A REVIEW ON CLOUD COMPUTING

Gurmeher Singh Puri
Department of Computer Science
Amity University, Uttar Pradesh
NOIDA, India

Ravi Tiwary
Department of Computer science
Amity University, Uttar Pradesh
NOIDA, India

Shipra Shukla
Department of Computer Science
Amity University, Uttar Pradesh
NOIDA, India

Abstract— **Cloud Computing is a network-built handling invention where information is provided to customers on demand. Present Cloud Computing systems holds serious restrictions to protect confidentiality of user's data. Cloud Computing consists of various technologies, policies to ensure data, services and infrastructure protection. The traditional security architecture does not apply because the customer does not own the infrastructure anymore. The report consists of the risks 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 needed 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 intigrity, Cloud Confidentiality.

I. INTRODUCTION

Cloud Computing is a network-built handling invention where information is provided to customers on demand. Cloud Computing is a registering phase for dissemination of advantages and assets that involve structures, programming, applications, introduction and commerce. Distributed computing is a robotic supply of handling assets.

Present Cloud Computing systems poses serious severe restrictions to protect 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 techniques 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 is much cheaper and efficient source to use.

A. Types of Cloud Computing

Public cloud is mostly used by the users and is available to public. Therefore, whenever a type of storage is used by public then it comes under public cloud. For example, 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 is very secured way and everyone login it using different emails and password. There are many risks and advantages using Cloud Computing.

Private cloud is mostly when an organization wants storage. It is a committed storage. So, the major difference between the public and private cloud is that in public cloud many users can share the storage but in private cloud, only independent organization they have dedicated storage.

Hybrid cloud is when any organization uses private cloud plus public cloud is known as hybrid cloud. For example, if one academy wants to store all of its precious videos to a dedicated storage then it would come under private cloud and the academy also replies to the student using email, so email is nothing but is an example of public cloud. So, this example suits for hybrid cloud.

Selvi et al. [3] demonstrated Community cloud as when many organizations which come with one idea that lets buy one storage and let's try to divide the part of storage for us. For example, assume there are three companies which are sharing the storage between them then this is Called the community cloud.

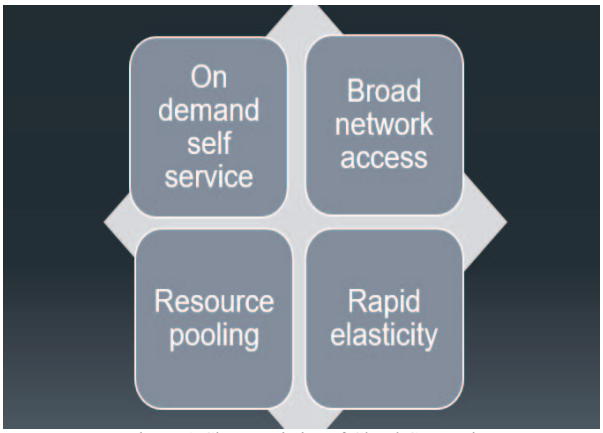

Figure 1 Characteristics of Cloud Computing

Suppose someone is opening an Ecommerce Company and in this Ecommerce company one has some amount of money and have to maintain the marketing department and the IT infrastructures, but you have a limited amount 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 providing the IT infrastructure, so now one can focus on sales and marketing department. Facebook is an example of Cloud Computing.

978-1-5386-5933-5/19/$31.00 ©2019 IEEE

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

Table 1. List of Cloud Challenges

S. No	AREA	CLOUD CHALLENGES
1.	Drawbacks in Cloud	A) Lack of Control [12] Execution, Financial and Solution Controls Are Several Levels of Controls Has to Be Considered in Cloud. B) Security Management [18] Explores the Difficulties of Securing Data and Information of The User C)Server Unavailability [2] If A Server Goes Down User Does Not Have Direct Access to Its Data Stored in The Cloud. D) Limited Features [11] Features Depends on The Plan the User Has Chosen. E) Shared Access [7] [12] Single Software Serves Multiple Customers F) Access Control [10] Regulates Who Can View or Use Resources on Cloud.
2.	Upshots in Cloud	A) Loss of Data [2] Data Is Destroyed by Failure in Storage or Processing. B) Data Breaches [14] Sensitive or Confidential Data Is Stolen by Unauthorized User. C) Insecure Interface [15] Reliance on Week Set of Interfaces Leads to Various Security Issues. D) Account Hacking [9] Cloud Is A Growing Target for Cyber Attackers Because Of Valuable Data.
3.	Need Of Security	A) Security of Data [4] Broad Set of Controls Used to Protect the Confidential Data Stored in The Cloud. B) Protection of Network [17] Ensuring Data Confidentiality of Organization and Ensuring Proper Access Control.
4.	Security Challenges	A) Cloud Accountability [1] Holistic Approach to Achieve Trust and Security in Cloud. B) Data Integrity [5] Accuracy and Constancy of Data Stored in The Cloud. C) Cloud Confidentiality [8] Provides Access to Sensitive and Protected Data Authorized User. D)Threats [17] Cyber-Attacks, Inside Threats, Legal Liability and Lack of Support E) Cloud Integrity [7] Ensuring That the Data Is Accurate and Safeguarded the Data.

B. Architecture

Babul and Kumar [15] explained the three main service in Cloud Computing are SAAS which is software as a service. Then there is PAAS which means software as a service and IAAS which means infrastructure as a service**.**

IAAS Structure as-an Administration is obtainable in the base layer, where all resources are amassed and supervised physically. PAAS Programming as-an Administration arranges in the best level, in which a cloud provider also restrains client versatility by basically providing programming uses as an organization.

For example: 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 code. So, the user is giving the code to google for execution of the code created by him. SAAS is when a user does not have its own software, this user depends on the companies. The companies have their own software. So, tis user is using the company's software with help of an interface. For example: Gmail software it has not been into your mobile, that is nothing but an interface. Google has maintained the Gmail software. So, Google maintains all the software and you are using Gmail with an interface.

II .RISKS IN PUBLIC CLOUD COMPUTING

A. Lack of Control

Kumar and Raj [12] explained the data that the user stores in the cloud can become accessible to more cloud customers than the user want. In some cases, the user deals with the machines, which are controlled by other cloud providers. If the user is putting data out there, then there is a chance that an unknown person from those third party might have access to the user's personal files, so if a person is dealing with Cloud Computing in their day to day life then the user should put restrictions on what other users are able to see in your account. The possible solutions overcome this type of problem is when the user does not store important data on cloud or maybe the data should be encrypted.

When the user uses cloud services then the service provider is in control and not the user. Hence, he has the ability to go through any user's data without making the user know.

User has no guarantee that the service he uses today would be provided to him for the same price. The service provider might double the price at the next moment. The service provider controls all the cloud services and the service provider might make users data hostage if one fails to pay the service provider at a given time.

B. Security Management

The other challenge the user has is that a third party manages the actual data in the cloud. If the user accesses the mail then the security is not managed by users for the security the user depends on the mail company which manages the user's security. The mail company makes sure that the user mail 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 create new opportunities 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 extra money. So always choose a reliable service provider as your stored data could be in a risk.

D. Data Not Secured

Ali et al. [13] explained in their 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, then they can access your personal information. Sometimes the service provider might gain access to your personal information and sell them to other companies to make profit which is a big risk in the public Cloud Computing.

E. Server Unavailability

Sabahi [2] in its paper on Cloud Computing security threats and responses explained about the problem's user face when the server in not available Now the servers the service provider uses to store the data of the user in the cloud maybe located somewhere else or far away from the user. In that, explicit 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, then the user doesn't have a direct access or be able to resolve that particular problem or issue, just because it is 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 stoppage and alleges for the user. As sometime there is the risk from the organization not having the access to the user's system, if that occurs then the user needs to have an understanding what that means.

F. Strong Connection

Ali et al. [13] and Sabahi [2] in their paper explained about the strong connection of internet required for the data stored in the cloud. Therefore, if the user needs to access our stored data in the cloud then we need a constant, a strong connection as it is online, and is all done over the internet. If a person does not have internet then 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 extra benefits and also some extra storage space. But to get the extra features one need to pay a certain amount of money to the service provider.

H. Shared Access

Ma [7] explained in his paper that the most important thing of public Cloud Computing is multitenancy. The meaning of multitenancy is that the user shares the same sources like Memory, storage, CPU, Namespace, Physical building. 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. This one flaw in the server can cause a big problem, could allow other users to see one's personal information, and could misuse one's personal information to earn some benefits.

I. Access Control

Kumar and Raj [12] explained that the authentication and access control for the Cloud Computing is dependent on the service providers. They only choose the authentication and security needed to secure one's personal information in the drive.

Sometimes the service providers might choose a wrong or week authentication or access control which could easily be accessed by other users and hackers, which could create many problems as the user's personal information is being misused by other people due to an authentication and access control.

J. Unauthorized Access

Ma [7] in its 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, then they can access your personal information.

Sometimes the service provider may misuse one's data stored in the cloud. The service provider may sell your data to earn profits.

K. User Access Control

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

L. Regulatory Compliance

It is like if we store our data in the cloud and afterword's the data was changed, then it would not be the responsibility of the service provider and could not be accused.

III. ISSUES IN SECURITY OF CLOUD COMPUTING

Cloud Computing consists of various technologies and policies to ensure that the data, services and infrastructure protection. The traditional security architecture does not apply because the customer does not own the infrastructure anymore. The key point, which needs to be remembered, is that overall security of the whole cloud-based system is equal to its weakest entity. By outsourcing, the user loses control over their data and they have to trust cloud provider storing their data on a remote server. Sabahi [2] explained that Cloud Computing security threats and responses about the security challenges in Cloud Computing and what are the issues affecting the cloud. The main issues with Cloud Computing are data loss, data breaches, API, account hacking and DOS (denial of service).

Loss of data: As the organizations, outsource their entire data to the people who provide service. There are many cases where the user loses his data due to a malicious attack, because of server crashes or because of provider negligence

As we know that, any breach to a cloud server will result in data leak for all of the users sharing the same database. This usually happens when any malicious activity or any bad actor get in the server and leaks the information. Parwekar et al. [9] in their paper "Public auditing: Cloud data storage" explained about account hacking in a cloud.

The mode of interaction between the user and provider is through API with the help of which the client can control and manage the data. The client is accessing the cloud data using a password, which can be stolen or hijacked. It is a serious issue as when an attacker uses all the resources then the other user cannot access their data.

IV.NEED FOR SECURITY

Dai et al. [4] explained that the customer that are depending on Cloud Computing are basically proportionate 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 standards and date-books that wouldn't have any critical behavior if one had their own specific vehicles. Cloud clients aren't careful about the zone of the data and finally need to rely upon the cloud authority association for rehearsing appropriate wellbeing endeavors.

Besides legal security necessities, it is essential to discuss some straightforward security necessities like authentication, Integrity, transparency, confidentiality, availability. Security in application level- Security must be provided to applications in order to stop providing opportunities to stop attackers to gain control over client's private data. The issues to be addressed at this level are:

Cookie Poisoning, DDoS, Manipulation of hidden field, Attack on dictionary, Google Hacking.

V. CLOUD SECURITY CHALLENGES

Subramanian and Jeyaraj [1], Accountability of cloud allows the cloud users to ensure obligations to protect data and are noticed by all who process the cloud data. Cloud providers provide proper control and transparency over their data. They can access and update the data whenever there's a requirement. Data should be protected using strong cloud data encryption techniques. There are some data outsource to the cloud by the company are meant to be restricted to a particular state or area such confidential or sensitive data is meant to be confined and defined geographical boarders. Policies need to be made to ensure the Integrity of such data and ensure the data residency. The enterprise is responsible for any breaches of data and must ensure strict cloud security.

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

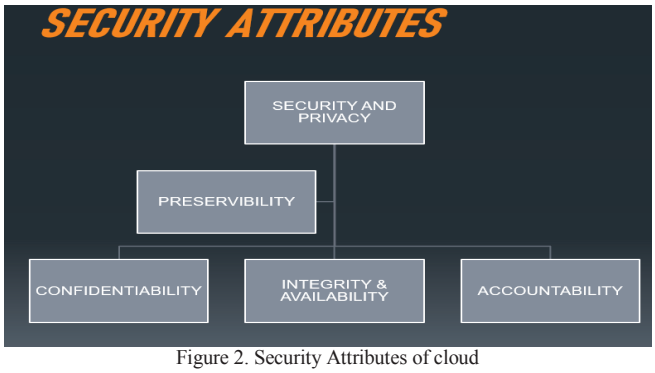

Figure 2. Security Attributes of cloud

The verification of the data Integrity is made at two levels of cloud. There are many ways due to which the data Integrity is impacted due to these two levels. Since Cloud Computing is not only about storage and needs some intense computation to perform its task the user has no way to verify that the data is intact or not.

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

A. Cloud Confidentiality

Amol D and Rastogi [8] explained in their paper that Secrecy is characterized as the confirmation that touchy data isn't unveiled to unapproved people, procedures, or Gadgets. i.e., client's information and calculation errands are reserved classified from both the cloud dealer and different clients. Privacy is one of the greatest worries with respect to circulated computing. This is to a great extent as of the way that clients outsource their material and calculation assignments on cloud servers, organized and overseen by deceitful cloud suppliers.

The specialist co-op recognizes where the clients' classified information is located in the distributed computing frameworks. The specialist organization has the benefit to gather the client's private information. Specialist organization can comprehend the significance of client's information. The authentication and access control for the cloud is dependent on the service providers. The user only chooses the authentication and security needed to secure its data in the cloud.

B. Threats

Cross-VM ambush looks at how others may harm secretly cloud customers that co-staying with the setback, despite the way that it isn't the fundamental hazard can implement strikes by getting to the recall of a customer's VMs. For instance, Xen get to engages a sysadmin to explicitly get to the VM. Advantaged framework administrator of the cloud benefactor reminiscence Protection strategies. Khan [17] explained the threats in Cloud Computing.

There are various possible threats that the mystery files (cash related, prosperity) and individuals' details (singular profile) is unveiled to open or professional contenders. Assurance is a problem of most vital need. All through this

substance, the user sees assurance preservability as the middle quality of security. Two or three security qualities clearly or roundaboutly affect insurance preservability, including protection. Clearly, with a particular ultimate objective to shield private data from being uncovered, mystery winds up vital, and trustworthiness ensures that data/computation isn't corrupted, which by some methods stick security.

Preservability is a strict type of privacy, because of the idea that they avert data spillage. Along these lines, if cloud secrecy is ever disregarded, protection preservability will likewise be damaged. Like other security benefits, the significance of cloud protection is two-crease: information protection and calculation security. It is recommended that Fully Homomorphic Encryption ensure security in spread enlisting. It empowers depend on blended information, which is anchored in the addressed servers of the cloud supplier.

C. Protection Ideas

To decrease hazard began by shared framework, couple of proposals are made to shield the assault in every progression are given in. For example, cloud suppliers might jumble co-home by not letting Dom0 to react in trace route, as well as by arbitrarily appointing inner Internet Protocol to propel VMs. To lessen the achievement percentage of arrangement, cloud suppliers may give clients a chance to select the position to place their VMs; be that as it may, this technique does not keep a savage power procedure.

A definitive preparation of cross-VM assault is to wipe co-residency. Cloud clients (particularly undertakings) may need physical segregation, which can be built into the Administration Level/Stage Assertions (SLAs). To guarantee segregation, a client should be empowered to check its VMs restrictive utilization of a physical engine.

Parwekar et al. [9] in their paper “Public auditing: Cloud data storage”

D. Integrity of Cloud

Babul and Kumar [5] explained the prospect of uprightness in circulated figuring concerns the two data reliability and count trustworthiness. Data genuineness proposes the security of data on the servers of clouds, and encroachment (balanced, exchanged 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 handling will be recognized.

The verification of the data Integrity is made at two levels of cloud. The two levels are the Data Level and the Computation Level. There are many ways due to which the data Integrity is impacted due to these two levels. Since Cloud Computing is not only about storage and needs some intense computation to perform its task the user has no way to verify that the data is intact or not. The SAAS platform is delivered to the clients with vast data. Due to Unreliability of the cloud, the data can be misplaced or manipulate during the process of data Integrity.

Preservability is a strict type of privacy, because of the idea that they avert data spillage. Along these lines, if cloud secrecy is ever disregarded, protection preservability will likewise be damaged. Like other security benefits, the significance of cloud protection is two-crease: information protection and calculation security. It is recommended that Encryption ensure security in spread enlisting. It empowers depend on blended information, which is anchored in the addressed servers of the cloud supplier.

CONCLUSION

The article clearly outlines that Cloud Computing is a widely accepted concept for the ease of storing the data, but its biggest setback is the security issues. Each new advancement has its upsides and disadvantages, there are an issue identified with anchoring, coordinating information, that isn’t managed by the owner of the information. With issues intertwine cloud unwavering quality, cloud secret, cloud accessibility, cloud affirmation. 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 technical issue or some server problem the user’s private information could be accidentally shown to other users sharing the resources. So, most of these problems could be solved 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 many benefits as well as disadvantages in the cloud. So, everyone should think twice before storing data in the cloud. The risks could be reducing by storing your personal data and work data individually in separate accounts as because of the data stored in the cloud would be more secured. And the second thing is to always choose a known and secured service provider. Then again, reliability of cloud is endangered because of the hardship and degenerate figuring in remote servers. Proper data ownership services should be used Lastly proper management strategies and keeping checks on the employees are the measures to secure data in hybrid Cloud Computing.

REFRENCES

[1] Nalini Subramanian, Andrews Jeyaraj, “Recent security challenges in Cloud Computing “Computers& Electrical Engineering, Volume 71, October 2018, Pp. 28-42.

[2] F. Sabahi, “Cloud Computing security threats and responses,” in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011 pp. 246-248.

[3] S Selvi, M. Gobi, M. Kanchana, S. Femina Mary, "Hyper elliptic curve cryptography in multi cloud-security using DNA (genetic) techniques", *Computing Methodologies and Communication (ICCMC) 2017 International Conference on*, pp. 934-939, 2017.

[4] Qinyun Dai, Haijun Yang, Qinfeng Yao, Yaliang Chen, "An improved security service scheme in mobile cloud environment", *Cloud Computing and Intelligent Systems (CCIS) 2012 IEEE 2nd International Conference on*vol.01, pp. 407-412, 2012.

[5] Suresh Babul, Maddali M. V. M. Kumar “An Efficient and Secure Data Storage Operations in Mobile Cloud Computing”,8 August 2015, Pp.1385-1386

[6] Priyanka Ora, P. R. Pal, "Data security and Integrity in Cloud Computing based on RSA partial homomorphic and MD5 cryptography", *Computer Communication and Control (IC4) 2015 International Conference on*, pp. 1-6, 2015.

[7] Xiaoqi Ma, "Security Concerns in Cloud Computing", *Computational and Information Sciences (ICCIS) 2012 Fourth International Conference on*, pp. 1069-1072, 2012.

[8] Wale Amol D., Vedant Rastogi, "Data Integrity Auditing of Cloud Storage". International Journal of Computer Applications (0975 – 8887) Volume 133 – No.17, January 2016.

[9] Pritee Parwekar, Prakash Kumar, Mayuri Saxena, Sakshi Saxena, "Public auditing: Cloud data storage", *Confluence the Next Generation Information Technology Summit (Confluence) 2014 5th International Conference* -, pp. 169-173, 2014.

[10] Fara Yahya, Robert J Walters, Gary B Wills, "Goal-based security components for cloud storage security framework: a preliminary study", *Cyber Security and Protection of Digital Services (Cyber Security) 2016 International Conference on*, pp. 1-5, 2016.

[11] Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi "Security, privacy & efficiency of sustainable Cloud Computing "Sustainable Computing: Informatics and Systems, Volume 19, September 2018, Pp. 174-184.

[12] P. Ravi Kumar, P. Herbert Raj, P. Jelciana "Exploring Data Security Issues and Solutions in Cloud Computing "Procedia Computer Science, Volume 125, December 2017, Pp. 691-697.

[13] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos "Security in Cloud Computing: Opportunities and challenges" Information Sciences, Volume 305, 1 June 2015, Pg.: 357-383

[14] Ashish Singh, Kakali Chatterjee "Cloud security issues and challenges": pp. 88-115 Volume 79, February 2017.

[15] Kumar Parasuraman, P. Srinivasababu, S. Rajula Angelin, T. Arumuga Maria Devi, "Secured document management through a third-party auditor scheme in Cloud Computing", *Electronics Communication and Computational Engineering (ICECCE) 2014 International Conference on*, pp. 109-118, 2014.

[16] Basel Saleh Al-Attab, H. S. Fadewar, "Authentication scheme for insecure networks in Cloud Computing", *Global Trends in Signal Processing Information Computing and Communication (ICGTSPICC) 2016 International Conference on*, pp. 158-163, 2016.

[17] Minhaj Ahmad Khan "A survey of security issues for Cloud Computing "Journal of Network and Computer Applications, Volume 71, August 2016, Pp. 11-29.

[18] Arpit Gupta, Vaishali Chourey, "Cloud Computing: Security threats & control strategy using tri-mechanism", *Control Instrumentation Communication and Computational Technologies (ICCICCT) 2014 International Conference on*, pp. 309-316, 2014.