ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 8, Issue 4 , April 2021

Cloud Computing and Associated Security Concerns

Gautami Mathur*, Anchal Kapoor, Muskan Munjal, Dr. Suman Madan

Research Student, Jagan Institute of Management Studies, sector- 5, Rohini, Delhi, India
Research Student, Jagan Institute of Management Studies, sector- 5, Rohini, Delhi, India
Research Student, Jagan Institute of Management Studies, sector- 5, Rohini, Delhi, India
Associate Professor, Jagan Institute of Management Studies, sector- 5, Rohini, Delhi, India

ABSTRACT:In a cloud computing environment, the entire data reside on a server, which enables the data to be accessed from anywhere in the world. Cloud eliminates the need to buy a stack of servers, maintaining and monitoring those servers and the need to buy more servers when there is high traffic and these advantages are huge and attracts the customers. But as organizations are depending more on cloud service providers and their data can be stored in any corner of the world, therefore there are numerous threats to the user's sensitive data on virtual storage.Also improper safety measures on part of developer can lead to data leaks and it is becoming a growing concern for IT organizations. This survey paper aims to analyze those issues which are threatening the Cloud adoption and affecting the privacy of various users linked to it.

KEYWORDS: Cloud computing,Server, Automation, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

I.INTRODUCTION

Cloud computing's concept relies on on-demand availability of computer resources, especially on data storage(i.e. cloud storage). This can be limited to a single organization(private clouds), or are also available to multiple organizations (public cloud). Cloud computing providers provide large datacenters at reasonable cost due to their expertise in organizing resources.

Cloud computing is a huge shift from the way businesses usually think about IT resources. Here are a few common reasons why several organizations are turning up to the cloud computing services: Cost, Speed, Global scale, Productivity, Reliability, Security.

Not all clouds are the same and not one type of cloud computing is right for everyone, it is judged according to the requirement of the customer. Several different models, types, services and resources have developed to help offer the right solution for your requirements.

Mostly, the cloud computing services lies into three main categories i.e.[1] :

- **Infrastructure-as-a-service(IaaS)**- No need to manage or purchase servers, storage, networking, etc.
- **Platform-as-a-service(PaaS)** –Runtime environment, Platform, OS, storage,etc. provided by service provider.
- **Software-as-a-service(SaaS)-.** Applications, Data, runtime environment, servers, etc. provided by service provider.

These are sometimes called the cloud computing stack due the reason they are build on top of one another. Knowing about what they are and how they are different makes it easier to accomplish your business goals with IT resources. At the same time, security has emerged as arguably one of the most significant barrier as well as the need to faster and more widespread acceptance of cloud computing.

In this paper, we'll investigate the security concerns of Cloud Computing systems. As Cloud Computing referred to the applications delivered as services over the Internet and the infrastructures that provide those services [10], we present the security concerns in terms of the diverse applications and infrastructures. More concerns on security issues, such as accessibility, availability, confidentiality, integrity, authorization and so on, should be taken into justification.There are plentiful security threats associated with cloud-data services. These threatscomprisesnetwork eavesdropping, illegal invasion, and denial of service attacks, and also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud services.

II. RECENT STUDY

Garima Gupta et al[1] stated, Cloud computing has various function like flexibility, multi-tendency, availability, etc.cloud computing has various threads but there are procedures to guard the cloud, also there are several tools and model that were introduced to counter the cloud from several malicious attacks. It has several computing techniques as well like distributed, grid, etc. cloud provide the various facility to their user through the internet. today cloud is used by both industry and academic sector.

RohitBhadauria et al[2] referred that now a days the data store in the cloud , the services and solutions are all used by the industries . there are several issues that are still unsolved and were threatening Cloud computing selection ,also there are severe server breakdown which can't be denied by anyone. There are many application and network-level threats and there are also ways to control them. The solution to prevent or secure cloud that is auditing .It should be done in regular intervals to protect the cloud from external threats.

According to Mohammad AbdurRazzaque et al[3] cloud computing provide multiple facilities i.e. storage, hosting ,servers,etc.Although cloud computing has several benefits it has disadvantages as well. There are various challenges to overcome these disadvantages like Tableau algorithm in which we obtain PKB that is Privacy Knowledge Base through which we can resolve the problem of user and can help him fulfilling his requirements, next is ordinal exchange in which privacy disclosure assert is used through which both user and service provider can be satisfy.

Minhaj Ahmad Khan Bahauddin[4] said that through the facility of effective usage of shared resources cloud computing provide the best services to his customers but even after all this there is still one thing that hinders it and that is security issues. plus the intrusion detection system as well as intrusion prevention system are good in the phase of working mechanism, scalability, and many more.there is a requirement of a large number of standard Acts and regulations only through which we will get an agreement by the cloud service.

As per Ashish Singh et al[5] cloud computing provides various benefits to its user i.e. large storage area to store their data plus it is cost-effective and easy to use, it is friendly, and can be accessed from anyplace that's the reason it is booming all over the world, but the issues of security and privacy became a large obstacle for its growth as user's are not much confident about their privacy on the cloud as there are a large number of security issues which can be classified as 1. data storage issue in this there are several kinds of issue a user can face like cryptography, untrust computing, Malware, etc. 2. legal aspects in this laws, acts, governance, legal problem, etc. all take place and many more such issues are there each problem has its solution to be prescribed for example if a user had access control issues in which he/she might concern about the user credentials then they can use encryption which is based on an attribute or they can Use Encryption based on Hierarchical Attribute.

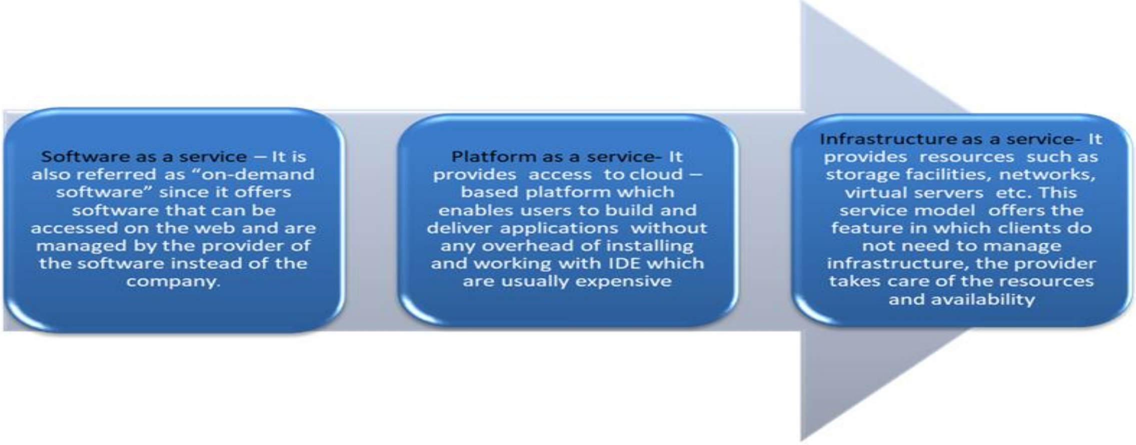
III. CHARACTERISTICS OF CLOUD COMPUTING

A few of characteristics of cloud computing includes the following[9]:

- **On-demand self-service**: It is one of the important features of cloud computing.
  It provisions to constantly monitor the server abilities, computing capabilities, and allocated network storage. This is the fundamental characteristic of Cloud Computing, and a client can check the computing abilities as per his requirements.
- **Resources Pooling**: One of the essential characteristics of Cloud Computing.
  This means that the service provider can share their resources among several consumers, providing them with different set of services according to their needs. This strategy can be applied to data storage, processing services etc.
- **Easy maintenance**: One of the best cloud computing characteristics. The servers are maintained throughout with best services therefore the downtime remains very low. The updates are more doable with the devices and perform more rapidly than the preceding versions.
- **Security:** Cloud always creates a copy of the data that is stored in it to prevent any data loss in any case. If data is lost by any chance so the data is retrieved by the copy version stored in other server. This feature is more relatable when several users work on the same file in real-time and the file might suddenly get corrupted.
- **Automation:** It is a vital characteristic of cloud computing. The capability of cloud computing to automatically maintain a cloud services, installing and configuring cloud services is termed as automation in cloud computing. In other words the process of reducing human effort and maximize machine work.

IV. CLOUD COMPUTING SERVICE MODEL

Cloud computing service models are as follows:-



Software as a service – It is also referred as "on-demand software" since it offers software that can be accessed on the web and are managed by the provider of the software instead of the company.

Platform as a service- It provides access to cloud – based platform which enables users to build and deliver applications without any overhead of installing and working with IDE which are usually expensive

Infrastructure as a service- It provides resources such as storage facilities, networks, virtual servers etc. This service model offers the feature in which clients do not need to manage infrastructure, the provider takes care of the resources and availability

Fig. 1:Cloud Computing Service Model

V. CLOUD DEPLOYMENT MODELS

These are following cloud deployment models[2]:

1) **Public cloud**: These Cloud services are provided for public use. It is based on the concept of shared cost model for all the users. This model in cloud supports all the users willing to use resources like OS, Storage, application server, database on subscription plans. Since many customers are sharing the resources, then danger to public cloud could be of service quality and security.
2) **Private cloud**: In this cloud model, the services are provided for private or single enterprises. In this infrastructure may be coped by the enterprise itself or by the service provider that takes care of it. These cloud models are expensive than public cloud and resources are limited to the clients that belongs to the enterprise that owns the cloud. The service quality and security is better.
3) **Hybrid cloud**: This type is a combination of both private and public cloud. In this, organizations can leverage public clouds services along with private cloud services.
4) **Community cloud**: In this deployment model, multiple enterprise can share resources that belongs to a community. In other words, infrastructure shared among enterprises with same requirements. The cloud services can be hosted by a third party or within the enterprise.

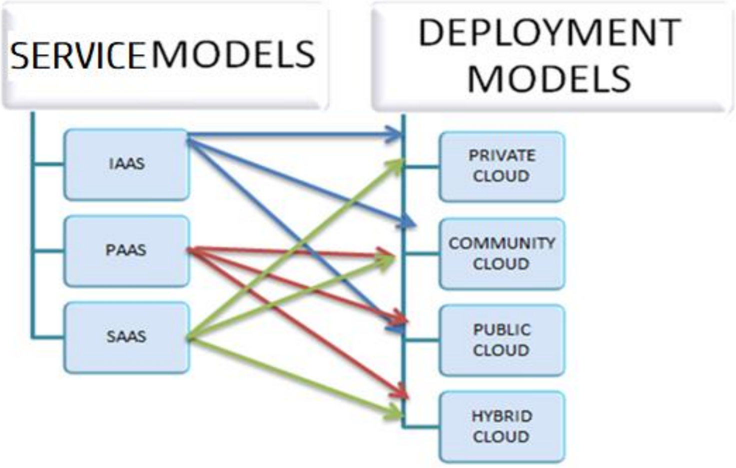


Fig. 2:Service model and Deployment model

VI. APPLICATION LEVEL SECURITY

Application level security refers to providing security to applications so that the attackers are not able to get access over these applications and make desirable changes to their format. To prevent the attack security software and hardware resources are used.These days, attackers impersonate as a authorized user and the system consider them as a trusted user, and allows full access to the attacker. The reason is that the outdated network level security policies. With the progression in technology, these security policies have become out of date. There have been instances when the system's reliability has been breached, as system can be accessed in the disguise of a authorized user. With the latest technological advancements, it is completely possible to impersonate a authorized user and manipulate entire data without being seen.Hence, it is required to minimize these risks by installing higher level of security checks.b
It has been noted that websites are secured at the network level ut there may be security escape route at the application level which may allow unauthorized access to information. The threats to application level security include Cookie manipulation, Hidden field attacks, DoS attacks, CAPTCHA Breaking etc. resulting unauthorized usage of the applications.

1) Cookies Manipulation

Cookies stores the user's personal information and once these cookies are accessible, the information stored in cookies can be used to disguise a trusted user. The information stored in cookies can be modified to have an unauthorized access to an application or to a web page. To avoid poisoning of cookie one can perform regular cleanup or implement encryption scheme for cookie data.

2)Hidden Field Attacks

There are hidden fields on a webpage which contains page related information and used by developers. These are highly vulnerable to attacks as they can be changed easily.

3)Denial-of-service attacks

DoS attack is a attack in which the attacker seeks to make services unavailable to authorized users by temporarily or indefinitely disrupting service. In this attack, the server providing the service gets a large number of requests and as a consequence the service becomes unavailable to the authorized user. Sometimes, we try to access a site and we see that due to overburden on the server with the requests to access the site, we are unable to access the site and discover an error. This happens when the server gets overburdened with the large number of requests and is unable to handle them. The happening of a DoS attack increases bandwidth consumption. It also lead to parts of cloud unreachable to users. Intrusion Detection System (IDS) can be used to provide defense against this type of attacks. All cloud is packed with separate IDS. In case of attack, the IDS alerts the entire system.

4)Dictionary Attack

In this attack, the attacker make use of every possible combination of words in order to decrypt the data residing on the network. To avoid this attack the client can be introduced to challenges when he tries to access a network and required to make a response back to the client to be able to access the network.

VII. CLOUD COMPUTING CONCERN SOLUTIONS

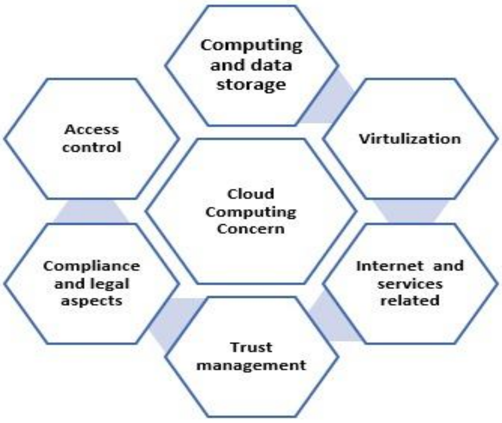

Computing and data storage
Access control
Virtulization
Cloud Computing Concern
Compliance and legal aspects
Internet and services related
Trust management

Fig. 3: Concerns related to cloud computing

- **Data storage and security concern and solutions**

Here data storage and security concerns are discussed with relevant solutions and are summarized below:

Table 1:Data storage and security concern and solutions

Security Topic	Security Concern	Solution
○ **Data storage**	• Remote data storage • Loss of control • Data pooling, data locality • Multi-location • Complex model for integrity checking	• Better security scheme for resident data • File Assured Deletion (FADE) scheme • SecCloud protocol
○ **Un-worthy computing**	• Top down SLAs • Malicious users, downtimes, slowdowns • Dishonest computing, root level error in backups	• A non-interactive solution • A lightweight and low-cost solution for e-banking
○ **Cryptography**	• Insecure cryptography mechanism, poor key management • faulty cryptography algorithms	• Order-preserving encryption • Cryptography in cloud computing
• **Cloud data recycling**	• Un-used hard discard • Hard disk multi-tenant usage • Resource recycling	• Secure data deletion
• **Malware**	• Failure of signature based anti-viruses • Cloud malware syncing	• Detecting malware

- **Virtualization, its security concern and solutions**

The below table focuses on virtualization, security threats and their solutions:

Table 2:Virtualization, its security concern and solutions

Security Topic	Security Concern	Solution
1. **Virtual machine monitor**	• Hypervisor failure, , untrusted VMM components, transparency of VMM, lack of monitor GUI, VMM separation, inspection, and interposition	• HyperCheck • DeHype • HyperLock • SplitVisor • NoHype
○ **Network virtualization**	• limited network access, • inapplicability of standard security mechanisms • Effectiveness of network security devices in virtual network	• Virtual network security

[1] **VMs image management**	• Cryptographic overhead due to large size images • VMs theft and malicious code injection Overlooked image repository	• VM image management system • VM image privacy and integrity
• **Mobility**	• VM cloning VM mobility Generation of untruth configurations Live VM migration, man-in-the middle attack Replay attack	• Protocol for vTPM based VM migration • Live VM migration • Security framework for VM migration
• **Malware**	• Avoidance of malware Spreading of malware onto VMs Metamorphic engines	• Intrusion prevention system

- **Internet and services related, its security concern and solutions**

In this table, Internet and the services related with their security concerns and solutions are discussed:

Table 3:Internet and services related and security concern and solutions

Security Topic	Security Concern	Solution
○ **Advanced repeated threats and venomous outsiders**	• Information collection, scan publicly available information Doxing	• Property hidden • Strong privacy laws
○ **Internet protocols TLS attack, cookie theft**	• network based cross-tenant attacks • Session hijacking • Mixed HTTP and HTTPS data streams • Weak cryptographic • key usages • Cookie theft, cookie poisoning, impersonation attacks	• Use Secure Flag for security of the cookies OpenSSL • Network Security Services (NSS) • Secure the server operators private keys Use secure HTTP protocol
○ **Web services**	• HTTP stateless protocol, • API transaction support for integrity • Metadata spoofing attacks, • improper WSDL documents	• XML Encryption • XML Signature • Encoding of binary tokens
○ **Web technologies**	• Increases infected web sites • authentication break, • code injection HTML hidden field manipulation attack • Watering hole attacks, • Faulty plugin	• Real-time security updates Video controls • Network port monitoring • Web Security and Filtering

- **Access control, its security concern and solutions**

Here all the threats related to Access control in cloud computing are summed together.

Table 4:Access control, its security concern and solutions

Security Topic	Security Concern	Solution
• **Physical access**	• Malicious insiders • Malicious system admin • Cold boot attack • hardware tempering	• Use extensible Access Control Markup Language (XACML) expressing access policies Secure data access
• **User credentials**	• Weak credential reset methods • Phishing attack, key-logger attack, man-in-the-middle attack, replay attack, sessions hijacking,	• Attribute based encryption • Use Hierarchical Attribute Set Based Encryption
• **Entity authentication**	• Archaic static password Inapplicability of alternative password schemes • Account lockout	• Hierarchy identity based cryptography • ID management framework Decentralized access control for cloud storage SMS based password recovery
• **Authorization**	• Data mashups, inapplicability on centralized access control • malicious third-party applications • Insufficient or wrong authorization assignment • URL guessing attack	• Role based multi-tenancy access control • Multi-tenancy authorization model for collaborative clouds
• **Anonymization[11]**	• Hidden identity of adversaries De-anonymization attacks	• Use a strong and secure anonymization technique that is not easily de-anonymized

➢ **Trust management, its security concern and solutions**

The next table displays trust management and several security concerns, solutions.

Table 5: Trust management, its security concern and solutions

Security Topic	Security Concern	Solution
○ **Cloud to cloud trust**	• Invalid enterprise trust model • Cloud environment openness	• Cloud Trust Authority provides security of the cloud services from multiple providers • Use different trust models
○ **Human aspect**	• Un-trusted employees Password sharing • Password strength and commonness Social engineering Phishing attack	• Public Key Infrastructure based trust model • Evidence based trust model

○ **Reputation**	• Isolation of reputation • Fate-sharing	• Reputation based trust model SLA verification based trust model • Evidence based trust model
○ **Trust on the audit-ability reports**	• Providers reports truthfulness Jurisdictional audits, court system • Data locality • Lack of privacy capable audits techniques	• Policy based trust Use cloud auditor's assessment Accreditation by Auditing Standards Board of AICPA

➢ **Compliance and legal aspects, its security concern and solutions**

Here we discussed about Compliance and legal aspects, its security concerns and summarized solutions below:

Table 6: Compliance and legal aspects, its security concern and solutions

Security Topic	Security Concern	Solution
○ **Forensics**	• Cross platform forensic techniques, public cloud, data locality, legal authority • Data collection and verification	• Use Oruta (one ring to rule them all) approach
○ **Acts**	• Outdated acts • Privacy breaking acts	• Asia Pacific Economic Cooperation (APEC) privacy framework
○ **Legal problems**	• Data jurisdictional borders • Providers compliance evidences • Providers and customers have different interests • Blocked lawful data	• Need an appropriate SLA for data privacy SecAgreement
○ **Incorrect resource usages metering**	• Attack on QoS property • Un-trusted computing, break protocol • Randomly billing	• Trust model based on QoS
○ **Governance**	• Vendor lock-in • Race-to-the-bottom	• Need to frame unified regulatory compliance

VIII. CONCLUSION

In this paper we discussed about the cloud computing, features, characteristics, services model, deployment model, application level security, security threats and challenges in Cloud Computing are highlighted. The threats may vary from network level threats to application level threats. In order to prevent the threats to the cloud, improvement in existing solutions as well as newer solutions are needed to ensure adoption of Cloud computing. The security and privacy improvement will impact its successfulness and widespread adoption.

REFERENCES

[1]A Survey on Cloud Security Issues and Techniques Garima Gupta, P.R.Laxmi2 and Shubhanjali Sharma ,Department of Computer Engineering, Government Engineering College, Ajmer

[2]Bhadauria, Rohit&Chaki, Rituparna&Chaki, Nabendu&Sanyal, Sugata. (2011). A Survey on Security Issues in Cloud Computing.

[3]A Survey Paper on Privacy Issue in Cloud Computing :-Yousra Abdul Alsahib S. Aldeen, MazleenaSalleh and Mohammad Abdur Razzaque,DOI:10.19026/rjaset.10.2495

[4]A Survey of Security Issues For Cloud Computing :-Minhaj Ahmad Khan, DOI: http://dx.doi.org/10.1016/j.jnca.2016.05.010

[5]Cloud security issues and challenges: a survey Ashish Singh and KakaliChatterjee DOI: http://dx.doi.org/10.1016/j.jnca.2016.11.027

[6]Cloud Computing Security Challenges & Solutions-A Survey Srijita Basu, Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury and Pritika Sarkar, DOI: 10.1109/CCWC.2018.8301700

[7]A Comprehensive Survey on Security in Cloud Computing GururajRamachandra, MohsinIftikhar and FarrukhAslam khan, DOI:https://doi.org/10.1016/j.procs.2017.06.124

[8]A Survey on Cloud Computing Security: Issues, Threats, and Solutions SaurabhSingh1 , Young-Sik Jeong2 and Jong Hyuk Park1, DOI:https://doi.org/10.1016/j.jnca.2016.09.002

[9]Cloud Computing Security Issues and Challenges: A Survey AmandeepVerma and SakshiKaushal, DOI:10.1007/978-3-642-22726-4_46

[10]A Security and privacy in cloud computing: a survey: Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, DOI:10.1109/SKG.2010.19

[11]Suman madan, Puneet Goswami;(2020) Adaptive Privacy Preservation Approach for Big Data Publishing in Cloud using k-anonymization, RACSC(Recent patents on CS), vol 14, pp 2689-2690, DOI : 10.2174/2666255813999200630114256

[12]Suman madan, Puneet Goswami, A Privacy Preserving Scheme for Big data publishing in the Cloud using k-Anonymization and Hybridized Optimization Algorithm, IEEE Xplore, DOI: 10.1109/ICCSDET.2018.8821140.