A.Logeshwari *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 2, February- 2018, pg. 82-89 **ISSN: 2321-8363**
Impact Factor: 5.515

DATA SECURITY, PRIVACY, AVAILABILITY AND INTEGRITY IN CLOUD COMPUTING: ISSUES AND SOLUTION

A.Logeshwari[1], M.Aiswariya[2], V. Swathi[3], K.Vivekavarthini[4]
[1]Assistant Professor, Department of IT, logeshwaria@skasc.ac.in
[2]Student, aswariyaa@skasc.ac.in, [3]Student, swathiv@skasc.ac.in, [4]Student, vivekavarthinik@skasc.ac.in,
Sri Krishna Arts and Science College, Coimbatore

Abstract: Cloud computing changed the world around us. It is well known that cloud computing has many advantages and many enterprise applications and data are migrating to public or hybrid cloud. Therefore, storing the data on the cloud becomes a norm. However, there are many issues that countered data stored in the cloud starting form virtual machine which is the mean to share resources in cloud and ending on cloud storage itself. In this paper, we present about data security and privacy protection issues in cloud computing, and those issues that prevent the people from adopting the cloud and give the solutions that have been done to reduce the risks and issues. The data stored in the cloud need to be confidential, preserving integrity and available. And moreover, sharing the data that are stored in cloud among many users is still an issue since the cloud service provider is untrustworthy to manage authentication and authorization. In this paper, we list some issues and solutions for the issues related to data in cloud storage. And the research work about the data security and privacy protection issues in cloud.

Keywords: cloud- computing, virtual machine, data security, privacy protection, confidential data, authentication, cloud storage and cloud service provider (CSP).

1. Introduction

Data security means protecting data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users such as a cyber attack or a data breach.

Cloud computing is now everywhere. in many cases, users are using the cloud without knowing they are using it. According to [1], small and medium organisations will move to cloud computing because it will support fast access to their applications and reduce the cost of infrastructure. Cloud service providers (CSP) offer cloud platforms for their customers to use and create their web services, much like internet service providers offers customers high broadband to access the internet however, security and privacy protection is a critical concern in the development and adoption of cloud computing.

Regarding definition of cloud computing model, the most widely used one is made by NIST as, “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

promotes availability and is composed of five essential characteristics, three service models, and four development models". [2]

1.1 Characteristic of Cloud Computing:

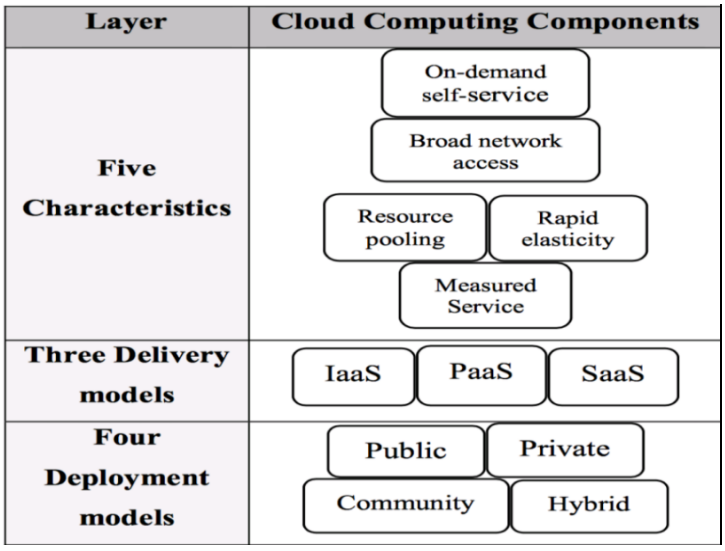

Fig.1: Block diagram of cloud environment architecture

1.2 The five characteristics in cloud computing are,

1. ***On-demand self-service:*** Where a consumer of services is provided the needed resources without human intervention and interaction with cloud provider.

2. ***Broad network access:*** Which means resources can be accessed from anywhere through a standard mechanism by thin or thick client platforms such mobile phone, laptop, and desktop computer.

3. ***Resource pooling:*** Which means the resources are pooled in order for multi-tenants to share the resources. In a multi-tenant model, resources are assigned dynamically to a consumer and after the consumer finishes it, it can be assigned to another one to respond to high resource demand.

4. ***Rapid elasticity****:* It is one of the cloud computing characteristics, which means that resources are dynamically increased when needed and decreased when there is no need.

5. ***Measured service:*** Also, one of the characteristics that a consumer needs is measured service in ordered to know how much is consumed. And also, it is needed by cloud provider how much the consumer has used in order to bill him or her.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

2. Service Models:

There are three models. According to [4], those models differ in the capabilities that are offered to the consumer. It can be software, platform, or infrastructure. In figure 2, it is comparison between those models with traditional model.

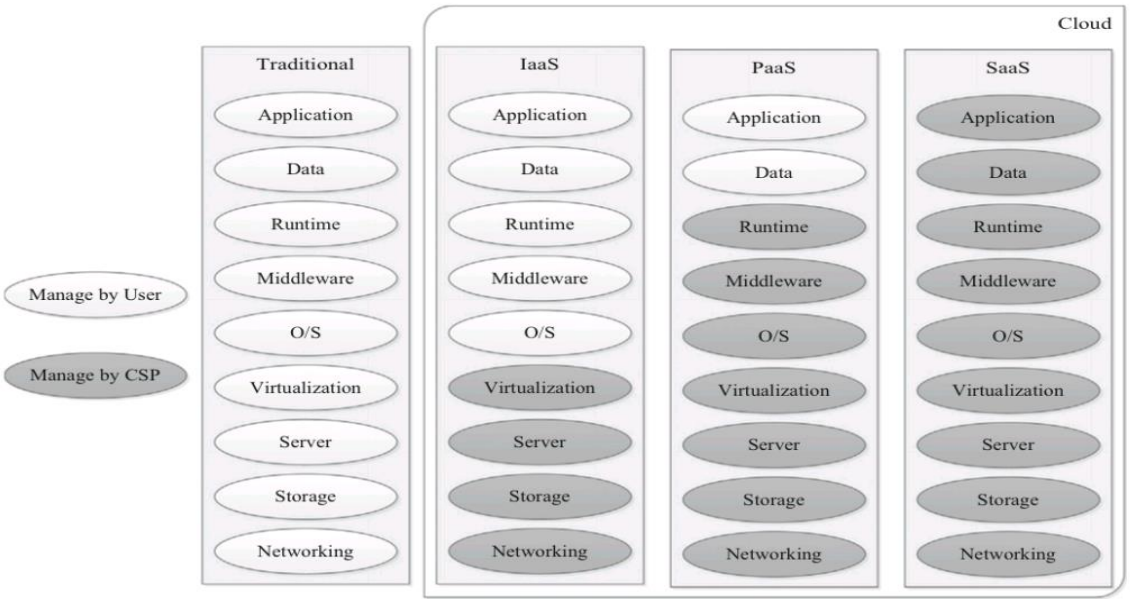

Fig.2: Service oriented cloud computing architecture

2.1. ***Software as a server (SaaS):*** In this service the cloud service provider provides software and the cloud infrastructure to the clients so they can use this software on the cloud infrastructure for their applications. since the clients can run the software and use it, they do not have the control over the physical settings such as network, operating system etc. only the cloud service provider is responsible for controlling the physical settings without client intervention. The client can access this software as a thin client through a web browser.

2.2. ***Platform as a service (PaaS):*** This service is similar to *SaaS* in that the infrastructure is controlled by the cloud service provider but it is different in that, in this the users can deploy and install their customized applications by using the tool offered by cloud service provider.

2.3. ***Infrastructure as a service(IaaS):*** Cloud services such as Amazon EC2 are adopting this model and charging their clients according to the resources are being utilized. In this service, computing resources such as storage, networks, and processing can be provisioned. The client of IaaS can install, deploy their applications and use any arbitrary operating system.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

3. Deployment Models:

There are four deployment models mentioned in as following: and they have been discussed in the literature [6], [7], [8].

3.1. ***Private cloud***: In this, the cloud provider provides cloud infrastructure to a single organization that has many consumers, that shares mission, security requirements, compliance consideration or policy. This infrastructure is used exclusively for their uses and needs. The manager, owner, and operator of this cloud can be the organization, third party, or the organization and third party together. This private cloud could be on or off premises.

3.2. ***Community cloud:*** In this model, the cloud provider provides cloud infrastructure to many organizations that forms a community, that shares mission, security requirements, compliance consideration or policy. This infrastructure is used exclusively for their uses and needs. The manager, owner, and operator of this cloud can be the organization, third party, or the organization and third party together. This community cloud could be on or off premises.

3.3. ***Public cloud:*** This model differs from the previous model in that it is open for the public, it is not private and not exclusive for the community. In this model, a public cloud can be used for public to satisfy their needs. The owner, manager, and operator of this cloud could be a government, private organization, a business or academic organization, and sometimes many of them can be in one cloud and get the service from the same provider.

3.4. ***Hybrid cloud***: A cloud can be considered hybrid if the data moves from a data center to a private or public cloud or vice versa. This model comprises of two or more deployment models (private, community or public). The cloud infrastructure can be combination of those models. These models are combined in order and to get the services and data from both in order to create a well- managed and unified computing environment.

4. Top Threats to Cloud Computing:

Cloud computing facing a lot of issues. Those issues are listed as a following: Data loss, data breaches, account or service traffic hijacking, insecure APIs, data ownership, data location.

4.1. ***Data loss*****:** Data loss may arise when disk drive dies without owner of data had not created backup, there are many possibilities of losing data due to a malicious attack and sometimes due to server crashes or an unintentional by the owner. It may also happen were encrypted data is used by some other unauthorized users.

4.2. ***Data breaches***: A cloud environment has many users. Any breach to this cloud environment will expose all the users and the information to be unclosed. The users of cloud may also require some confidential information like credit card information. When normal processing it may be possible that some unauthorized users may theft the confidential information and they can misuse it. Therefore, there is a data breach in cloud computing.

4.3. ***Account or service traffic hijacking***: Account hijacking is a common factor in a cloud. There a many service on internet but for using the user need to create an account and then they can start using the services. Sometimes due to trafficking and buffer, overflow may take place. This all risks may lead to loss of control over their account.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

4.4. *Insecure APIs:* The API (application programming interface) that defines how third party connects an application to the service and providing verification that the third party is producing. It is necessary to overcome these all kinds of risk. And it is require to use the security control that helps to overcome data loss and protects sensitive information, data breach and trafficking.

There are complex data security challenges in the cloud:

- Cloud service models with multiple tenants sharing the same infrastructure.
- The need to protect the confidential government, business, or regulatory data, accounts, reports, and compliance concerns.
- Data mobility and legal issues relative to government rules.
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security and risk management.
- A new type of insider who does not even work for your company, but may have control and visibility into your data.

There are some effective cloud security solutions and that incorporate three keys

- Data lockdown
- Access policies
- Security intelligence

5. Identity and Access Management:

In today's cloud computing world it becomes very complicate to protect data from unauthorized. Identity management focus on who is owner of data which provides that particular information is of this particular owner. Identity mainly focuses on privacy of user information. Whereas access management mainly focus on accessibility of information .Access Management concern about who have the permission to access data. Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern. One recurring issue is that the organizational identification and authentication framework may not naturally extend into the cloud and extending or changing the existing framework to support cloud services may be difficult [Cho09]. The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Mark up Language (SAML) standard or the Open ID standard.

- **Authentication:**

  A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the extensible Mark up Language (XML) for its format. SOAP messages are digitally signed. For example, once a user has established a public key certificate for a public cloud, the private key can be used to sign SOAP requests. SOAP message security validation is complicated and must be carried out carefully to prevent attacks. For example, XML wrapping attacks have been successfully demonstrated against a public IaaS cloud [Gaj09, Gru09]. XML wrapping involves manipulation of SOAP messages. A new element (i.e., the wrapper) is introduced into the SOAP Security header; the original message body is then moved under the wrapper and replaced by a bogus body containing an operation defined by the attacker.

- **Access Control:**

  SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud subscriber privileges and maintain control over access to resources is also needed. As part of identity management, standards like the extensible Access Control Mark up Language (XACML) can be used by a cloud provider to control access to cloud resources, instead of using a proprietary interface. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML's focus on the means for transferring authentication and authorization decisions between cooperating entities. XACML is capable of controlling the proprietary service interfaces of most providers, and some cloud providers already have it in place. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification.

6. Current Security Solutions for Data Security and Privacy Protection:

There is Decentralized Information Flow Control (DIFC) and differential privacy protection technology into data generation and calculation stages in cloud and put forth a privacy protection system called airavat [9]. This system can prevent privacy leakage without authorization in Map-Reduce computing process. A key problem for data encryption solutions is key management. On the one hand, the users have not enough expertise to manage their keys. On the other hand, the cloud service providers need to maintain a large number of user keys. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) is trying to solve such issues [10].

About data integrity verification, because of data communication, transfer fees and time cost, the users cannot first download data to verify its correctness and then upload the data. And as the data is dynamic in cloud storage, traditional data integrity solutions are no longer suitable. NEC Lab's provable data integrity (PDI) solution can support public data integrity verification. Cong Wang proposed a mathematical way to verify the integrity of the data dynamically stored in the cloud. In the data storage and use stages, Mowbray proposed a client-based privacy management tool. It provides a user centric trust model to help users to control the storage and use of their sensitive information in the cloud.

Munts Mulero discussed the problems that existing privacy protection technologies (such as K anonymous, Graph Anonymization, and data pre-processing methods) faced when applied to large data and analyzed current solutions [11].

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

The challenge of data privacy is sharing data while protecting personal privacy information. There are some proposed a privacy protection framework based on information accountability (IA) components. The IA agent can identify the users who are accessing information and the types of information they use. When inappropriate misuse is detected, the agent defines a set of methods to hold the users accountable for misuse. To protect the data from unauthorized person we can protect the data by making simulator which ask the sender for password when sender saves the information and when it received by receiver and when receiver opens the file at that time simulator ask receiver for password which is created by sender. This password is personal between both parties that is sender and receiver.

7. Conclusion:

Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. According to the analysis for data security and privacy protection issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defence in depth. Regarding privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of cloud-based applications.

References:

[1] s. Subashini and v. Kavitha, "a survey on security issues in service delivery models of cloud computing", journal of network and computer applications, vol 34, no. 1, pp.1-11,2011.

[2] Sun cloud architecture introduction white paper (in Chinese).
http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[3] M. ALZain, E. pardede, B. soh, and J. Thom, "cloud computing security: from single to multi-clouds," in system science (*HICSS),* 2012 45th*Hawaii international conference on,* JAN 2012, pp. 5490-5499] .

[4] Mell and T. Grance, "The nist definition of cloud computing," 2011.jan 2012, pp. 5490-5499.

[5] M. sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," *journal of network and computer applications,* vol. 43, pp. 121-141, 2014.

[6] E. Aguiar, Y. Zhang, and M.Blanton, "an overview of issues and recent developments in cloud computing and storage security," in *High performance cloud auditing and applications.* Springer, 2014, pp.3-33.

[7] I. Gul, M. Islam et al., "cloud computing security auditing," in *next generation information technology (ICNIT),* 2011 *The second international conference on.* IEEE, 2012, pp. 143-148.

©2018, IJCSMA All Rights Reserved, www.ijcsma.com

[8] E. M. Mohamed, H. S. Abdelkader, and S. El-etriby, "Enhanced data security model for cloud computing," in *Informatics and systems (INFOS)*, 2012 8th international conference on. IEEE, 2012, pp. cc-12.

[9] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E. "Airavat: Security and privacy for MapReduce," In: Castro M, eds. Proc. of the 7th Usenix Symp. on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010. 297.312.

[10] "OASIS Key Management Interoperability Protocol (KMIP) TC",

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip.

[11] Muntés-Mulero V, Nin J. Privacy and anonymization for very large datasets. In: Chen P, ed. Proc of the ACM 18th Int'l Conf. on Information and Knowledge Management, CIKM 2009. New York: Association for Computing Machinery, 2009. 2117.2118. [doi: 10.1145/1645953.1646333]

A Brief Author Biography

1st Author Name – A.Logeshwari MCA, M.Phil, Assistant Professor, Specialization in Computer Networks

2nd Author Name – M.Aiswariya, Student, I B.SC(IT)

3rd Author Name- V.Swathi, Student, I B.Sc(IT)

4th Author Name-K.Vivekavarthini, Student, I B.Sc(IT)

©2018, IJCSMA All Rights Reserved, www.ijcsma.com