Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

CLOUD COMPUTING: FUNDAMENTALS AND CLOUD SECURITY CHALLENGES

[1]D.Srivani and [2]Kondogu Swetha
[1]Assistant Professor, Avinash College of Commerce, Hyderabad
[2]Associate Professor, Avinash College of Commerce, Hyderabad

Abstract:

Cloud Computing is a network- erected running invention where information is handed to customers on demand. Present Cloud Computing systems holds serious restrictions to cover confidentiality of user's data. Cloud Computing consists of colourful technologies, programs to insure data, services and structure protection. The traditional security armature doesn't apply because the client doesn't enjoy the structure presently. The report consists of the problems related to Cloud Computing and ways in which the user could overcome the risks and issues in the cloud. The study also consists of the security demanded in cloud and how the cloud company manage to secure the cloud from hackers and different risks.

Keywords: Cloud Computing, Cloud Architecture, Types of clouds, Cloud provider, Data integrity, Cloud Confidentiality.

INTRODUCTION:

Cloud Computing is a network- erected running invention where information is handed to customers on demand. Cloud Computing is a registering phase for dispersion of advantages and means that involve structures, programming, operations, preface and commerce. Distributed computing is a robotic force of handling means.

Present Cloud Computing systems poses serious severe restrictions to cover confidentiality of user's data. Since user's sensitive data is accessible in unencrypted forms to remote machines and operated by third party service providers. There are many ways for the protection of user's data from attackers. The user can access the storage anytime and anywhere without carrying an external hard drive. The data that is stored in a cloud is safer than the data stored in a hard drive. It's much cheaper and effective source to use.

A. Types of Cloud Computing

Public cloud is mainly used by the users and is available to public. Therefore, whenever a type of storage is used by public also it comes under public cloud. For illustration, Google drive comes under the type of public cloud where public uses the storage gets certain amount of storage space and they could access it anytime and anywhere. It's truly secured way and everyone login it using different emails and password. There are multitudinous risks and advantages using Cloud Computing.

Private cloud is mainly when an association wants storage. It's a committed storage. So, the major difference between the public and private cloud is that in public cloud many more users can distribute a storage but in private cloud, only independent association they have devoted storage.

Hybrid cloud is when any association uses private cloud public cloud is known as hybrid cloud. For illustration, if one academe wants to store all of its precious videos to a devoted storage also it would come under

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

private cloud and the academe also replies to the pupil using email, so email is nothing but is an illustration of public cloud. So, this illustration suits for hybrid cloud.

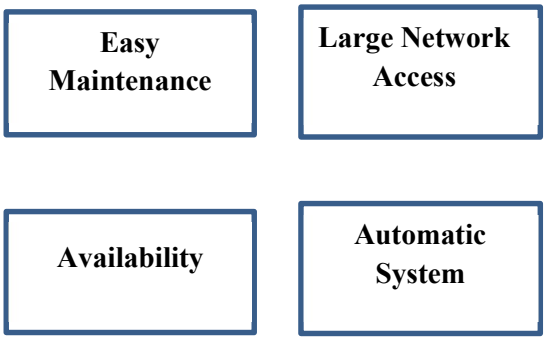


Figure 1: Characteristics of Cloud

Suppose someone is opening an Ecommerce Company and in this Ecommerce company one has some quantum of money and have to maintain the marketing department and the IT infrastructures, but you have a limited quantum of money.so Cloud Computing can help one to manage the sales and market department having limited amount of money. So, in Cloud Computing the cloud is furnishing the IT structure, so now one can concentrate on sales and marketing department. Facebook is an illustration of Cloud Computing.

Security of data on the cloud can be sometimes questionable. Table.1 demonstrates the list of Cloud specific challenges faced by the users and implicit cloud security auditing algorithms. Disadvantages, outgrowths in cloud and need of the security and its challenges are mentions in the given table.

S.No.	Area	Challenges
1	Disadvantes	A) Lack of Control execution, Financial and Solution Controls Are Several situations of Controls has to be Considered in Cloud. B) Security Management Explores the Difficulties of Securing Data and Information of The user C) server unavailabity If A server Goes Down server Does Not Have Direct Access to Its Data Stored in The Cloud. D) Limited Features Features Depends on The Plan the user Has Chosen. E) Shared Access Single Software Serves Multiple customers F) Access Control Regulates Who Can View or Use resources on Cloud.
2	Outgrowths in cloud	A) Loss of Data (2) Data Is Destroyed by Failure in Storage or Processing. B) Data Breaches Sensitive or Confidential Data Is Stolen by Unauthorized user. C) Insecure Interface Reliance on Week Set of Interfaces Leads to colourful Security Issues. D)

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

		Account Hacking cloud Is A Growing Target for Cyber attackers Because Of Valuable Data.
3	Need of the security	A) Security of Data Broad Set of Controls Used to cover the Confidential Data Stored in The Cloud. B) Protection of Network Ensuring Data Confidentiality of Organization Proper Access Control.
4	Challenges	A) cloud Responsibility Holistic Approach to Achieve Trust and Security in Cloud. B) Data Integrity Constancy of Data Stored in The Cloud. C) cloud Confidentiality Provides Access to Sensitive and Protected Data Authorized user. D) threats Cyber-Attacks, inside threats, Legal Liability and Lack of Support E) Cloud Integrity ensuring That the Data Is Accurate and shielded the Data.

B. Architecture

Babul and Kumar explained the three main service in Cloud Computing are SAAS which is software as a service. also, there is PAAS which means software as a service and IAAS which means Infrastructure as a service. IAAS Structure as- an Administration is accessible in the base caste, where all resources are amassed and supervised physically. PAAS Programming as- an Administration arranges in the best position, in which a cloud provider also restrains client versatility by basically furnishing programming uses as an association.

For illustration: Google provides the platform for execution of the java programme, so the user is writing the Java programme but doesn't have the platform for execution of the law. So, the user is giving the law to google for execution of the law created by him. SAAS is when a user does not have its own software, this user depends on the companies.

II RISKS IN PUBLIC CLOUD COMPUTING

A. Lack of Control

The data that the user stores in the cloud can come accessible to farther cloud guests than the user want. In some cases, the user deals with the machines, which are controlled by other cloud providers. However, also there is a chance that an unknown person from those third party might have access to the user's particular lines, so if a person is dealing with Cloud Computing in their day-to-day life also the user should put restrictions on what other users are suitable to see in your account, If the user is putting data out there. The possible results overcome this type of problem is when the user does not store important data on cloud or may be the data should be restated. When the user uses cloud services also the service provider is in control and not the user. Hence, he has the capability to go through any user's data without making the user know.

A. Security Management

The other challenge the user has is that a third party manages the factual data in the cloud. If the user accesses the correspondence also the security is not managed by users for the security the user depends on the

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

correspondence company which manages the user's security. The correspondence company makes sure that the user correspondence stays safe and no one gets the information that the user has in the mail.

C. Ownership

Subramanian and Jeyaraj (1) explained that in many big companies and public providers have some clause in their contract that the data stored in the cloud is the providers and not the consumers. therefore, they have the power to search costumer data to produce new openings for themselves. There are so many cases when the cloud provider goes out of business and sell their costumer data as a part of asset to other companies. They search costumer data to find opportunities to earn some spare money. So always choose a reliable service provider as your stored data could be in a trouble.

D. Data Not Secured

In this paper that sometimes the data stored in the cloud might not be in safe hands because as we are dependent on the service provider and if the service provider is not reliable, also they can pierce your particular information. sometimes the service provider might gain access to your particular information and sell them to other companies to make profit which is a big trouble in the public Cloud Computing.

E. Server Unavailability

In this paper on Cloud Computing security risks and responses explained about the problem's user face when the server in not available Now the severs the service provider uses to store the data of the user in the cloud may be located nearly else or far down from the user. In that, unambiguous case the user may not have control if a problem occurs with that server. Like if a server goes down, loses power a hard drive fails or perhaps the user gets locked out from its account, also the user doesn't have a direct access or be suitable to resolve that particular problem or issue, just because it's in the cloud doesn't means that the data is always available to the user. There are still people who are managing the mechanical system and sometimes cloud creates conclusion and alleges for the user. As ultimately there is the trouble from the association not having the access to the user's system, if that occurs also the user needs to have an understanding what that means.

F. Strong Connection

In this paper explained about the strong connection of internet demanded for the data stored in the cloud. Therefore, if the user needs to access our stored data in the cloud also, we need a constant, a strong connection as it's online, and is each done over the internet. If a person does not have internet also, he could not access his stored data in the cloud. Hence, the person always needs a stable and a strong internet connection.

G. Limited Features

This means that the features or the storage space depends on the plan you chose given by your service provider. Some people have a better plan and get spare benefits and also some spare storage space. But to get the spare features one need to pay a certain amount of money to the service provider.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

H. Shared Access

In this paper that the most important thing of public Cloud Computing is multitenancy. The meaning of multitenancy is that the users share the same sources like Memory storage, CPU, Namespace, Physical structure. But due to some technical problem or server issue the users private information could be accidentally be leaked to other tenants sharing the resources due to multitenancy in public Cloud Computing..

I. Access Control

The authentication and access control for the Cloud Computing is dependent on the service providers. They only choose the authentication and security demanded to secure one's particular information in the drive. sometimes the service providers might choose a wrong or week authentication or access control which could easily be entered by other users and hackers, which could produce many problems as the user's particular information is being misused by other people due to an authentication and access control.

J. Unauthorized Access

In this paper explained that sometimes the data stored in the cloud might not be in safe hands because as we are dependent on the service provider and if the service provider is not reliable, also they can pierce your particular information. sometimes the service provider may misuse one's data stored in the cloud. The service provider may sell your data to earn gains.

K. User Access Control

Sometimes user's private data in the cloud is given to a third person for some improvement, but it's a big trouble as user do not know how the third person is going to pierce or use your data or may change your data.

L. Regulatory Compliance

It's like if we store our data in the cloud and appendix's the data was changed, also it would not be the responsibility of the service provider and could not be criminated.

III. ISSUES IN SECURITY OF CLOUD COMPUTING

Cloud Computing consists of various technologies and programs to ensure that the data, services and structure protection. The traditional security architecture does not apply because the customer does not enjoy the structure presently. The pivotal point, which needs to be flashed back, is that overall security of the whole cloud-predicated system is equal to its weakest reality. By outsourcing, the user loses control over their data and they have to trust cloud provider storing their data on a remote garçon. The main issues with Cloud Computing are data loss, data breaches, API, account hacking and DOS (denial of service)

Loss of data:

We know that, any breach to a cloud server will affect in data leak for all of the users participating the same database. This generally happens when any malicious activity or any bad actor get in the server and leaks the information

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

IV. NEED FOR SECURITY

The client that are depending on Cloud Computing are principally commensurate to a person depending on exposed transference because it drives one to belief over one who has no access, restrictions what one can send, and topics us to norms and date- books that wouldn't have any critical behaviour if one had their own specific vehicles. The issues to be addressed at this position are Cookie Poisoning, DDoS, Manipulation of hidden field, Attack on wordbook, Google Hacking.

V. CLOUD SECURITY CHALLENGES

Subramanian and Jeyaraj (1), Responsibility of cloud allows the cloud users to insure scores to cover data and are noticed by all who reuse the cloud data. cloud providers give proper control and translucency, over their data. They can access and modernize the data whenever there's a demanded. Data should be protected using strong cloud data encryption ways. There are some data outsource to the cloud by the company are meant to be confined to a particular state or area such confidential or sensitive data is meant to be confined and defined geographical boarders.

Data Integrity: There might be a chance that the data stored in the cloud may suffer some transmission and it may affect in loss of data. So, Regular keep should be done to confirm that data is safe.

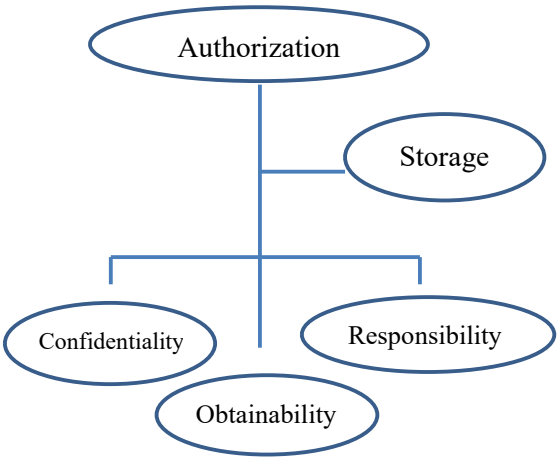


Figure 2: Security Attributes

Data loss: The SAAS platform is delivered to the clients with vast data. Due to Unreliability of the cloud, the data can be lost or manipulate during the process of data Integrity.

A. Cloud Confidentiality

In their paper that Secrecy is characterized as the evidence that touchy data is not unveiled to unapproved people, procedures, or widgets. i.e., customer's information and computation errands are reserved classified from both the cloud dealer and different clients. Privacy is one of the topmost worries with respect to circulated computing.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

This is to a great extent as of the way that clients outsource their material and computation assignments on cloud servers, organized and overseen by deceitful cloud suppliers.

B. Threats

Cross-VM ambush looks at how others may harm intimately cloud customers that co-staying with the reversal, despite the way that it is not the fundamental hazard can apply strikes by getting to the recall of client's VMs. For case, Xen get to engages a sysadmin to explicitly get to the VM. Advantaged frame director of the cloud donator reminiscence Protection strategies.

C. Protection Ideas

To drop hazard began by participated frame, couple of proposals are made to shield the assault in every progression are given in. For illustration, cloud suppliers might jumble cohome by not letting Dom0 to reply in trace route, as well as by arbitrarily appointing inner Internet Protocol to propel VMs. To lessen the achievement chance of arrangement, cloud suppliers may give clients a chance to select the position to place their VMs; be that as it may, this fashion doesn't keep a savage power procedure.

D. Integrity of Cloud

Babul and Kumar explained the prospect of uprightness in circulated figuring enterprises the two data trustability and count responsibility. Data proposes the security of data on the servers of clouds, and encroachment (balanced, changed off) is perceived. Count respectability proposes the prospect that ventures are executed without being bended by malware, cloud providers, or distinctive noxious customers, and that any off- base running will be honored.

CONCLUSION

The composition easily outlines that Cloud Computing is a extensively accepted concept for the ease of storing the data, but its biggest reversal is the security issues. Each new advancement has its trends and disadvantages, there are an issue linked with anchoring, coordinating information, that isn't managed by the proprietor of the information. With issues intertwine cloud unwavering quality, cloud secret, cloud availability, cloud protestation. The most important thing in the public Cloud Computing is multitenancy. The meaning of the word is that in a public cloud several users share the same sources like memory, storage etc. Due to some specialized issue or some server problem the user's private information could be accidentally shown to other users participating the resources. So, utmost of these problems could be answered if a user chooses a secured service provider, who's service is good and are giving access to the cloud at a reasonable price. Authentication is important in the Cloud Computing as it implements numerous benefits as well as disadvantages in the cloud. So, everyone should suppose doubly ahead storing data in the clouds. The risks could be reducing by storing your particular data and work data collectively in separate accounts as because of the data stored in the cloud would be more secured. And the alternate thing is to always choose a known and secured service provider.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:9(3), September 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

References:

1. Alini Subramanian, Andrews Jeyaraj, "Recent security challenges in Cloud Computing " Computers & Electrical Engineering, Volume 71, October 2018,Pp. 28- 42.
2. S Selvi, M. Gobi, M. Kanchana, S. Feminary," hyperactive elliptic wind cryptography in multi- security using DNA ways", International Conference on, pp. 934- 939, 2017.
3. Suresh Babul, Maddali M.V.M. Kumar "An effective and Secure Data Storage Operations in Mobile Cloud Computing", 8 August 2015, Pp. 1385- 1386.
4. Priyanka Ora, P.R.,"Data security and Integrity in Cloud Computing RSA partial homomorphic and MD5 cryptography", Computer Communication and Control (IC4) 2015 International Conference on,) Xiaoqi Ma," Security in Cloud Computing", Computational and Information (ICCIS) 2012 Fourth International Conference on, pp. 1069- 1072, 2012.
5. Pritee Parwekar, Prakash Kumar, Mayuri Saxena, Sakshi Saxena," Public auditing cloud data", the Next Generation Information Technology Summit 2014 5th International Conference-,pp. 169- 173, 2014.
6. Fara Yahya, Robert J Walters, Gary B," thing- security factor for security study", Cyber Security of Digital Services (Cyber Security) 2016 International Conference on, pp. 1- 5, 2016.
7. Arpit Gupta, Vaishali Chourey, "Cloud Computing Security & control strategy using tri-language", Control Instrumentation Communication and Computational Technologies (ICCICCT) 2014 International Conference on, pp. 309- 316, 2014 International Conference on, pp. 309- 316, 2014
8. Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi "Security, of sustainable Cloud Computing "Sustainable Computing Informatics and Systems, Volume 19, September 2018, Pp. 174- 184.