Indian Journal of Science and Technology, Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/92880, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# A Study of Security and Privacy Issues at Service Models of Cloud Computing

**Vaishali R. Thakare*** **and K. John Singh**

School of Information Technology and Engineering, VIT University, Vellore – 632014, Tamil Nadu, India;
vaishalir.thakare2014@vit.ac.in, johnsingh.k@vit.ac.in

## Abstract

**Objectives:** Presently, cloud computing is efficiently sharing data and resources over the internet. It is composed of five crucial characteristics such as On-Demand self-service, Resource Pooling, Broad network access, Rapid elasticity and Measured Service. With these characteristics cloud computing is introduced with some open issues like, Security, Availability, Scalability, and Interoperability. Traditional techniques cannot keep cloud computing secure fully. In cloud deployment and delivery models, mostly arrives the privacy and security issues. Hence, cloud computing security and its techniques are hot topic for researchers. **Methods:** To deal with the current security issues in IT market, industries are developing their architectural models with having strong level of security to their data center. **Findings:** In this paper, cloud security and privacy issues are analyzed and cloud deployment model security is explored. Moreover, service models of cloud computing are also described with its security issues. The observation from this study is to consider Audit as the important parameter in presenting security solution that covers maximum parameters of security, which are taken into consideration from literature. **Application/ Improvements:** This paper studied about the cloud security concerns and brings a new challenge to the cloud service provider and a parameter wise comparison of existing security solutions. Based on these comparison a new security model is proposed which describes user's security requirements.

**Keywords:** Cloud Computing Security, Cloud Technologies, Data Security Attacks, Deployment Models, Service Delivery Model

## 1. Introduction

Internet is a large collection of networks where all the types of resources are globally networked. With the help of it we can access the required services over the globe; the required information will be available to us in the minute of our fingertips. Keeping this in mind, the concept of cloud computing[1] is evolved; this implies fine access to remote computing services offered by third parties via a TCP/IP connection to the public internet[1]. In IT world the current fastest growing segment is cloud computing[2] and it is developing the business concepts along with the rate of growth of IT Industry. Cloud computing evolves from distribute ccomputing, grid computing, utility computing, P2P computing, virtualization[3] and server clusters shown in Figure 1. However, it will be a subversion technology, which represents the growth cycle of IT industry from hardware, software, and distributed services to software, services and centralized service respectively as shown in Figure 2. Primarily, Cloud computing focuses on web industry related applications. From the year 2008, cloud computing makes IT industry more exible in case of sharing IT resources (Software resources, hardware resources, operating system, etc.) Over the internet with the help of cloud service models, Cloud storage and Cloud providers (Microsoft Azure, Amazon EC2, Salesforce.com, Google App Engine (GAE), 3Tera, IBM Blue cloud, etc).

Cloud computing provides everything as a service such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). SaaS typically the web accessible via browser or program interface, incorporate the applications, which deployed over the network,: sometimes mentioned as on demand software. Examples: Facebook, Google Apps (email, calendar,

*Author for correspondence

documents), Salesforce.com, Twitter, etc. PaaS includes a platform on which users can build the application using services, libraries, languages and tools supported by the cloud provider. Examples:Force.com, Google App Engine, Red hat open shift, Windows Azure shown in Figure 3. A Study of Security and Privacy Issues at Service Models of Cloud Computing[4].

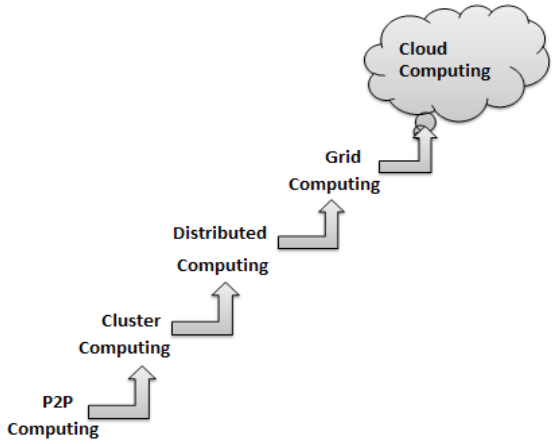


**Figure 1.** Origin of cloud computing.

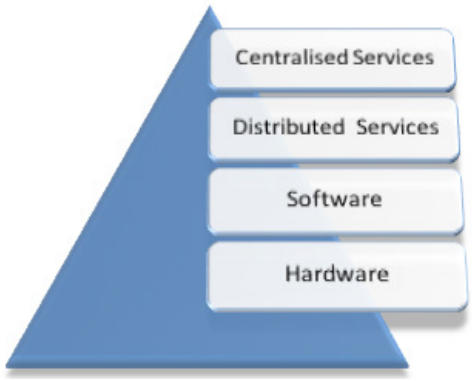


**Figure 2.** Growth cycle of IT.

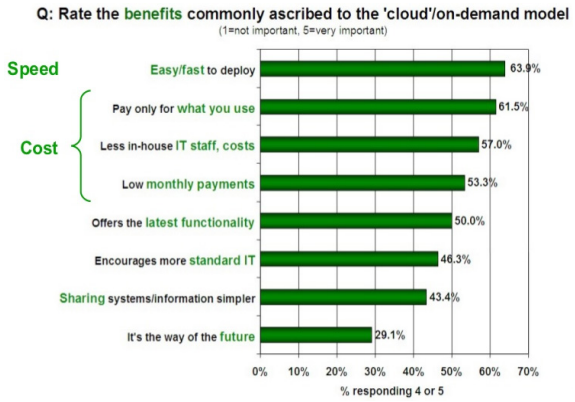


**Figure 3.** Benefits of cloud computing: IDC survey [IDC:2008].

The control of user over operating system and deployed applications where IaaS incorporate storage capacity, Network resources, Processing and computing resources, sometimes referred as utility computing. Examples: Amazon web services (EC2, S3, Dynamo DB, other), Go Grid, etc. Figure 3. Shows the rate of benefi`ts commonly ascribed to the `cloud'/ondemand model. IDC collected 244 respones after survey, amongst 244 respondent it has been asked to give ratings to the importance of cloud services varierty benefits to the businesses. The Figure 3 shows the respondents percentage ratings as follows, 1 shows least preference (not important) to 5 shows highest preference (very important). IDC survey says the topmost benefits of cloud computing is speed and ease of deployment. The other three benefits deal with improving the economics of industries Following is the definition of cloud computing by Cisco and National Institute of Standards and Technology (NIST) respectively:

"Cloud Computing is IT resources and services that are pre-occupied from the fundamental infrastructure and provided "on-demand" and "at scale" in an environment of multi-tenancy and, Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of congurable computing resources that can be rapidly provisioned and released with minimal management eort or service provider interaction[5]. IT industry can choose deployment model according to their requirement. It incorporates private, public, hybrid, and community cloud[6,7].

Private cloud works for a single organization. It offers a significant number of characteristics of open distributed computing including resource pooling, On-Demand self-service, flexibility and pay-as-use carried in standardized way with the extra control and customization accessible from dedicated resources. Private cloud has an exclusive infrastructure, and put inside the inner server of an organization, normally behind a firewall. In this way, the management and security requirements are much simpler to do. To manage the infrastructure[7] of private cloud big budgets and highly skilled IT technicians are needed. Examples: Microsoft ECI data center (Microsoft enrollment for core infrastructure), Ubuntu enterprise cloud-UEC (powered by Eucalyptus), Eucalyptus, Amazon VPC (Virtual Private Cloud), VMware cloud foundation suite. Public cloud is a most popular form of cloud and many times referred as multi-tenant resources are provisioned on a fine-grained, organization toward oneself premise over the web, by means of web admin-

istrations from an off-website third-party supplier who offers resources and bills on a fine-grained utility figuring premise. You pay for your utilization. A cloud supplier claims the framework behind an open cloud. The resources of cloud are found at an off-site area, which transforms this model into less secure and more vulnerable than other organization models, on the grounds that the administration service models can be subjected to malicious activities. It is accessible to overall public or large-scale group of industries; processed by associations offering services of cloud. Examples: Windows Azure services platform and Office 360, Amazon EC2, Google App Engine, IBM Blue Cloud. Community cloud denotes to environment of cloud computing managed by a few associations that have comparable necessities. It might be administered by the manager's board of trustees or third party association and may be put at on location or off-site area. The parts of the group cloud can freely get to the information in the cloud. The group cloud eliminates the security vulnerability and the expense of private cloud. Examples: Microsoft Government Community Cloud, Google Apps for Governments. Hybrid cloud is an environment where in an association gives and deals with a few resources inside and has others provide remotely. It is a combination of two or more cloud organization models. The combination of private and public cloud will brings the more advantages to overcome the obstacles in each of them. This model is overseen by both the organization and an entity of third party and is put in both on location and off-site areas. Examples: An association may utilizes services of public cloud, service for filed information yet keep on maintaining in-house storage for operational client information.

To analyze the advantages of customers, industry is offering the customer to have first look at available deployment[8] model. Mainly customer should concerns in terms of security as observed by interoperability of NIST amongst various clouds is still boundary that needs to succeed. The more expensive deployment model is a private cloud than other models but having more security. Public clouds are cheaper but less secure hence the research is going in this deployment model, comparison is shown in Table 1. Nowadays, to increase on-premise infrastructure of enterprises, they are moving towards an environment of cloud computing. However, most cannot bear the cost of the threats of compromising the security of their applications and information.

**Table 1.** Summary of main characteristic, and requirements of cloud deployment models

| Parameter Deployment Models | Infrastructure Owned by | Infrastructure Managed by | Infrastructure Located | Client base | Cost | Security |
|---|---|---|---|---|---|---|
| Public Cloud | Third Party | Third Party | Off-site | Large as well as SMEs | Low | Low |
| Private Cloud | Organization or Third Party | Organization or Third Party | On-site | Large Enterprises and corporations | High | High |
| Community Cloud | Third Party | Organization or Third Party | On-site | Small SMEs | High | High |
| Hybrid Cloud | Both | Both | Both | Multiple internal and/ or external providers | Medium | Medium(application compatibility issues) |

Figure 4 shows the taxonomy of this article, which shows concerns of cloud security covered. There are five major concerns on which this article is based upon, data security, network security, security concerns in service delivery model, deployment model and threats. Data security[7] is explored as data locality, data integrity, data segregation, data access, data confidentiality issues, data breaches, reliability of data storage, data center operation, and data sanitization. Network security contains, application vulnerabilities, host and network intrusion, DoS, Man-In-The-Middle, IP spoofing, port scanning, packet sniffing. Deployment model contains public, private, community and hybrid cloud. Service delivery model contains [6] SaaS, PaaS, IaaS.

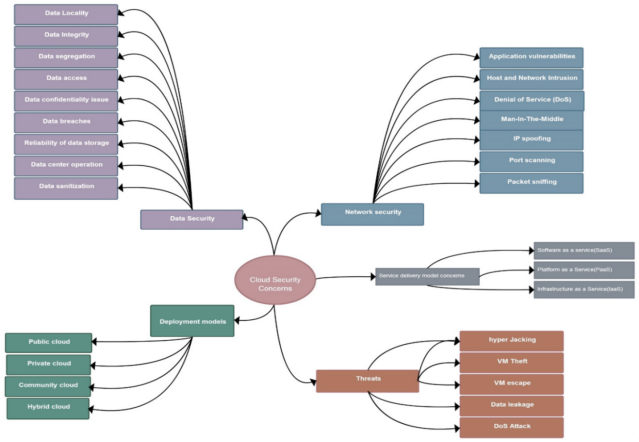


**Figure 4.** Illustration of taxonomy proposed in this paper, showing five major concerns and several sub values.

## 2. Related Work

The development of cloud computing begins approximately in 2008 with the new model of distributed computing and future computing system as a utility. Many researches are going on cloud security issues, industries like Microsoft, Cisco, Google, NIST, etc. are also concentrating the security issues of cloud computing.

In[3] authors evaluated scenarios of deployment models based on requirement of privacy and security. Authors have designed a framework that gives a language and a process to provision the cloud deployment models selection built on privacy requirement and security requirement of organizations and they have integrated secure Pris and Tropos to develop the privacy requirements and security requirements engineering method for the Cloud.

In[8] authors have described and proposed "secure cloud architecture design", and how these attacks e.g. DoS, Cloud injection Attack, wrapping Attack, browser-based attack implemented the security architecture are counteracted by proposed model. Architecture divided into four zones: Demilitarized zone, Internal Customer Zone, Management Zone, External Customer Zone.

In[9] proposed "Security as a Service Model for Cloud Environment". This model focused on a security benefits that a cloud supplier can offer as a component of its framework for clients to respond attacks. Primary assurance is to give the architecture of security that gives adaptable security as a service. Moreover, discusses how different sorts of attacks are counteracted by proposed building model.

In[10] authors elaborated a survey fundamental ideas concerning the security condition environment of cloud. They observed that enterprises are facing security issues in service delivery as well as in deployment models and they suggested solutions for the same.

In[10] authors explored design of security approaches in Infrastructure as a service model. To overcome the traditional security disadvantages they have given the different arrangement that intends to determine this testing issue. TCCP and TCG security outline that attempt to implement security by confirming the fingerprint of the hub Excalibur tries to utilize arrangements to distinguish trusted hubs.

In[11] authors stated the privacy protection and issues in data security. They said that the actual problem of cloud computing is privacy as well as security that need to be solved. According to deployment model, service delivery model, and vital features of cloud computing, issues in privacy protection and data security need to be solved soon as they are prime problems of security. They clarified that privacy as well as data security exists at all levels in SPI delivery models and information life cycle phases.

In[12] authors have given the dynamic security solutions in public cloud workflows. Established researchers is yet to characterize the security issues of deploying work process examples to an open cloud setting and expressive answers for guarantee sending is agreeable enterprise strategy and legitimate orders. They started to address this by highlighting the past data security issues being accomplished by enterprises at present utilizing open cloud base.

In[13] authors have described the cloud computing security issues and challenges. They highlighted the challenges

**Table 2.** Comparisons of various existing security model

| Survey | Year and publication | Topics Focused | Industry References | Security Issues | Solutions |
|---|---|---|---|---|---|
| M. Zhou and R. Zang | 2010 | Security Design in IaaS | × | _ | √ |
| Bhaskar Prasad Rimal et al | 2010 | Requirements of architecture of cloud computing system | × | | √ |
| John C., A. Moosel, P. Watson | 2011 | Issues of security for deploying workflow cases to public cloud model | × | √ | √ |
| Kuyoro S. O., ibikunle F. and Awodele O. | 2011 | Security challenges and issues of cloud computing. | × | √ | × |
| Subhashini and Kavitha | 2011 | Software, Internet,Web Storage, access | - | * | + |
| M. Jog and M. Madiajagan | 2012 | Security design in IAAS | × | - | √ |
| D. Chen and H. Zhao | 2012 | Protection of Information Security, Privacy | - | + | - |
| C. Kalloniatis, H. Mouratidis, S. Islam | 2013 | Deployment scenarios, and security requirements | √ | * | √ |
| Vijay Varadharajan and Udaya Tupakula | 2014 | Security as a Service Model | + | √ | √ |
| Abir Khaldi et. all | 2014 | Design of the security architecture | √ | * | √ |

and main security concerns, which are presently challenged in, cloud computing.

In[14] authors have surveyed on security and privacy in cloud computing. They have examined that a few cloud computing framework suppliers are finding solutions for their worries on security and protection issues. They discover those concerns are not sufficient and more have to be included in terms of five qualities (i.e., availability, data integrity, confidentiality, control, audit) for security.

In[15] authors have examined the architectural requirements for cloud computing systems and explored cloud computing features, architecture and group them as per the prerequisites of end-clients, endeavors that utilize the cloud as their platform, and cloud suppliers themselves. Additionally gives key rules to programming draftsmen and application developers of cloud computing for making future architectures[16].

Table 2 listed the survey done till now, it compares with the parameters like year and publications, topics focused, industry references, security issues and solutions with the help of some notations (+, -, *,√,×, etc.) where + and * are utilized to highlight that specific consideration is paid to a particular subject. √ is utilized to indicate that viewpoint is secured in that article. – is utilized to indicate less consideration is paid to that theme while, × is utilized to signify that subject is not secured in that article.

This literature survey study found a primary challenge for the enterprises in cloud computing is security[17]. It can be clearly understood that there are no security norms defined, significantly after a couple of specialists attempting to detail them. Similarly, it can be followed that despite the fact that few organizations and professionals attempted to form techniques to handle security issues in cloud, there are still numerous organizations that are hesitant to join the gathering of CC clients. Security is still the significant concern for them in cloud computing.

## 3. Cloud Security and Privacy Concepts

The cloud computing is mainly concern about the security and privacy. The capacity of individual and delicate data in the cloud raises worries about the privacy and security of such data. The cloud computing is mainly concern about the security and privacy. On that basis the trustworthiness of cloud is evaluated. In a conventional IT-base set-up, an association structure is called as trusted environment.

Security is categorized into two main areas:

3.1. Data Security

3.2. Network Security

## 3.1 Data Security

In cloud computing, cloud service providers provides some security formulas to prevent their data, but these kinds of security formulas may not be in budget for small administrations. However, when group of companies decides to share their resources commonly then, in such cases data can be misused by other organizations. Hence, secure data sources are required. In the shared areas, it is more challenging thing to keep our data secure amongst the group of organizations.[11] explains that the issues in Data security and privacy protection need to be taken care of. Whereas, the design of security architecture is given by [8]. Table 3 shows challenges of cloud in Data Security[18,19].

Data security is the act of safeguarding data from unauthorized access, disclosure, use, disruption, inspection, recording, modification, or destruction. The data security[19] contains three attributes Confidentiality, Integrity and Availability (CIA) as shown in Figure 5. Confidentiality ensures that our data is confidential, unauthorized user cannot access user information, Some test are utilized to help associations to survey and accept, to which degree of information is secured from malicious client and they are as per the following:

(a) Cross-site scripting [xss]

(b) Access control weaknesses

(c) OS and SQL injection defects

(d) Cross-site demand imitation

(e) Cookie Manipulation

(f) Hidden eld Manipulation

(g) Insecure stockpiling

(h) Insecure configuration

Integrity verifies that your information is stays as it is approved client that can change our information. Availability ensures that authorized user only can access information all the time. All security instrument spins around these three ideas. Similarly, AAA (Authentication, Authorization, Auditing[19]) are another popular concepts as shown in Figure 6. The process of verifying that just approved client can get to the information. Tentative analysis of exercises in your base and staying informed regarding what has happened and if there should be an occurrence of attack or something inconsistency, backtracking and being verify that attack.


**Figure 5.** CIA Triad.

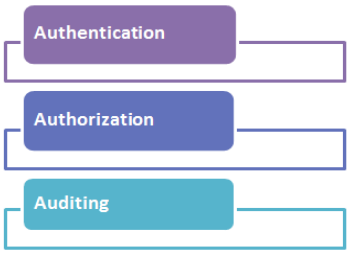


**Figure 6.** AAA (Authentication, Authorization, Auditing).

The process of verifying who the user is? Will it be authorized user or unauthorized? is called Authentication[20]. Authorization is a procedure of verifying that just approved client can get to the information. Examining is a methodology of experiencing all the exercises in your base and staying informed regarding what has happened and if there should be an occurrence of attack or something inconsistency, backtracking and being verify that what has happened

In data security few points are still there that need to be take care:

i. Who has control (accessibility) of data?

ii. Check for the participating companies while communication and make sure that any third party organization in involving or not.

iii. While communicating and transferring data, the clients who are involved they need to check that data which is transferring from cloud service provider is carrying with the use of standard protocols or not.

iv. When it comes to data protection, if it fails then while transferring then, it might results into managerial, civil type of issues. (This depends on controlling data of country). Because of multi-transferring of data logs in associated provides these issue may happen.

v. There is a strong need of updating and maintaining security algorithms time to time, if not then data leakage may happen.

vi. With the help of security algorithms, the data which has stored in cloud server need not to be completely secured. While searching some data in cloud server, it is necessary to take care while retrieving data from cloud server.

vii. Not only this, but complicated security algorithms also raising security problems while retrieving data from server.

**Table 3.** Challenges of cloud in Data Security[19]

| Relation | Description |
|---|---|
| Data Security Related-- | Data Locality |
| | Data Integrity |
| | Data Segregation |
| | Data access |
| | Data Confidentiality Issue |
| | Data Breaches |
| | Reliability of Data Storage |
| | Data Center Operation |
| | Data sanitization |

### *3.1.1 Data Locality*

Here, client does not know where the information is stored away. In numerous cases, this can be an issue. Due to consistency[20] and information protection laws in different countries, locality of information is of most extreme essentialness in numerous architectures[21] of organizations. Ex. In numerous EU and South America nations, certain sorts of information can't leave the nation in light of the fact that of conceivably touchy information. An expansion of the issue of neighborhood laws, there's additionally the inquiry of whose purview the information falls under when an examination occurs.

### *3.1.2 Data Integrity*

Information respectability is one of the most discriminating components in any framework. Integrity is effortlessly attained in a standalone framework with a solitary database. Data integrity in such a framework is kept up by means of transactions and constraints of the database. Transactions ought to take after ACID (atomicity, consistency, isolation and Durability) properties to guarantee information integrity. Most databases help ACID exchanges and can protect information.

### *3.1.3 Data Segregation*

From all existing characteristics of Cloud, one of the important is Multi-tenancy. With the help of this major characteristics, multiple users can store their data by utilizing cloud services. In such a circumstance, information of different clients will locate in the same area. Intrusion of information of one client by an alternate gets to be conceivable in this environment. This Intrusion is possible either by hacking through the loopholes in the application or by infusing customer code into the SaaS system. A customer can compose a masked code and infuse into the application. if the application executes this code without verification, then there is a high capability of Intrusion into other's information.

### *3.1.4 Data Access*

Security policies relates issues of data access[22]. In a typical situation, a small business organization can use a cloud provided via some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations where in some of the employees are not given access to certain amount of information. These security policies must be added here by the cloud to evade intrusion of data by unauthorized users.

### *3.1.5 Data Confidentiality Issue*

The definitional limits of cloud computing are quite wrangled about today. Distributed computing includes the offering or stockpiling by clients of their own data on remote servers possessed or worked by others and gets to through the Internet or different associations. The whole substance of a client's capacity gadget may be put away with a solitary cloud supplier or with numerous cloud suppliers.

### *3.1.6 Data Breaches*

Breaches into the cloud environment will conceivably assault the information of all clients. In spite of the fact that SaaS supporters assert that SaaS suppliers can give better security to clients' information than by conventional means, Insiders still have entry to the information yet it is simply that they are getting to it in an alternate manner. The SaaS suppliers' representatives have admit-

tance to a considerable measure more data and a solitary occurrence could uncover data from numerous clients. SaaS suppliers must be agreeable with PCI DSS (Payment Card Industry—Data Security Benchmarks) (PCI DSS, 2009) with a specific end goal to have dealers that must consent to PCI D.

### 3.1.7 Reliability of Data Storage

Through there exist no issues with virtualization supervisor, engineer will have better control over security. The virtual machines have numerous issues inside it, yet it still a decent answer for giving secure operation in CC connection. With becoming virtualization in every part of distributed computing, there is an issue with dependability of data storage and holder holding control over information, giving little concern to its physical area. The clients additionally believe that storage systems are most certainly not solid in CC. In CC, dependability of information storage is a general issue.

### 3.1.8 Data Center Operation

Organizations utilizing cloud computing applications are worried about securing information while it's consistently exchanged between the cloud and the business. The concern is about what will happen to client's information if something happens to cloud storage? If the information is not overseen legitimately, information storage and information access can turn into an issue. For example, information reconciliation, information consistency, strategy administration and so forth, are not given obliged consideration. Adding to this specify that cloud is not secure unless systems to debug, diagnose disseminated questions and break down exists for the cloud suppliers.

### 3.1.9 Data Sanitization

It is the methodology of uprooting undesirable or antiquated sensitive information from the storage. At the point when a client redesigns information in the cloud, he/she can secure the information by encrypting infor-

**Table 4.** Effects and solution directives of different parameters in data security

| Sr No | Data Security Parameters | Effects | Affected Service Models | Solution Directions |
|---|---|---|---|---|
| **1** | Data Locality | Loss of control over the data | SaaS, PaaS and IaaS | Provide monitoring control system on offered services |
| **2** | Data Integrity | Confidential data can be compromised, deleted or modified | SaaS, PaaS and IaaS | Use data retention and backup techniques<br>Apply secure data encryption algorithm<br>Configure secure API's |
| **3** | Data Segregation | Intrusion of information of one client by an alternate gets to be conceivable | SaaS, PaaS and IaaS | Use security policies<br>Strong authentication mechanism<br>Activity monitoring |
| **4** | Data Access | Intrusion of data by unauthorized user | SaaS, PaaS and IaaS | Use strong passwords<br>Strong authentication mechanism |
| **5** | Data Confidentiality | Unauthorized access | SaaS, PaaS and IaaS | Strong encryption mechanism |
| **6** | Data Breaches | Attack on information of all other clients in cloud | SaaS and PaaS | Authentication mechanisms<br>Use monitoring and altering system<br>Use compliance reporting notifications |
| **7** | Reliability and Data Storage | Dependability of information storage | SaaS and IaaS | Use virtualization techniques<br>Use secure infrastructure |
| **8** | Data Center Operation | Data center breakdown,Data reconciliation,Data consistency,Strategy administration | SaaS, PaaS and IaaS | Use consistent data updating and checking services |

mation on the cloud. Regardless of the possibility that the information deleted or no more required ought to be erased in a protected manner such a manner, to the point that unapproved access is impractical. It is likewise a benefit if the client is kept up-to-date how his information is erased. Amazon Web Services (AWS) technique incorporates a decommissioning procedure when the storage device arrived at to the end of useful life. Following Table 4 gives the effects and solution directives of different parameters in data security.

## 3.2 Network Security

In[23] cloud, while communicating one organization with another[24,25] organization sensitive data may transfer, to ensure that this sensitive data secure from leakage through network traffic. We need to provide a security to that extent. To secure this data, some strong network traffic encryption techniques are there: Secure Socket Layer (SSL), Transport Layer Security (TLS)[26,27]. Let us consider Amazon Web Services (AWS), there are some traditional network attacks such as Man-In-The-Middle (MITM) attack, packet sniffing, port scanning, IP spoofing. AWS provides a strong security to its clients from such attacks[27]. Following are some tests and approve the network security of merchant:

a) Network penetration and packet analysis
b) Session management weaknesses
c) Insecure SSL trust configuration

### *3.2.1 Application Vulnerabilities*

With new points of interest cloud likewise bring to the vulnerabilities of developers and dangers identified with APIs. It is realized that in the cloud, any application or programming that is utilized lies as a part of cloud yet not with the real client and if this product has vulnerabilities then it can have a decrement effect on all the clients utilizing the cloud.

### *3.2.2 Host and Network Intrusion*

Especially in PaaS this issue emerges, where control may be given to a client by Service Provider to some degree. Service suppliers have to remember that control the application level.

### *3.2.3 Denial of Service*

These are conceivable in cloud which can be a danger to information under transmission. Dissimilar to bypassing preventively and securely measures the aggressor utilizes strategies, for example, bundle part, payload transformation, shell-code change and copy insertion[28]. There are three distinctions of DoS:

- Direct denial of service
- Indirect denial of service
- Distributed Denial of Service (DDoS)

### *3.2.4 Men in the Middle of Attack*

Assailants make a free association which hand-off on the messages between client and supplier. The assailant[29] makes the client and supplier accept that this association is secured and makes them talk straightforwardly, however behind the scene aggressor controls the entire association and gets each message which is sent to them (client and supplier). The assailant can likewise potentially alter the message before sending to the respondent.

### *3.2.5 IP Spoofing*

Utilizing someone's IP address and making packets of TCP/IP is called IP spoofing. In this situation, interloper gets access to trusted framework and sends messages as in the event that trusted host is sending these messages. Here the vindictive client imitates the real client with the assistance of IP location. Amazon Ec2 can't send a case satirize system traffic Firewall composed in amazon web server precludes a case sending messages with whatever other IP location or MAC address other than its own.

### *3.2.6 Port Scanning*

A port is a spot from which information goes in or out of a framework. At the point when a framework's security fields are configured to send or get information through a port. At that point, that specific port is powerless against port output. At the point when a system is examined for vulnerabilities, port examining demonstrates these powerless ports as open entryways. At the point when a machine tries to get to web, a port is opened as a matter of course and it is impractical to stop port examining. This can result in security ruptures in distributed computing stages.

### *3.2.7 Packet Sniffing*

It is listening to system gadgets and catch raw packets. On the off chance that a programming finds a packet suiting a specific criteria, it logs into a file. A virtual case running in unbridled mode can't get or sniff „traffic which

is planned for a different virtual case. The hypervisor won't convey any train clients place their interfaces into unbridled mode. On the off chance, that two virtual occurrences are dead set on the same physical host and are possessed by same clients then they can't hear each out other's traffic.

The organization selects the security model as per their requirements; since diverse associations have distinctive cloud models (IaaS, SaaS, PaaS) have different security dangers. The Cloud Service Provider (CSP) and the client association's security responsibilities contrast incredibly between the cloud models. Provision must be taken to guarantee that the client organization has the same conspicuousness and control of their applications and Wikipedia characterizes distributed computing security as „cloud computing security (normally indicated by just as „cloud security") is a developing sub-area of machine security, system security and all the more comprehensively, data security. It alludes to an wide set of strategies, advances and controls deployed to ensure an information, applications and the related base of distributed cloud computing. Table 5 shows summary of network security issues with their mitigation directives.

**Table 5.** Summary of network security issues with their mitigation directives

| Sr. No. | Network Security Parameters | How?/ When? | Effect | Affected Service Model | Mitigation Techniques |
|---|---|---|---|---|---|
| 1 | Application Vulnerabilities | Service availability<br>Integrity of workload state | Dangers with APIs<br>Decrement effect on all the clients utilizing cloud<br>Affects service integrity | SaaS, PaaS and IaaS | Use strong APIs<br>Use Firewalls<br>Check service integrity through hash function |
| 2 | Host and Network Intrusion | When service provider gives control to a client with some degree | Trojan horse and malwares attacks on delicate data | PaaS | Incorporate efficient firewalls<br>Secure SSL trust configuration |
| 3 | DoS (Denial of Service) | During data transmission from client to provider | Danger to information under transmission<br>Affects availability of cloud services | SaaS and PaaS | Proper configuration of IDS/IPS |
| 4 | Man-In-The-Middle | Accessing data communication between client and provider | Affects data security and data privacy | SaaS, IaaS and PaaS | Configure proper SSL |
| 5 | IP Spoofing | Modifying web service description file such as WSDL<br><br>Utilizing someone's IP address and making packets of TCP/IP | Abnormal behaviour of deployed services<br><br>Affects service confidentiality | SaaS and PaaS | Strong isolation between VMs<br>Use firewalls<br>VPN protects external connections coming into network |
| 6 | Port Scanning | When ports are identified as powerless for vulnerabilities | Affects data security and data privacy | SaaS and PaaS | Use firewalls<br>Configure proper SSL |
| 7 | Packet Sniffing | Catch raw packets<br>Logs the files of packets | Affects data transmission and communication | PaaS | Use firewalls |

## 4. Security Issues in SaaS, PaaS and IaaS

The security apprehended identifies with the different cloud computing service delivery models. Cloud service[30] mainly classified into three major types: (answer for RQ2)

- Ø Software as a Service (SaaS)
- Ø Platform as a Service (PaaS)
- Ø Infrastructure as a Service (IaaS)

Concerns of these three models are explained:

### 4.1 Concerns in SaaS

It is a conveyance of business applications intended for particular reason. Salesforce.com is a best case in point of SaaS. The client[31] has to depend on the provider for fitting security measures in SaaS model. Here, security issues arises in SaaS while sharing each other's data. The aim is to enhance the security functionality provided by the legacy application and attaining as unsuccessful data migration but not on the ability of softwares.

### 4.2 Concerns in PaaS

It incorporates the conveyance of the more than simply platform. It delivers a solution stack- a corresponding set of programming that gives everything and designer need to construct an application for both programming advancement and runtime.

PaaS Provides developers to build its own softwares on the platform. Hence, it is more extensible than SaaS. This extends to security characteristics and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security[32].

### 4.3 Concerns in IaaS

Foundation as an issue is the conveyance of machine equipment (servers, organizing engineering, stockpiling, and server farm space) as an issue. It might likewise incorporate the conveyance of OS and virtualization innovation to deal with the resources. In spite of the fact that generally accepted, however virtualization[33] could conceivably be the piece of the foundation being conveyed as an issue. To achieve maximum trust and security on a cloud resource, several techniques would have to be applied.

Examples: An association may utilizes services of public cloud, service for filed information yet keep on maintaining in-house stockpiling for operational client information.

## 5. Available Solutions for Cloud Security from Literature

According to the study of papers, this survey comes with the various solutions that are provided by various authors for cloud security. They are as follows:[8] proposed the architecture on secure cloud computing, this architecture consists of four zones: Cloud architecture zone which is again divided into four zones; Demilitarized zone (DMZ) which offers its services to client ex. web server, email, etc. Second zone is internal customer zone which host the organization's workstations and also perform internal tests to validate servers and provides levels of security. Third zone is a trust zone contain critical server that controls and manages all architecture hence, called as management zone, fourth zone is for external customer via this zone external client access the required services. Cloud architecture policy focuses on security policies. Cloud security requirement to enhance the security of architecture. Cloud architecture components contain following components: one is IPS (Intrusion Prevention System) allows to audit the information system, second is a cluster firewall and a third one is Tunnel SSL/VPN.

[9] has given the design of security architecture and discussed different types of attacks are counteracted by proposed architecture that provides security as a service model that a cloud provider can offer to its multiple tenants and customers of its tenants.

[34] has proposed the solution to support the elicitation of security and privacy requirements[35] and selection of appropriate deployment model based on requirements, this framework provides the modeling languages that builds on concepts from requirements, security, privacy[35] and cloud engineering and a system process, this framework composed of two components a modeling language and a process. To strengthen the security, this framework used secure Tropos and Pris from large number of different existing security and privacy requirement engineering and methodologies. Tropos focuses on elicitation and analysis of security requirement and Pris specifically focuses on privacy requirement. On the other hand, second component a process that aims to provide a structured for elicitation and selection of deployment model based on requirements.

To strengthen cloud computing security, [10] has given the solution that deals with security challenges faced by cloud vendor and not consumer since, vendor's responsibility to ensure security is maximum at Infrastructure as a Service (IaaS) level:

A. Integrating TCG standards to cloud. This is first method of cloud security implementation, this integrates existing trusted computing standards into the cloud with the use of some technologies TPM (Trusted Platform Module), TNC (Trusted Network Connect) and trusted Storage.

B. TCCP (Trusted Cloud Computing platform): It enables IaaS providers to provide a closed execution environment that guarantees the confidential execution of guest VM.

[12]has given a secure public cloud workflow deployments to maintain efficient productivity and achieve competence advantage to reach this aim authors have given the policies, retaining control, setting policy, monitoring and runtime security.

## 6. Issues in Available Solutions of Cloud Security

[8–12,34] have presented various solutions for cloud security issues. This paper analyzed available security models of authors based on five parameters i.e. Availability, Data Privacy[31], Access control, Authorization and Audit. This analysis shows which authors security model focused on which parameter, i.e. what are the parameters authors considered by presenting their cloud security solution.

Table 6 shows comparative issues analysis based on five parameters where √√ shows that parameter is fully focused on security solution, √ shows parameter is partially focused, and × shows not considered.

From this issues analysis of various security solutions, this paper concluded that, Audit parameter has not taken into consideration of maximum security solutions, very few solutions are considering auditing. So, the observation from this study is to consider Audit as the important parameter in presenting security solution.

## 7. Proposed Solution

This paper presents the solution with the consideration of maximum-security parameters including auditing for public cloud environment. To achieve security goals by following security policies User's Security Requirements Framework idea is presented. Figure 7 shows proposed security model where Security Layer contains four factors; security goals, security policies, security parameters and resource constraints, based on these factor the architecture is proposed.

To provide flexibility to service users, this idea is proposed. Figure 8 shows the security workflow, service user is defining its security goals, for example confidentiality of data should be maintained, access control (Authentication, Authorization, and Auditing) and Integrity. To express these goals to the provider user will fix Security policies like, "data should store in encrypted format" , "key length". Which are then translated into security parameters. This translation is done because; parameters will help to compare security parameters of provider and service mechanism.

After translation, list of security parameters will be stored and then it will be delivered to the service provider, so that service provider can compare those parameters with its own parameter and if maximum parameters fulfills the requirements then service provider will get ready to provide service to the user based on SLA agreements. Now after finishing the agreements, provider translates security parameter into security constraints. By doing this step processing time will decrease as service user may not need all the functionalities of provided service.

**Table 6.** Parameter wise comparison of existing security models from literature

| Existing models by authors | Availability | Data Privacy | Access Control | Authorization | Audit |
|---|---|---|---|---|---|
| **Author**[1] | √√ | √√ | √√ | √√ | × |
| **Author**[2] | √√ | √√ | √√ | √√ | √ |
| **Author**[4] | × | √√ | × | × | × |
| **Author**[5] | - | √√ | √√ | √ | × |
| **Author**[6] | × | √√ | √√ | √√ | - |
| **Author**[7] | × | × | √√ | √√ | √ |

## 8. Conclusion

This paper covered the topics related to cloud security[35] such as cloud deployment models; public cloud security. In the study of cloud deployment model security, it is found that public cloud is popular form of cloud and it is more flexible than the other cloud deployment models but main concern is related to its security, in public cloud the resources are located off-site hence public cloud is less secured and the service delivery models can be subjected to malicious activities.

Moreover, this paper studied about the cloud security concerns brings a new challenge to the cloud service provider and a parameter wise comparison of existing security solutions. Based on these comparison a new security model is proposed which describes Users' security requirements architectural Framework (USRAF).

## 9. Acknowledgement

I would like to thank all the authors of referred papers for introducing the issues in cloud security by giving the various architectural models and solutions to resolve the issues concerns to the cloud computing security. A special note of thanks to VIT University for providing necessary infrastructure facilities to carry out the Research work and all the ones who has directly and indirectly helped me to complete this study.

## 10. References

1. Jennings R. Cloud computing with the windows azure platform. John Wiley and Sons; 2010 Dec 29.
2. Buyya R, Ranjan R, Calheiros RN. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. Algorithms and Architectures for Parallel Processing; 2010 May 21. p. 13–31.
3. Janbeglou M, Yan W. A novel agent-based framework in bridge-mode hypervisors of cloud security. 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing Springer Berlin Heidelberg; 2013. p. 467–79.
4. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR. Security issues in cloud environments: A survey. International Journal of Information Security. 2014 Apr 1; 13(2):113–70.
5. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems. 2009 Jun 30; 25(6):599–616.
6. Krutz RL, Vines RD. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing; 2010 Aug 9.
7. Rajarajeswari S, Somasundaram K. Data confidentiality and privacy in cloud computing. Indian Journal of Science and Technology. 2016 Jan 19; 9(4):1–8.
8. Sheshasaayee A, Margaret TS. The challenges of business intelligence in cloud computing. Indian Journal of Science and Technology. 2015 Dec 3; 8(36):1–6.
9. Varadharajan V, Tupakula U. Security as a service model for cloud environment. IEEE Transactions on Network and Service Management. 2014 Mar, 11(1):60–75.
10. Jog M, Madiajagan M. Cloud Computing: Exploring security design approaches in infrastructure as a service. 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), IEEE; 2012 Dec 8. p. 156–9.
11. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE). 2012 Mar 23; 1:647–51.
12. Mace JC, Van Moorsel A, Watson P. The case for dynamic security solutions in public cloud workflow deployments. 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W); 2011 Jun 27. p. 111–16.
13. So K. Cloud computing security issues and challenges. International Journal of Computer Networks. 2011, 3(5):247–55.
14. Zhou M, Zhang R, Xie W, Qian W, Zhou A. Security and privacy in cloud computing: A survey. 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG); 2010 Nov 1. p. 105–112.
15. Rimal BP, Jukan A, Katsaros D, Goeleven Y. Architectural requirements for cloud computing systems: An enterprise cloud approach. Journal of Grid Computing. 2011 Mar 1, 9(1):3–26.
16. Bhushan SB, Reddy P, Subramanian DV, Gao XZ. Systematic survey on evolution of cloud architectures. International Journal of Autonomous and Adaptive Communications Systems, Inderscience. 2015.
17. Liu W. Research on cloud computing security problem and strategy. 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet); 2012. p. 1216–19.
18. Manjusha R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015 Apr 1; 8(S7):220–7.

19. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011 Jan 31; 34(1):1.
20. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr 1; 6(4):4396–401.
21. Mell P. What's Special about Cloud Security?. IT Professional. 2012; 4(14):6–8.
22. Mohan K, Aramudhan M. Ontology based access control model for healthcare system in cloud computing. Indian Journal of Science and Technology. 2015 May 4; 8(S9):218–22.
23. Beulah S, Dhanaseelan FR. Survey on security issues and existing solutions in cloud storage. Indian Journal of Science and Technology. 2016 Apr 14; 9(13):1–8.
24. Vaquero LM, Rodero–Merino L, Morán D. Locking the sky: A survey on IaaS cloud security. Computing. 2011 Jan 1; 91(1):93–118.
25. Fusenig V, Sharma A. Security architecture for cloud networking. 2012 International Conference on Computing, Networking and Communications (ICNC); 2012 Jan 30. p. 45–9.
26. Celesti A, Tusa F, Villari M, Puliafito A. Security and cloud computing: Intercloud identity management infrastructure. 2010 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE); 2010 Jun 28. p. 263–5.
27. Kaufman C, Perlman R, Speciner M. Network security: Private communication in a public world. Prentice Hall Press; 2002 Apr 22.
28. Alarifi S, Wolthusen SD. Mitigation of cloud-internal denial of service attacks. 2014 IEEE 8th International Symposium on Service Oriented System Engineering (SOSE); 2014 Apr 7. p. 478–83.
29. Bicakci K, Unal D, Ascioglu N, Adalier O. Mobile authentication secure against man-in-the-middle attacks. 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud); 2014 Apr 8. p. 273–6.
30. Behl A. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. 2011 World Congress on Information and Communication Technologies (WICT); 2011 Dec 11. p. 217–22.
31. Sheshasaayee A, Margaret TS. The challenges of business intelligence in cloud computing. Indian Journal of Science and Technology. 2015 Dec 3; 8(36):1–6.
32. Christodorescu M, Sailer R, Schales DL, Sgandurra D, Zamboni D. Cloud security is not (just) virtualization security: A short paper. Proceedings of the 2009 ACM workshop on Cloud Computing Security; 2009 Nov 13. p. 97–102.
33. Durairaj M, Manimaran A. A study on security issues in cloud based e-learning. Indian Journal of Science and Technology. 2015 Apr 1; 8(8):757–65.
34. Kalloniatis C, Mouratidis H, Islam S. Evaluating cloud deployment scenarios based on security and privacy requirements. Requirements Engineering. 2013 Nov 1; 18(4):299–319.
35. Mather T, Kumaraswamy S, Latif S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media, Inc.; 2009 Sep 4.