information to be shared. Depending on the negotiation results, CSUs may decide not to use the services provided by the CSP. In fact, many CSUs choose not to use CSPs because of the frustration associated with this negotiation process and the resulting lack of transparency. For cloud computing to be more widely used, this challenge of transparency is one of the biggest obstacles to be removed.

C. **Virtualization Issues Related**

Virtualization refers to the logical abstraction of computing resources from physical constraints. One representative example of virtualization technology is the virtual machine (VM). Virtualization can also be performed on many other computing resources, such as operating systems, networks, memory, and storage. In a virtualized environment, computing resources can be dynamically created, expanded, shrunk or moved according to users' demand, which greatly improves agility and flexibility, reduces costs and enhances business values for cloud computing . In spite of its substantial benefits, this technology also introduces security and privacy risks in the cloud computing environment.

D. Multi-Tenancy Related Issues

Multi-tenancy is defined as "the practice of placing multiple tenants on the same physical hardware to reduce costs to the user by leveraging economies of scale". It indicates sharing of computational resources, storage, services and applications with other tenants, hosted by the same physical or logical platform at the provider's premises.

While the multi-tenancy architecture allows CSPs to maximize the organizational efficiency and significantly reduce a CSU's computing expenses, it does not come without costs. Adversaries taking advantage of the co-residency opportunities may launch diverse attacks against their co-residents, resulting in a number of security/ privacy challenges.

Specifically, in the multi-tenant environment, different tenants' security controls are heterogeneous. The tenant with less security controls or misconfigurations is easier to compromise, which may serve as a stepping stone to the more secured tenants located in the same host. This could reduce the overall security level for all the tenants to that of the least secured one. Furthermore, the security policies made by different tenants may disagree or even conflict with one another. Such disagreements or conflicts could introduce threats to tenants' needs, interests or concerns.

Furthermore, attackers taking advantage of the multitenancy architecture may be able to launch diverse attacks against their co-tenants, such as inferring confidential information or degrading co-tenants' performance.

4.RELATED WORK

Subashini et al proposed a metadata based data segregation and storage methodology, concerns with the security of the data that stored in the cloud computing data centers. The model fragments the data in a way such that the database contains invaluable data during residing in the storage location. The information gains its value only during acquisition or updating when those fragments of information are mapped.

There is no problem even if the data is accessed by an intruder since only the authenticated users and owners are allowable to view the information in a mapped manner. The fragmentation is done by Data Migration Environment (DME) based on the metadata that describes the database tables as normal or sensitive or critical according to the importance of the stored data. The input to DME should be the existing schema of the database and Metadata information.

The DME will fragment the data into pieces based on the level of data security. The table created by the DME will be the most sensitive data and will be stored either in a different server at the same geographical location or at a different geographical location. Additionally the DME will prepare a mapping table to reassemble the data during access or update. However, the fragmentation provides high security but it will cause a considerable overhead cost. This model is suitable for the database that is being designed from scratch and it is not effective for enterprises who want to move their existing data to the cloud.

C. P. Ram and G. Sreenivaasan proposed a mechanism to achieve security through encryption and decryption of user's data using cryptographic co-processor which is a trusted third party service. The cloud provider should ask the customer whether his data need to be segmented or not. Customer's data are divided into pieces of constant size called data chunks; the chunk size is based on the available bandwidth. After segmentation a header and a tail will be added to each data chunks and they will be distributed randomly in separate databases.

A log file that serves as an index to find chunks must be created and stored in a master database that can be accessed only by highly privileged user, since it is difficult for hackers to find the master database, they will not be able to find the data chunks. By this way, the security of user data will be enhanced .Michel et all proposed Secure Logical Isolation for Multi-tenancy (SLIM) model to provide security close to physical isolation by applying the principle of least privilege that is designed to be tenant _specific. This principle is implemented using mechanisms such as security gateway, proxy and gatekeeper to address this issue..

5. CONCLUSION

Cloud computing is a new paradigm of computing utilities that promises to provide more flexibility, less expense, and more efficiency in IT services to end users. Firstly this paper presents an introduction to cloud computing and discusses about characteristics of a cloud computing. Secondly focused on the different types of service models such (SaaS, PaaS, IaaS) used for specific application. Thirdly this paper presents how the cloud services can be deployed. Lastly about some of the key challenges of cloud computing.

REFERENCES

1. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011; http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf.
2. P. Viswanathan, "Cloud computing – Is it really all that beneficial?"http://mobiledevices.about.com/od/additionalresources a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm
3. D. Sheppard, "Is loss of control the biggest hurdle to cloud computing?" 2014; http://www.itworldcanada.com/blog/isloss- of-control-the-biggest-hurdle-to-cloud-computing/95131.
4. Top Threats Working Group, "The notorious nine: cloud computing top threats in 2013," 2013; https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
5. Independently Conducted by Ponemon Institute LLC, "Achieving Data Privacy in the Cloud," 2012; http://download.microsoft.com/download/F/7/6/F76BCFD7-2E42-4BFBBD20-A6A1F889435C/Microsoft Ponemon Cloud Privacy Study Germany.pdf.
6. J. R. Raphael, "The worst cloud outages of 2013 (so far)," 2013; http://www.infoworld.com/article/2606768/cloud computing/ 107783-The-worst-cloud-outages-of-2013-so-far.html.
7. A. Murphy, "Storing data in the cloud raises compliance challenges," 2012; http://www.forbes.com/sites/ciocentral/2012/ 01/19/storing-data-in-the-cloud-raises-compliance-challenges/.
8. S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proceedings of 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom), Indianapolis, IN, 2010, pp.693-702.
9 W. Pauley, "Cloud provider transparency: an empirical evaluation," IEEE Security & Privacy, vol. 8, no. 6, pp. 32-39, 2010.