Cloud Computing Scheduling Algorithms and Resource Sharing

Dr. Mayuri Desai
Assistant Professor, Amity Institute of Information Technology, Amity University Noida Campus, India

Corresponding Author: mayuridesai911@amity.in

Received: 16-08-2023 Revised: 03-09-2023 Accepted: 24-09-2023

ABSTRACT
A flexible, affordable, and trustworthy platform for delivering IT services to customers or businesses online is cloud computing. It is a collection of applications, infrastructure, distributed services, and information. It is described as a collection of services that offer internet-based infrastructure resources and data storage on a third server. In comparison to other infrastructure, it offers its users scalability, dependability, high performance, and an affordable option. However, because crucial services are frequently contracted out to a third party, it is more difficult to ensure data security and privacy, support data and service availability, and mitigate risk associated with cloud computing. With relation to cloud-connected automobiles, we examine here vulnerabilities, related dangers, and potential solutions for assessing algorithms.

Keywords: *scheduling, cloud computing, sharing, resources*

I. INTRODUCTION

A study by Gartner considered Cloud Computing as the first among the top 10 most important technologies and with a better prospect in coming years by almost all companies and organizations.

Cloud computing is now known for accessing resources from a pool which is owned and maintained by a third party vendor using internet. It is a technology which keeps up data using internet and remote servers. In cloud computing generally res88ources are kept in someone else's authority and are accessed remotely by the user. It is a type of computing that depends on sharing of data. The term cloud computing is originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources.

Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service with all computing resources visualized as services and delivered over the Internet. The cloud enhances agility, availability, collaboration, scalability, ability to adapt to fluctuations according to demand, accelerate development work, and provides scope for cost reduction through optimized and efficient computing. While there are many benefits to adopting Cloud Computing and also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters. Security concerns relate to risk areas such as external data storage, lack of control, multi-tenancy, dependency on the "public" internet and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form.

Moving critical applications and sensitive data to public cloud environments is of great concern for those organizations that are moving beyond their data center's network under their control. Connected Vehicles using these data will lead to solutions to many vehicle motions and create a new way of vehicle movement. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors.

If we are talking about the different layers of cloud, the basic cloud management structure can be divided into four basic layers resource & Network Layer, Service Layer, Access layer and User Layer. The basic set of functions performed by each layer is as follows:

- The physical and virtual resources are being managed by the Resource & Network Layer.
- The Service Layer is mainly concerned with the cloud operation function as NaaS, IaaS, PaaS, etc.
- Inter-cloud peering and API termination is done by Access Layer.

- End-user function, Partner function and Administration function is done by User Layer.

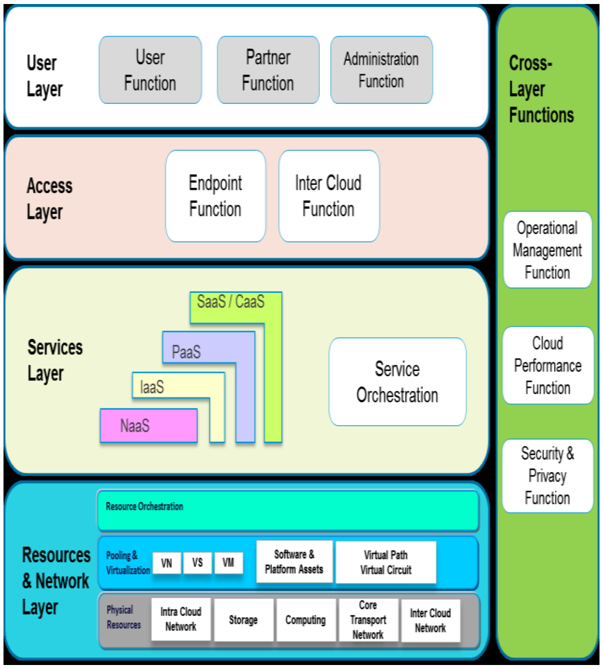

Figure 1: The Cloud Computing Components

Cloud computing is a broad term which is used for hosting services over the internet. The hosted services can be divided into three main broad categories:
Infrastructure As A Service (IAAS),
Platform As A Service (PAAS) and
Software As A Service (SAAS).

Infrastructure As A Service (IAAS)

According to Internet Engineering Task Force (IETF) it is the most basic cloud service provider. This service is also referred as the cloud resource which is mainly used to provide resource which can be easily managed with a different variety of users. IAAS provides the users online services which keep the users isolated from the details of the basic properties like basic computing resources, location, data partitioning, scaling and security, backup etc.

Platform As A Service (PAAS)

Paas is a service on cloud computing that provides the users a platform to build their applications. This service provide user to develop applications using tools supplied by provider. Using PAAS user can subscribe to different kinds of pre subscribed services. Adaptability, Security and Flexibility are the major benefits for user while using PAAS services.

Software As A Service (SAAS)

In this process the users can use the different services provided by the vendors on the cloud using pay per use basis. It is also known to the user as "on-demand software". It is known as a well known application for many official needs as payroll, database, messaging software etc, The main examples of the providers using this service are Google, Gmail etc.
In today's scenario cloud computing is gaining its importance day by day among the different users. Almost all of the organizations are using the cloud via Internet. The main reason behind shifting everything to cloud is safety and security. It is an important thing for cloud service providers that whatever information is being saved on cloud must not fall in the hands of the hackers.

II. THREATS FOR CLOUD SERVICE USERS

In this section firstly we are going to discuss the basic threats to cloud security, later we will discuss the threats related to cloud service providers (CSP) and cloud service customers (CSC).

Security Issues: the several security issues are of concern to the cloud service users.

Privacy

Privacy is the most emerging issue while discussing the data and network. It is a aspect of security which is always expected by CSC on an absolute level. It ensures CSC that its data and information will not be leaked and will not go in unwanted hands and remain secure. For this method several encryption and decryption keys are being used to make the data secure. The encryption process is required even if we are saving multiple copies of the data at several locations. In privacy we have one more type of threat known as insider threat. In this threat the insider can easily access the data and information of the user saved in cloud

Confidentiality

It is one of the major aspects while discussing cloud security. In cloud it is essential that all the Information of a user remain confidential from the rest of the users as the data moves between different communication channels. The data must be secured using end to end encryption scheme and client server authentication ensuring no leakage of data.

Integrity

Integrity is the process in which modification or changes in data are not allowed while travelling from source to destination. In the transfer, storage and retrieval of data integrity must be maintained.

Protection

Cloud has an immense amount of data for storage do it is very important to protect the data from the outside vendors. Data isolation is a major factor that needs to be maintained in using cloud computing. The data is generally associated with virtual machines if we need to maintain data isolation.

Identity Management

It is an important factor while discussing authentication, authorization and access control of data. It is always assumed that the service providers provide “principle of least privilege” to the data stored. According to the “principle of least privilege” only least access to perform any particular operation is granted to the data and the access is granted for minimum amount of time.

Security

It is needed in every enterprise that the data must be protected wherever it is stored. The organizations can go for encryption and other security measures for securing the data and information. To secure the data the data must not be allowed to the outside vendors. Also it may not be allowed to be used by the unknown persons.

III. MAJOR SECURITY RISK IN CLOUD

The major security risks involved vary from different models depending upon the asset information, architecture of cloud and security involved in the cloud. Major security risks involved in cloud computing are described as follows:

Privileged User Access

The data is stored in the cloud to provide proper access to the user with the major security means. Encryption is the major method used for securing the data and protecting it from the hackers. Data confidentiality is the major factor which needs to be maintained in the cloud. The cloud provides unlimited store and access to the data by the user. Sensitive data processed outside any organization is the major factor of risk in the cloud. Encryption technology is also restricted based upon the type of data and information being used by the provider. It is always mandatory in cloud that data must be reviewed properly that it is properly encrypted or not.

Data Location and Segregation

Data location and segregation are the major factors while discussing cloud computing. The major risk associated in the situation is as follows:

i. The cloud provider is basically used to disclose the information and hand over the physical media to a third party vendor.
ii. The liabilities of paying tax to local authorities are the result of processing sales and other jurisdiction.
iii. The customer's security is also affected by the natural calamities like earthquake, flooding and extreme weather conditions.
iv. Some of the providers' conditions are also affected by the macroeconomic hazards as hyperinflation or deep recession.

The data which is stored in the central server is also considered as the main source of attack for the attackers. In a simple single attack the attacker can gain access to the rich source of the confidential information which belongs to the several customers' organizations. Sagaration of the data is equally important as if the process of Saga ration is not applied most of the customers suffer from security deficiency as a single customer.

Virtualization is the technology enabling the cloud computing as one of the method of data processing which is used in data segregation. Major security issues are related with the adequate security controls. Hypervisor layer is used to gain access between hardware and virtual machine.

Data Disposal

Cloud computing basically provides high level availability of data. This facility is provided by cloud providers by creating multiple copies of data. If the cloud customer wants to delete the data from a particular point it becomes difficult for the data to be deleted from each end and server.

Deleting of data sometimes depend upon the type of data hosted in the cloud. The providers are required to delete the data in accordance with the industry standards.

E-Investigation

Implementation of protective monitoring efforts by the user is an important effort by the user while discussing cloud. There is always a risk of malicious insiders and the monitoring and e-investigation process is always required for making the data secure.

Effective monitoring of cloud is required to maintain integrity between the cloud provider and the cloud user. Managing identity and user access in cloud is an important factor required in integration and pre-identity management of the cloud system. Protection of the identity is maintained and done in cloud in order to trace the identity of cloud and customer in the cloud computing environment

IV. CLASSIFICATION OF SECURITY ISSUES IN CLOUD COMPUTING

The security issues used in cloud can be categorized as follows:

These methods were the least possible and least easy for moving a service provider to the cloud. The major concerns in this cloud category are as follows:

VM Level Attacks

This technology is used by the cloud computing vendors in multi-tenant architecture. Attacks on virtual machines are most common in cloud computing data. The work for the researcher is to just places the data inside the virtual machines and to watch the simple behaviour of the data that how it works. Once the analysis of the data is complete then the work on data can be performed.

Phishing

Phishing is major attempt to acquire sensitive information as user name, passwords and other confidential information of the user. It is a kind of fraud in which the attacker tries to learns the information through the other communication channels.

Forensics in Cloud

Cloud forensics is the use of digital forensics in cloud computing as a subset of network forensics. It is a cross discipline between cloud computing and digital forensics. Digital forensics is the application of science to identification, examination, collection and analysis of data while preserving the information and maintaining a strict chain of custody for the data. Cloud computing is based on broad network access which follow the main principles found in the main network.

Auditability

The difficulty in audit is the problem concerned with lack of problem. The major factor discussed in this problem is transparency of data. The transparency is provided in the documentation and manual audits. Audit maintenance is a major factor in maintaining a onsite global system. Certain regulations are being implied to perform operations at certain geographic locations.

V. DATA INVESTIGATION TOOLS

Viivo

Viivo is a software development tool which is developed by PKWARE invented in 1986. It is developed as a free encryption service which is used to make the process of encryption easy. It is the best standard used on the multiple platforms to encrypt the data. Synchronization is the process which is used to secure the documents by transferring data to the Drop box or Drive. In this method server never copies data to the cloud. It uses a multi level encryption standard which secures all the files on the secured level. This method uses RSA standard where data is secured by using a public keys where the secret key is known to the user.

The main advantage of this method is the data is synchronized before it is compressed to the cloud. It has multi cloud support system where data is shared among all common clouds. The main disadvantage of this data method is the tool is visible to all the attackers where the information is shown to the attacker that which tool is used to encrypt the given data. The second main disadvantage with the tool is that the extension of file .viivo is always shown to the given attacker.

Skycrypt

This security method is used to secure data on local cloud providers and local files. It is the latest solution which is used for data encryption of cloud providers and local files. Here in this system the files are encrypted on the desktop before uploading the files on the server. The main advantage of this method is transparency which is used to encrypt the files. In this method two-factor authentication. Local encryption and decryption method used in this method. This method can be used to connected two or more pc's. The disadvantage is that only encrypted files can be shared with this method. In this method mobile or MAC method is not provided. To share any resource the security question and the password is provided to the recipient.

Tools	Security Concerns	Protection Mechanism	Features
Viivo	-Privacy -Integrity -Confidentiality	-Public Key Cryptography -Folder Sharing -File Encryption	-Extended Customer Support -Compression -Multi Cloud Support -Right management -Mobile Encryption
SkyCrypt	-Confidentiality -Integrity -Privacy	-AES bit encryption -Invisibility mechanism for folder	-Fully Compatible -Free one time password -Encryption is easy
CipherCloud	-Privacy -Data Privacy -Residency -Regulatory compliance	-Encryption- AES256 bit -Tokenization -Cloud discovery	-Encryption -Tokenization option -Enterprise key management -High performance architecture -Multi-organization support
Bitglass	-Privacy -Transparency -Mobility	-Single sign-on (SSO) -AES 256-bit encryption	-Discover Shadow IT -Detailed cloud application analysis -Ease of deployment -Control Shadow IT
Skyhigh	- Privacy -Regulatory policies	-Unstructured data encryption -Selective encryption -Format preserving Encryption -Searchable encryption -Order preserving encryption	- Contextual Access Control - Application Auditing - Encryption - Cloud LP - Cloud – to - Cloud Control

Ciphercloud

This method is used to encrypt the data directly at the business gateway. This method used to encrypt data during uploading process and decrypt during downloading. This method also comes with built-in malware detection and data loss prevention. The main advantages with this method are enforcing data loss prevention, delivering malware detection, activity monitoring, retaining usability and functionality, maintaining the existing infrastructure. The main disadvantage of this method is it doesn’t provide semantic security.

Bitglass

It is a method founded in 2013 by a team of industry veterans with a proven record of innovation and execution. It provides transparent protection for the data. It reduces the risk of data loss and maintains data visibility among the users. The main advantage with this method is it is available free of cost for files up to 1 GB. The major disadvantage with this method is this method is expensive and basically provides services to big enterprise only.

Skyhigh

This method secures cloud application. This method is a control point for cloud servers which enable enterprise to gain visibility into cloud usage and risks. The advantage is it providing governance to the data in all the fields including custom fields. The main disadvantage is service is provided only in private clouds.

VI. CONCLUSION

Although cloud computing is not a new idea and offers plenty of advantages to consumers, the security of cloud data is the key issue holding back its widespread use and dependability. By embracing the obstacles presented to it, the techniques addressed in the paper increase the security of cloud data. The main security concerns and the technologies used to secure the data in the cloud infrastructure based environment have been described in this paper. The tools mentioned play a significant role in both data security and data prevention. The best possible data protection is achieved with these techniques. The study provides a fundamental analysis of the tools that are employed to safeguard data in the cloud. For enterprises that are expanding outside of their data center's network under their control, shifting sensitive data and important applications to public cloud environments is a major source of anxiety. Additionally, using these data from the cloud, connected vehicles will establish a new way for vehicles to travel and provide better, more secure, and efficient access to the cloud data used in various computing elements. In order to allay these worries, a cloud solution provider must guarantee that clients will continue to enjoy the same security and privacy protections for their applications and services. Clients must also be given proof that their businesses are secure, capable of meeting service level agreements, and able to demonstrate compliance to auditors. This will enable a better comprehension and effectiveness of cloud computing.

REFERENCES

1. Backialalshmi.M. (2016). Survey on scheduling algorithms in cloud computing. *IJERS, 2*(6), 2091-2730.
2. Dr. S.K. Singh. (2016). Analysis of security issues in cloud connected vehicles within cloud security threats and computing challenges. *International Journal of Engineering and Management Research, 6*(4), 433-437.
3. Pallavi Marathe. (2015). *Cloud computing security threats and tools*.
4. T Amith Kumar. (2014). Trustworthy resource sharing on collaborative cloud computing. *IJCSIT, 6*(3).
5. Kangchan Lee. (2016). Security threats in Cloud Computing Environment. *IJSIA, 6*(4).
6. http://en.wikipedia.org/wiki/Cloud_computing.
7. Rashmi Nigoti. (2016). A survey of cryptographic algorithms for cloud computing. *IJETCAS*.