Analysis on Cloud Computing Security Issues, Threats and Solutions

K.B. Priya Iyer, Ph.D.
Associate Professor,
Department of Computer Science
M.O.P. Vaishnav College for Women
(Autonomous),
Chennai, India

Padma Priya, R. Anusha
B.C.A - Undergraduate Students
M.O.P. Vaishnav College for Women
(Autonomous)
Chennai, India

ABSTRACT
Cloud computing is becoming very popular computing standard for network application. It is the result of existing technologies and paradigms. It is a set of resources and services offered to customers through network or internet. It provides resources that are provided as on request services to end user. It mainly aims at reduced cost, less complexity, flexibility, scalability and efficiency. Cloud computing extends various techniques such as grid computing, distributed computing and utility computing [1]. Cloud computing is used in both industrial and academic field. The data storage as a service (DAAS) in cloud provides the user a facility to store their data in remote servers which may be accessible by the user anywhere he is through the internet facility [3]. The data stored in cloud can also be accessed by other users. There is also a possibility where a hacker can pierce the cloud by stealing a genuine user's data. He is also capable of infecting the cloud which in turn affects the entire user's who are sharing the infected cloud. Here comes the problem of providing security to the cloud. Likewise both customer and service provider face few security threats [2].

Data communication through any network is at risk now, there are many encryption techniques used to protect the data. This paper discusses about security issues faced by client and server and also have analyzed about threats involved in different service models such as infrastructure as a service (IAAS), software as a service (SAAS) and platform as a service (PAAS). We have also tried to provide few countermeasures for those security issues

Keywords
Cloud computing, Encryption, data security, security issues, threats.

1. INTRODUCTION
Cloud computing provides online access to computer resources through centralized data storage. Huge group of remote servers are networked together to platform and resources as a service. It is based on sharing of resources to achieve coherence and economies of scale, similar to a utility over network. It describes a type of outsourcing of computer services [1]. The user can simply use store data, compute any operation, or use any special technique, without having to worry how these works internally. They just need to pay for what they used [4]. It is also popular in today's organization because it provides flexibility, scalability and availability of data. Organizations pile up their data in the cloud. So, that all the share holders can view the document with complete access rights.

Many developers of cloud are even now not able to give a high end security to the cloud environment [5]. Resources of the cloud can be used by the client and deployed by the vendors such as Google, Amazon, IBM, Microsoft etc. It is of great use to many IT industries as it provides so many tools and software's required for them on-demand and they need not buy it rather they use it as and when required. Because of the interaction between the clouds components they are able to give the answer for the clients request at a faster rate. The cloud architecture basically concentrates on two things frontend and the back end. Frontend is the client who gives request to the back end and the back end is where the actual cloud server is present [4]. The main aim of the paper is to analyze different security issues based on user & provider level, service level etc... And to analyze different techniques proposed to handle security threats.

1.1 Cloud Architecture
Four deployment models used in cloud architecture are

- **Private cloud:** The cloud infrastructure is made available for only private organization. It may be organized by the organization or a third party and may exist on premise or off premise [3].
- **Public cloud:** The cloud infrastructure is accessible to general public or large industry group. It is owned and managed by organizations that provide cloud services.
- **Community cloud:** The cloud infrastructure is operated by several organizations and supports a specific community that has a communal concern (e.g. mission, security requirements etc…).
- **Hybrid cloud:** This is a combination of any two clouds (Private, Public and community). It contains unique entities but bound together by standardization or proprietary technology.

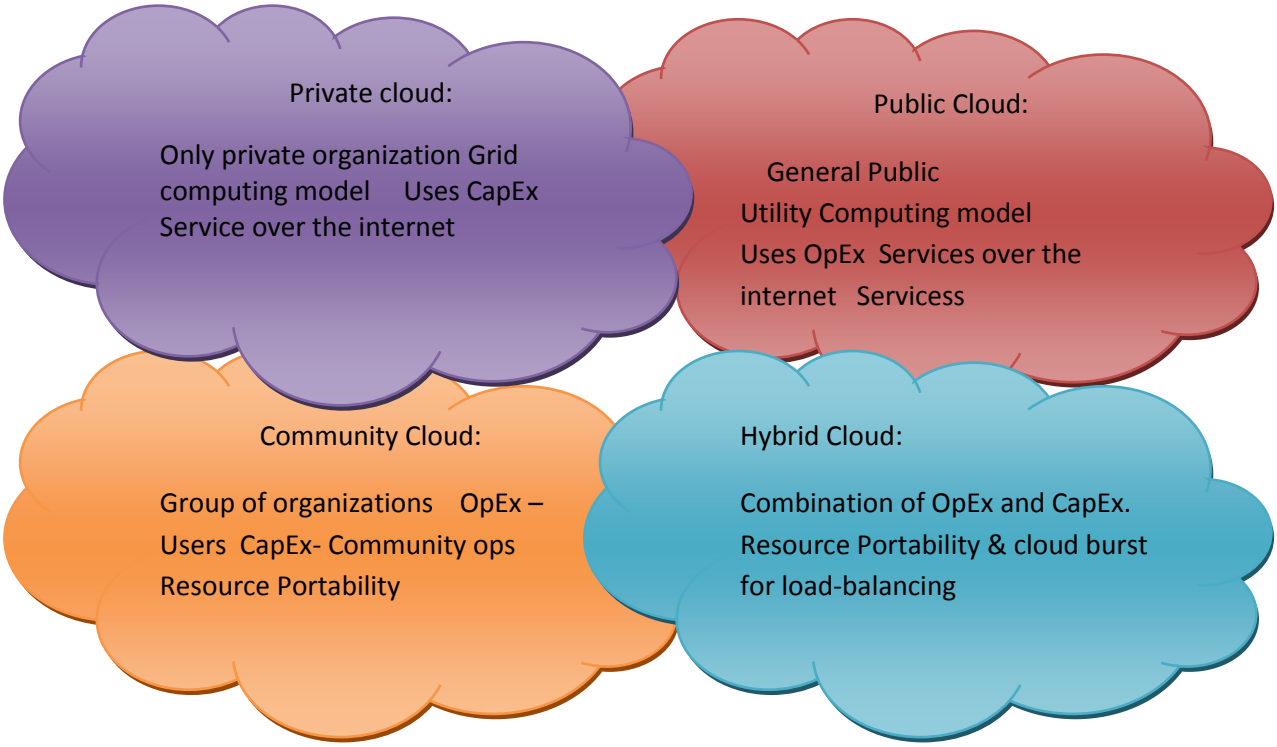


Fig1.Deployment models used in cloud architecture

1.2 Layers of Cloud Computing

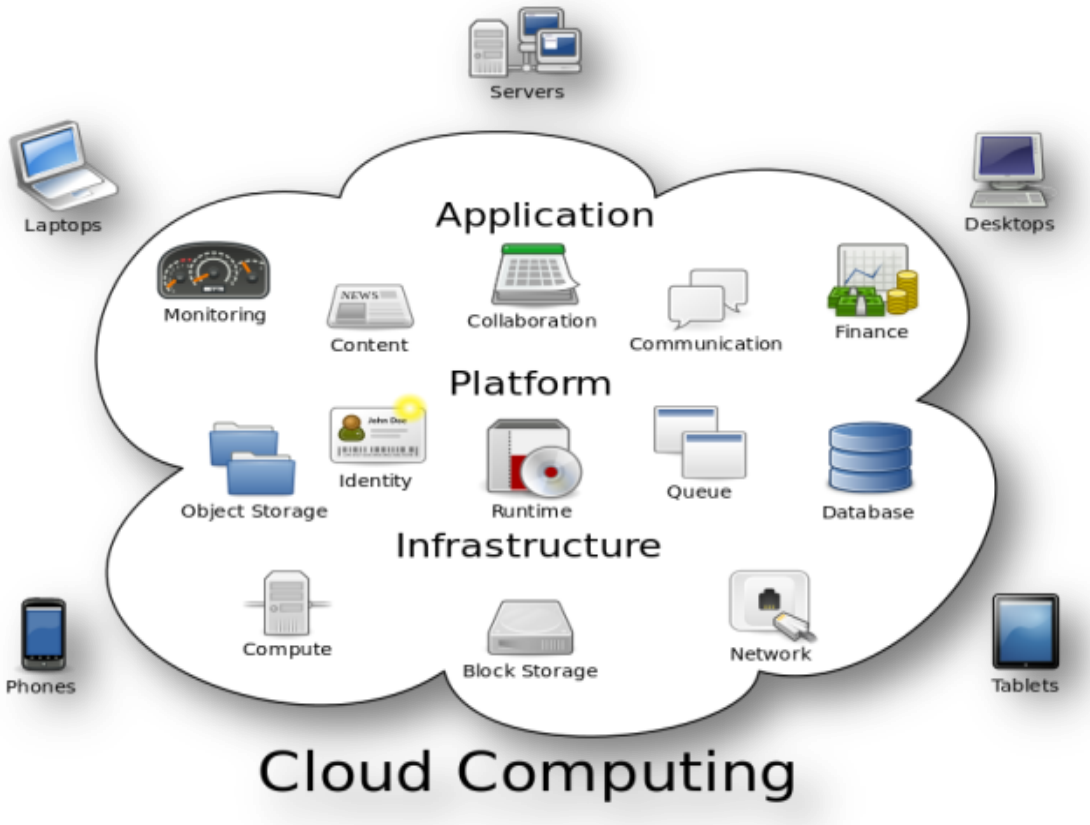
Cloud computing are divided into different layers which are known as [7]:

Hardware as a service (HAAS)

Infrastructure as a service (IAAS)

Platform as a service (PAAS).

Software as a service (SAAS).



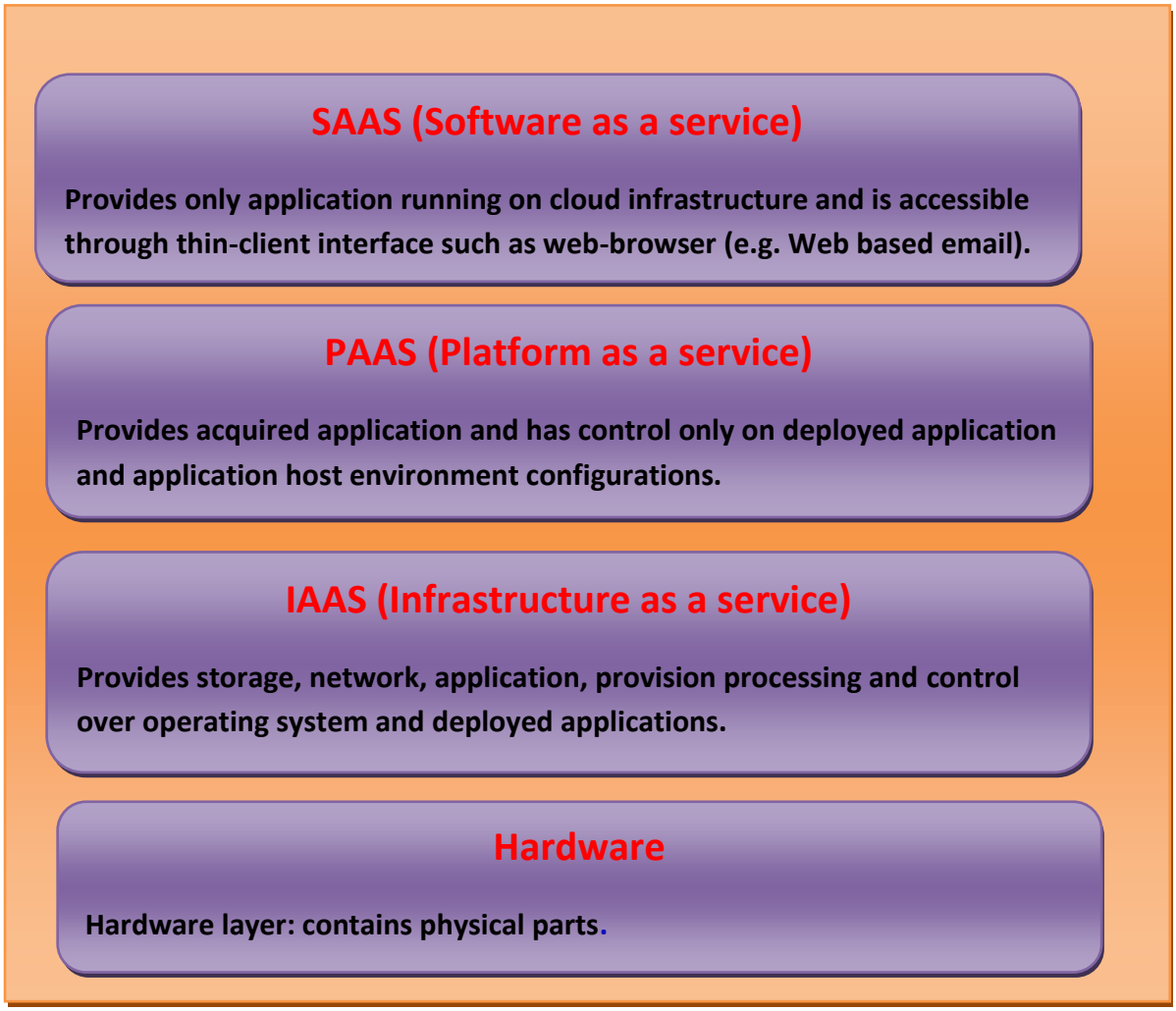


Fig2.Layers of cloud computing

2. RELATED WORKS

This section contains the reviews of various cloud security issues faced by cloud service provider and user and the solutions given by different authors.

In [1] [10], Authors have described the various issues faces in cloud computing and also have described about the threats prevailing in a cloud environment. They have also suggested few countermeasures for the same and have believed in trust management factor to achieve security on the whole.

In [2] [4], Authors have done analysis on threats in cloud computing and the various components of cloud in detail. The authors have mainly believed in cloud security standardization.

In [5], Anjana chaudhary, Ravinderthakur and manishmann have proposed methods for data storage and security in cloud computing using encryption techniques.

In [7], Navdeep singh, abhinavhans, ashish Sharma and Kapilkumar conveys the readers about the various cloud securities issues prevailing in different models.

In [6][3], Authors have introduced a new concept called trusted third party management and also have proposed two methods called SSO and LDAP to provide security to the cloud.

In [9] [8], Authors have proposed various security algorithms to solve the cloud security issues and attacks.

3. SECURITY ISSUES FACED BY CLOUD SERVICE PROVIDERS

3.1 IAAS

Infrastructure as a service outsources equipments such as network, storage, hardware and applications. Characteristics of IAAS are policy based services, desktop virtualization, utility computing services and internet connectivity [7]. It deals with VM ware and the major problem faced by IAAS is because of the VM ware which leads to the delay in the delivery of packets to the upper levels. The issue basically slows down the system and the countermeasure for this is done using security management technique [7].

3.2 PAAS

Platform as a service provides service on application and allows customer to configure on them. In PAAS distribution development team works for the same project. It provides virtualized servers and operating systems features can be upgraded frequently. Major security problem faced by PAAS is that data is accessible between two applications. The impact that it creates is code gets interchanged during compilation. Many authors have suggested that blocking of visibility of code is the best solution for this problem [7].

3.3 SAAS

Software as a service allows users to access only on the application which they try to utilize using the cloud infrastructure [7]. They access through thin client interface such as web browsers. It provides automatic updates and patch management global accessibility and compatibility. Because of global accessibility data is lost and if a particular user requests a file which is being used by another user. And the request of the user is denied. The data that is stored is very sensitive because of the outside the boundary of enterprise. The proposed solution for theft of data is encryption technique.

Table1.Analysis on the issues faced by cloud service providers

Model	Characteristics	Issues	Impact
IAAS	1.Policy based services 2.desktop utilization	Problem in VM may lead to delay in delivery of packets to the upper level	System slows down
PAAS	1.virtualized servers 2.OS features can be upgraded	Data is accessible between two applications	Codes may get interchanged
SAAS	1.Automatic upgrades and patch management 2.Global accessibility	Data is very sensitive because of being stores in outside the boundary of enterprise	Theft of data may occur

4. SECURITY ISSUES FACED BY THE CLIENTS

4.1 Confidentiality

Securing user data in the cloud system is known as confidentiality. Cloud is basically a public network where in the data of other users can be seen [5]. Hence, a major attention has to be paid to make the clients data confidential.

4.2 Data loss

Data loss may occur due to lack of backup, unauthorized access or due to loss of encryption key. It is a major issue for business organization because they mainly depend on their data and if it is lost, it creates a financial crisis to the organization [4]. Cloud does not provide any facility to keep a copy of a data. So, if the user deletes or updates the data, the data is lost entirely.

4.3 Availability

Availability is a major concern in cloud environment because resources that are requested by the clients have to available all the time. Hardening and redundancy are two major strategies used to improve the availability of resources as redundancy increases cloud service provides offers geographical redundancy which in turn increases the availability of resources [5].

4.4 Privacy

Privacy is another aspect that every user of cloud wishes to have [5]. It basically discloses the personal information of the users. Privacy needs to be checked at every level while designing the cloud architecture.

4.5 Malicious attack

Malicious attacks are mostly done by hackers. There are two types involved in a malicious attack such as insider attack and outsider attack. Insider attack is done by the persons like third party vendor who has access to all data stored in a cloud [4]. This third party vendor can be a person who may steal those data and sells to other organization. Outsider attack is done by a hacker who works for an agency and so.

Table2.Analysis on issues and solutions for the problems faced by cloud users (1) Authentication and identity, (2) Data Encryption, (3) SLA, (4) Backing up of data

Issues	Techniques Used				Level
	(1)	(2)	(3)	(4)	
Confidentiality	√	√	X	√	Virtual level
Data Loss	X	X	X	√	Application level
Availability	X	X	√	X	Application level
Privacy	√	√	X	X	Application level
Malicious Attack	√	√	X	X	Physical level

5. TECHNIQUES USED TO SOLVE SECURITY ISSUES

5.1 Authentication and identity

Authentication is the access rights provided by user to view his data. The most common authentication technique used is cryptography [11]. This is a means of providing access rights through passwords and security tokens. Authentication solves man issues such as confidentiality issue, privacy risk and malicious attacks.

5.2 Data encryption

Encryption is a technique that is used to secure data, where in the normal plain data is converted into a non-readable form called as cipher-text [11]. An encryption key exists that is used to decrypt the encrypted message into normal text. Common encryption algorithms used are RSA, MDS and AES. It

solves confidentiality issues, privacy risk and malicious attack.

5.3 Service Level Agreement (SLA)

SLA is an agreement that exists between the user and the customer. It lets the user to know whether the resource is available to him at the time of usage or not [11]. It is a way to have a backup for local resources. It solves only the availability problem.

5.4 Backing up of data

This is one of the methods to provide data security in a cloud networks. It basically reduces data loss and if data is lost it can be recovered using back up files [11].

6. SECURITY THREATS IN CLOUD COMPUTING

6.1 Loss of governance

For a cloud user say an IT company giving their system to the cloud infrastructure is considered like giving control of their system to the cloud service provider [2]. Loss of governance is basically depends on the cloud service model that is used, that provides services to the cloud service user say for example like IAAS only delegates hardware and network to providers, wherein SAAS delegates OS and service integrity.

6.2 Loss of trust

Because of the black box feature of the cloud it becomes difficult for a cloud user to know exactly the trust level given by the provider's. There is no other means by which a user can get and share provider's security level. [2] Users have no ability to estimate the level that is being provided or achieved by the provider.

6.3 Data loss/leakage

Many issues like encryption key loss or privileged access code may bring a serious of problem [2]. Because of this lack of cryptographic management information it leads to great damages like data loss and leakage.

6.4 Shared environment

Because of virtualization feature of the cloud different users' share the same infrastructure in a cloud environment, due to this data integrity and confidentiality is affected very badly [2].

6.5 Protection inconsistency

Among distributed security modules protection inconsistency occurs because of clouds decentralized architecture [2]. This is because an access denied by one module is granted by the other. So this inconsistency helps the hackers to steal the data which affect the data confidentiality and integrity.

7. CONCLUSION

Cloud computing provides service on resource, hardware and application through networking infrastructure. It is one of the tremendous information technologies which have a large impact on financial management [6]. Though it provides many services and has several advantages, it also has some security issues faced by both cloud supplier and customers [5]. In this paper we have done analysis about different security issues faced by cloud providers and users. Some techniques and solutions to handle those issues are also analyzed [6]. A few general guidelines for the secured cloud computing environment are architecture ontology approach, well enhanced encryption algorithm, authentication of user, mirage image management system, using client based privacy manager, and Transparent Cloud Protection System (TCPS) [7]. Third party Trust management can also help to reduce the cloud computing security issues. Providing security algorithms is also one of the best ways to reduce cloud security issues. Our future work is to analyze on security algorithms that prevent cloud data loss and leakage.

8. REFERENCES

[1] VahidAshktorab, Syed Reza Taghizadeh(2012)," Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 1, Issue 2, October 2012.

[2] KangchanLee(2012)," Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[3] PradnyeshBhisikar, Prof. AmitSahu," Security in Data Storage and Transmission in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 3, March 2013.

[4] Prince Jain," Security Issues and their Solution in Cloud Computing", International Journal of Computing & Business Research.

[5] Anjanachaudry, Ravinderthakur, manishmann,"A Review: Data Security Approach in Cloud computing by using RSA Algorithm ",International Journal of Advance Research in Computer Science and Management Studies ,Volume 1, Issue 7, December 2013 .

[6] DimitriosZissis&Lekkas," Addressing cloud computing security issues,Future Generation Computer Systems.

[7] Navdeep Singh, Abhinav Hans, Ashish Sharma, and Kapil Kumar," A Review on Security Issues in Cloud Computing", International Journal of Innovation and Applied Studies, Vol. 8 No. 3 Sep. 2014.

[8] HarshalMahajan, Dr.NupurGiri," Threats to Cloud Computing Security", International Technological Conference-2014 (I-TechCON), Jan. 03 – 04, 2014.

[9] K.S.Suresh,Prof K.V.Prasad," Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 10, October 2012.

[10] Frederick R. Carlson," Security Analysis of Cloud Computing"

[11] Garima Gupta, P.R.Laxmi and Shubhanjali Sharma," A Survey on Cloud Security Issues and Techniques",