"A Survey for Secure Cloud Replication in Private Cloud Environment "

Shweta Shah[1] ,Sumeet Kothari [2] ,Arpit Agrawal [3],Ashish Soni [4]
Computer Engineering
Institute of Engineering & Technology
Indore, India

Abstract: Cloud compute may be know-how enables to percentage useful resource, services and platform with every other person. This is often the generation wont to planned widespread amount of records and more than one service for set up opportune manner of statement and implementation. In smooth words, cloud computing understanding make viable to get entry to offerings and supply even as now not installing or configuring into local system. It affords and platform to get entry to common laptop code and operating out surroundings at single purpose and simple focus coping with.
Keywords: Cryptography, SaaS Model, Reliability.

1 INTRODUCTION

Cloud computing understanding is seen because the hodgepodge of net base more frequently than no longer services for better utilize the wherewithal and offerings. It's the new usefulness that provides virtualization, equal and concentrated compute into on its personal element. It implies the distribution of assets to handle software with reduce funding and coffee renovation significance. It presents multiply quantifiability and smooth proper to apply excellent with low complexness.

Cloud compute is outline "a reproduction for sanctionative omnipresent, unlucky, on lay down complicated manner in to a shared organization of property (e.g., network, garage, applications and offerings)"

The cloud version consists of five vital traits and 3 carrier model. Cloud computing is generation that is not product but pretty provider provision. It's the combination of computing and offerings. It believes in something –anywhere idea and presents offerings thru net at single browser. Five necessary fundamentals of cloud environment are listed below;

1. Statistics: It the congregation of matter which can be obliging may not.

2. Garbage area: this is often the based set of statistics for clear-cut access, replace and supervision cause. It considers datacenters, disk, and taps for storage reason and data servers for involvement of records.

3 Purchaser Networks: It includes plentiful campaign like organizer, reasonable handset, I-telephone, laptop, laptops and so on. it have to non-public as transportable client, presume and thick purchaser**.**

4. Packages & compute:

Applications location unit the man or women or system advanced compute time table enables to persuade the need and implementation of venture. Further, it desires Computing, that is that the purpose of head movement making collection of steps maltreatment algorithms**.**

5. Virtualization:

It's far the creation of digital edition in place of actual. It facilitates to get entry to assets and services. A block instance of element layout of cloud computing is proven in discern one.

Figure 1: Cloud Computing Elements

The cloud computing surroundings perpetually enforced with the assistance of cloud services. It is delineate as follows.

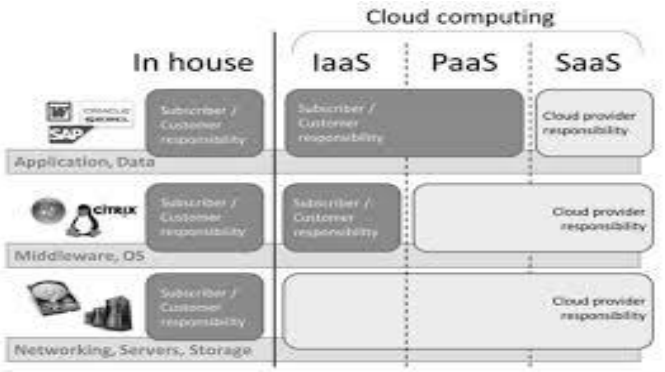


Figure 2: Cloud computing services

1. Computer code as a Service [Saas]: This provider configures get entry to of computer coverage and functions for our network. it's miles accessed through browser of mention as primary processing unit rules (codes) on insist facility[1] [1].

2. Platform as a Service [Paas]: A collection of libraries, runtime surrounds, development languages, and device laptop code should understand because the platform. This provider allows to get entry to platform in addition to implementation environment mistreatment net offerings.

3. Infrastructure as a service[IaaS]: Infrastructure may want to reflect on consideration on due to the fact the storage area or method ability of the node. IaaS gives facility to contribute to assets and install purpose as price computing.

Cloud computing prepared fashions: cloud services place unit typically usual obtainable to its customer through type of cloud. a petite assessment of forms of cloud is referred to under

Non-public [confidential] Cloud: It delimits the services absolute and get admission to up-to constrained group place unit. It in hand keeps as well as proper of access via unmarried agency and deployed amongst pc network. Customers along with the alliance will use the data, accessible offerings and different software.-+

Public Cloud: This kind of cloud needed accomplishment of cloud offerings exploitation net facility. It must very own by way of single person even though presents facility for everyday public conjointly Throughout this all services place unit available and any person gets the ones services with the aid of paying satisfactory amount.

Network Cloud: it is in hand and maintained by using a corporation for a particular institution of people. This cloud can be collective by several affiliations for any unambiguous reason, almost without a doubt it manage via internally or externally, in phrases of fee it is less expensive than now not public but dearer than public.

Hybrid Cloud - This type of cloud may be a mixture of two or additional clouds (for example combining public and community clouds) [2].

Hybrid Cloud - this sort of cloud may be a combination of 2 or additional clouds (for example combining public and community clouds)

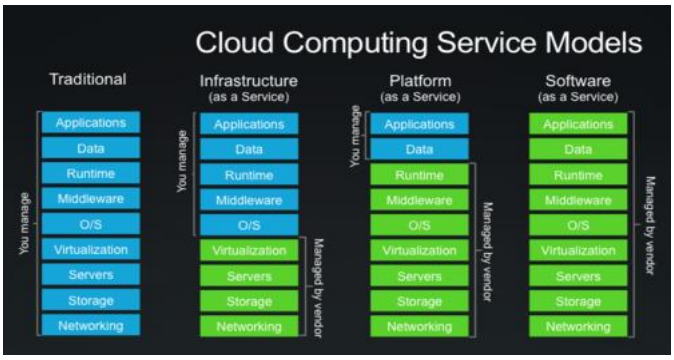


Figure 3: Cloud Computing Service model.

2 RELATED WORKS

K. Nasin, et. al. [1 explores that cloud frameworks is one a number of the maximum essential utility phenomena for these days's development. right here, they explores the latest troubles and deal with protection due to the truth the one most of the most essential challenge for cloud computing. assurance concerning safety offerings no longer absolutely allows to hold up privacy and originality of facts but maintains man or woman recollect on carrier companies. To implement the protection mechanism with cloud environment they uses AES and RSA algorithmic rule with key sharing mechanism. AES may be a bilaterally symmetric key algorithms wont to generate non-public key for RSA algorithms. moreover, RSA helps variable key duration with robust technological know-how algorithmic rule. eventually, they completely concentrate on relaxed report communique and be triumphant to obtain confidentiality with cloud packages

.Chen, D.[2] et. al. address that info security have an effect on the performance of cloud applications and should degrade the standard of service execution. Opponent could explore the vulnerabilities and deploy security threats or sniffing activity to compromise the privacy of the communication. So, to keep up the user trust and reliableness on services similarly improvement into quality of services execution, a implementation of security model is necessary. Finally, they compare their resolution with airawet framework and take a look at to cut back info run issue.

Jayant, D. [3] projected a access management resolution mistreatment RBAC theme through AES and RSA algorithmic rule. Here, they uses RSA and AES model for secret writing and decoding purpose wherever RBAC is employed for access management purpose. It provides the uploading rights and totally different completely different} rights to different user as per RBAC model.

Cindhamani.J et. al. [4] address that there's sturdy got to revised the information security style and add security because the integrated element of cloud surroundings. They uses a 128-bit key for RSA algorithmic rule and third party auditor to stay safe eye of authentication and verification method. Here, deployed resolution improves the protection feature into 2 ways in which one is storage finish and another is access of knowledge.

Shilpi Singh et al[5] projected security through elliptic curve science algorithmic rule. User initial logins into the server and certify himself. Afterwards, 2 exchanges happened with ECDH key exchange and bilaterally symmetric key algorithmic rule to write in code and rewrite the information. a 1 Time parole technique is additionally used for sturdy authentication purpose.

Kawser Wazed Nafi et al[6] conjointly projected a security framework similar with higher than researchers. they need conjointly projected OTP mechanism and security services for secure communication.

3. SECURITY CHALLENGES

Internet is that the key bone for Cloud computing surroundings and purpose area unit deploy all the way through public networks. With cloud application, association will use services in addition to data from any objective location. Outside access is also apprehensive and lifts question about privacy, privacy, dependability etc and demand responsible compute surroundings whereby knowledge privacy, verification with access managing is maintained [3].
The study of complete cloud environment raises sure problems which can be listed below;

- Data protection
- Identity and access managing
- Key managing
- Virtual mechanism security

Among these main security problems within the cloud, knowledge security and integrity is believed to be the foremost tough drawback that may limit the employ of cloud compute. In fact, access management and key management area unit all problems anxious in data security.

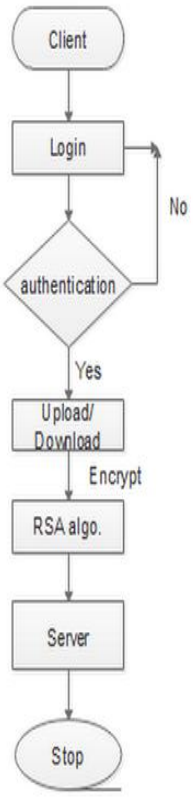
considerate of protection threats in cloud computing environment for analyze the requirement of protection, in no doubt precautions threats area unit unwavering those area unit demarcate into Table 1.

Table 1: Security Threats in Cloud Environment

Attack	Description
Data breaches	When a data breach occurs, companies may incur fines, or they may face lawsuits
Hacked interfaces and APIs	Apis and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet
Account hijacking	Attackers can eavesdrop on activities,manipulate transactions, and modify data.
Malicious insiders	The insider threat has many faces: a current or former employee,a system administrator, a contractor, or a business partner
Inadequate diligence	Operational and architectural issues arise.
Cloud service abuses	Cloud computing resources to break an encryption key in order to launch an attack.
DoS attacks	Consume large amounts of processing power

4. PROBLEM STATEMENT

Cloud computing environment have huge software space and ought to install with varied motive. even though, security was primary issue in view that origin of web because of its public association, it will become extraordinarily vital because of involvement of net with cloud computing. Cloud computing



gives extensive computing nature environment with disbursed garage with parallel execution facility. It wishes internet to reinforce its scope from computer community to international and uses internet services to get admission to cloud application from outdoor the network.

- Any employer or laptop node that method statistics through public network is situation for protection breach and ought to be goal for varied protection threats and attackers. It creates perplexity in consumer's thoughts concerning the agree with and privateness of know-how. Any consumer who get admission to or store their steering exploitation cloud packages invariably needed assurance concerning protection and protection of content material.
- The observe of complete current device discover that, existing answers gives protection however either one or 2 stage. they're doing now not offers complete security version or framework to integrate protection with cloud programs. They cope with an exceptionally sturdy need of security model that must give security not due to the fact the call for but as vital detail of software. Following predominant troubles has been discovered all through the have a look at [4].

Figure 3: FLOW CHART

Following main issues has been located in cloud environment.

- lack of safety provision at some point of communiqué.
- privateness is major requirement and challenge for user.
- A green storage approach and higher integrity verification is required in new answer.

5. SOLUTION STATEMENT

A disseminated atmosphere increases kind of safekeeping problems. First, the published nature of most local area networks makes them extensively vulnerable to eavesdrop. Anyone with a personal virtual pc on correlate LAN will essentially supervise all network passage. Secondly, the dearth of handling over the guidelines run in a non-public digital pc makes masquerade, replay, and comparable active threats potential [5, 6, and 7]. These troubles square calculate solved in single-device or principal environment by means of great safety: bolt gadget rooms and watched over terminal lines. Unluckily, the suburbanized nature of disseminated structures precludes such measures. Logical in place of physical schemes have to be used as an alternative. The handiest poor component to unravel is that of eavesdropping. The solution makes use of encryption: 2 individuals need to talk achieve this through encrypting all their messages with a secret key illustrious totally to them. This correctly constructs a at ease non-public channel on high of the underlying insecure public channel.

Certain steps are worried to attract proposed concept into physical way. A Java based totally application has been evolved with replication idea and safety concepts. A mysql Database has been used to design backend of the assignment [8,9,10].

The complete scenario is urbanized into three Modules which are listed below;

Module 1: Client End

Java based upload file relevance has been developed to select and upload text file and forward to Main Server or Master Server for protected duplication and endorsement purpose[11,12,13].

Module 2: Master Server / Distributed Server

This unit is accountable for in receipt of the text file from consumer end and groundwork of reliability verification, secure duplication and chunk research. The absolute modules perform four major measures which are listed below;

1. SHA-1 computation for reliability confirmation.
2. Chunk Preparation as per given size.
3. Encryption of Chunk for privacy managing.
4. Replication formation and circulation.

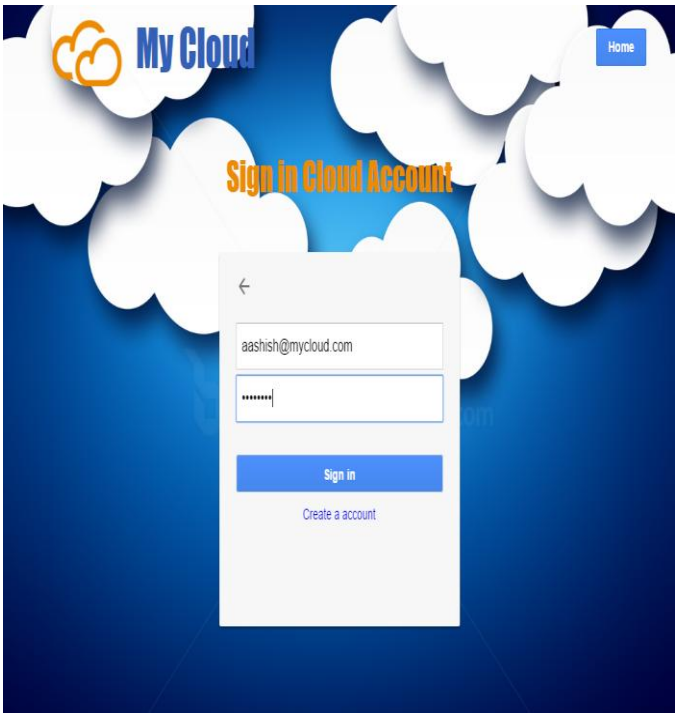
A detailed explanation of all the above written process has been explained in the next section of the chapter.

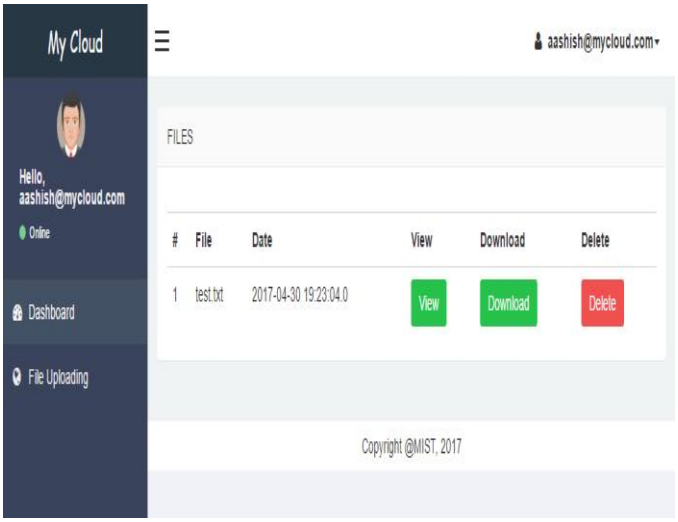
Module 3: Replication

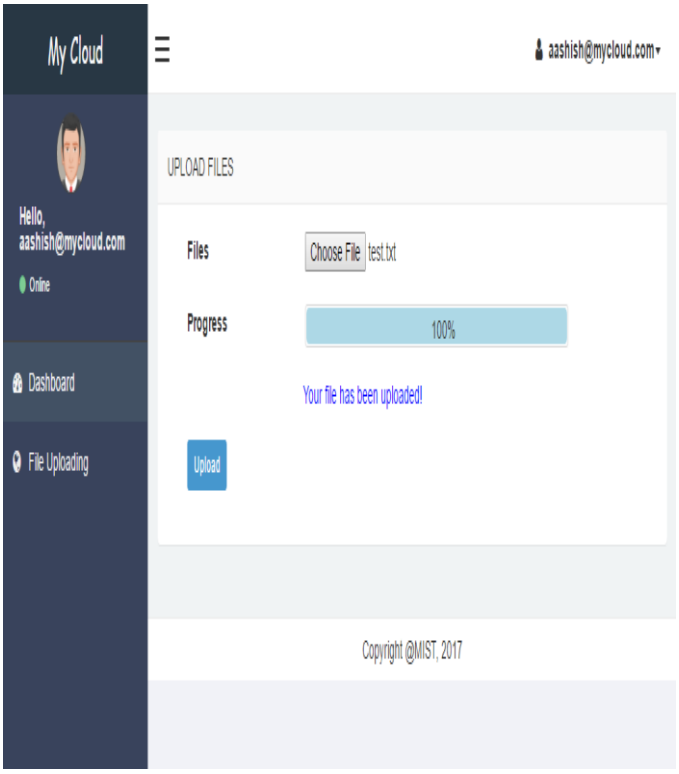
This module executes the replication procedure of the chunk files. It uses Even-Odd Scheme for replication of the chunk file.

1.Even duplication Server consist all even id replica chunk files and preserve backup of the replication.
2.Odd Replica Server consist all odd id replica chunk files and maintain backup of the replication.

6 SNAPSHOTS







8 CONCLUSIONS

Cloud computing is turning into greater secured via the use of the cryptography algorithm and it's miles a artwork of changing the relaxed messages into non readable shape of records. Now days every n every organization is transferring towards the cloud computing to comfortable their organization facts towards the unauthorized user. Cloud is presenting the storage areas to the consumer in addition to safety.Cloud Computing has the present cryptographic algorithms are unmarried level encryption algorithms. Cyber criminals can without problems cracked unmarried level encryption.In our proposed set of rules solution is a multilevel encryption and decryption algorithm for cloud computing. in this cloud computing server only a licensed consumer can get entry to the records. in case intruder receives the facts accidently or can hack deliberately . Unauthorized customers should crack the multilevel encryption which provides the greater safety for the cloud storage than the use of any single stage of encryption and decryption algorithm

6. REFERENCES

[1].Atul Kahate "Cryptography and Network Security", Second Edition-2003, Tata McGraw Hill New Delhi, 10th reprint-2010.
[2].Do Van Thanh, Tore Jenvik, Do Van Thuan & Ivar Jorstad :"Enhancing Internet service security using GSM SIM authentication" , Proceedings of the IEEE Globecom 2006 conference - ISBN 1-42440357•X - San Francisco, USA, Nov 27 - Dec 1, 2006.
[3].Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012
[4.]Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process

and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia
[5].Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015
[6.]P. Triantafillou and C. Neilson "Achieving Strong Consistency in a Distributed File" IEEE Transactions on Software Engineering vol 23.No1 January 1997.
[7].M. Wiesmann, F. Pedonet, A. Schiper, B. Kemmet, G. Alonso "Database Replication Techniques: a Three Parameter Classification" published in Reliable Distributed Systems, 2000. SRDS-2000. Proceedings The 19th IEEE Symposium on at Lausanne PP. 206-215
[8].H. Shen,; "Integrated File Replication and Consistency Maintenance in P2P Systems" , IEEE Transactions on Parallel Systems,Vol. 21,no 1, January 2010.
[9].Y. Huang, J. Cao, B. Jin, X. Tao, J. Lu and Y. Feng "Flexible Cache Consistency Maintenance over Wireless Ad Hoc Networks" IEEE Transactions on Parallel Systems,Vol. 21, no 8, August 2010.
[10] T. Repantis, A. Iyengar, V. Kalogeraki and I. Rouvellou "Consistent Replication in Distributed Multi-Tier Architectures" published in International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, Florida, USA, October 15-18, 201
[11]Diana, P. Fatos Xhafa, F. Pop and V. Cristea "Evaluation of Optimistic Replication Techniques for Dynamic Files in P2P Systems" published in International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2011.
[12Sulistio, C. Shin Yeo, and R. Buyya "Simulation of Parallel and Distributed Systems: A Taxonomy and Survey of Tools".
[13]. A. Ahmed', A. Abdullah2, and P.D.D.Dominic3; "A multi-Agent Based Replication Strategy for Improving Availability and Maintaining Consistency of Data in Large ScaleMobile.