International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-01, Apr 2018

Efficient Disaster Recovery in Cloud with Performance Guarantee for Satellite Data Processing

[1]P Manivannan, [2]Gujare .N. Sonali, [3]Mestri A. Rutuja, [4]Pardhi C. Arti

[1,2,3,4]Dept. of Information Technology, Mahatma Gandhi Mission's College of Engineering and Technology, Mumbai, Maharashtra, India.

[1]*pmvannan.mtech@gmail.com*, [2]*gujaresonali@gmail.com*, [3]*mestrirutuja23@gmail.com*, [4]*artipard000123@gmail.com*

Abstract - In satellite data processing approach , tremendous measure of information is produced each moment. It winds up plainly basic to deal with this sensitive information productively since in view of this information different computations and estimations are finished by the researchers and the specialists. Each association managing this sensitive information must have information recuperation designs and information reinforcement designs prepared in the event of fiascos. For this, cloud gives a superior arrangement. Cloud gives you better execution and accessibility as well as gives you cost-productive information recuperation. The point of this paper is to give a review of the procedures which will ensure elite information recuperation with least Recovery Time Objective(RTO) and Recovery Point Objective(RPO).

Index Terms— Cloud Computing, HS-DRT, ERGOT, PCS, Outlier Detection, Replication.

I. INTRODUCTION

Cloud computing is a standout amongst the best approaches to recuperate from a fiasco, since cloud as a type of calamity recuperation empowers the replication of the framework and information to a remote site. This empowers the information and framework capacities to be available in a brief timeframe interim when the essential site is down. In addition, cloud computing depends on virtualization, influencing the recuperation to process repeatable and more reliable, since manual intercession won't not be fundamental. Likewise, virtualization abstracts equipment and programming conditions bringing down the necessities at the recuperation site. Although numerous SMBs don't have an IT Department, despite everything they have IT assets (e.g., site, email, record stockpiling, reinforcement, et cetera) which must be reestablished if there arises an occurrence of calamities. We contend that a private fiasco recuperation cloud can be utilized by SMBs because of automated virtual platforms that can limit the recuperation time after a calamity, and in addition empower other uses of the spare infrastructure while the disaster recovery service is not requested. Cloud computing is a developing model for business figuring and in addition dissecting the extreme information.

II. EXISTING SYSTEM

1. HS-DRT

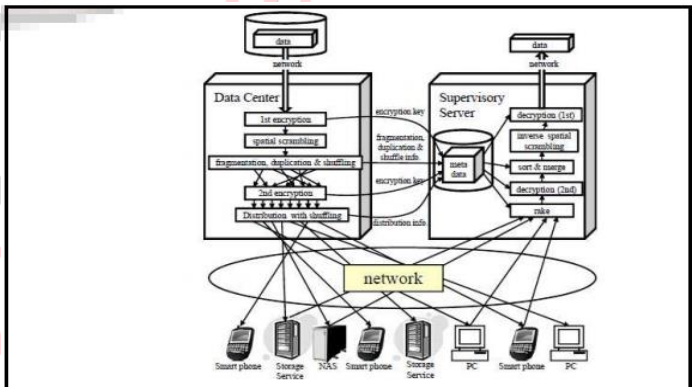

Figure 1 The Basic Configuration Of HS-DRT System

The HS-DRT document backup mechanism has three foremost segments as appeared in figure and those are Data Center, Supervisory Server and different customer hubs:

1. Backup grouping: When the Data Center gets the information which is to be backed up, it encodes it, scrambles it, and partitions it into pieces, and from that point replicates the information. The Data Center encodes the parts again in the second stage and circulates them to the customer hubs in an arbitrary request.
2. Recovery sequence: When a catastrophe happens, the Supervisory Server starts the recuperation grouping. The Supervisory Server gathers the encoded parts from different fitting customers in a way like a rake gathering methodology.

 DOI : 10.18231/2454-9150.2018.0090

3. Security Level of HS-DRT: The Security level of the HS-DRT relies upon spatial scrambling, fracture/replication, and the rearranging calculation. In light of these three variables, no one can decode without gathering every single applicable part, choosing a one of a kind arrangement of pieces, and arranging the sections into the right request. Regardless of the possibility that a few pieces are captured, no one can decode parts of the first information from such sections.

Merits:

This system can be utilized by customers like Smartphone's, portable workstation and so on.

Demerits:

1.High execution cost.
2.Increase redundancy.

2. Parity Cloud Service (PCS) :

Parity cloud is the strategy that uses parity recuperation service .PCS has ease of recuperation and recoups information with high efficiency. For information reinforcement, PCS makes the virtual disk in clients framework for information reinforcement, make parity gatherings and store parity information of gathering in cloud. The PCS calculation works utilizing Exclusive – OR for making parity data.

Merits:

1. Provides Reliability
2. Security to information
3. Low usage cost

Demerits:

High Implementation complexity

3. Cold and Hot Backup Strategy :

Cold and Hot Backup Service procedure is trigger based . It is activated when there is failures in service and won't be activated when service is accessible . In Hot Backup Service substitution procedure (HBSRS) amid the execution of administration reinforcement benefits in unique state. And after that initially gives consequence of administrations will be received to give fruitful usage of administration sythesis. Among the CSBRS and HSBRS , the HSBRS lessen the administration recuperation time.

Merits:

-Triggered just when disappointment distinguished

Demerits:

-Cost increment as information increment

4.ERGOT:

The expanding requests for online administrations needs disseminated engineering for advancing its adaptability and semantics to empower to their productive recovery . So by utilizing two diverse methodologies towards objective are Semantic Overlay Network (SON) and Distributed Hash Tables (DHT). Semantic based disclosure is done in distributed infrastructure such as grids and clouds. By consolidating SON and DHT, ERGOT (Efficient directing grounded on scientific categorization) is presented. ERGOT exploits in two ways initially is administrations are publicized in DHT on premise of their explanations and another is comments empower semantic based administration coordinate making, so these methodologies empowers us for exactness of search and network traffic.

Merits:

Quick and correct match information recovery Privacy to information.

Demerits:

1. High time
2. Implementation complexity .

III. PROPOSED SYSTEM

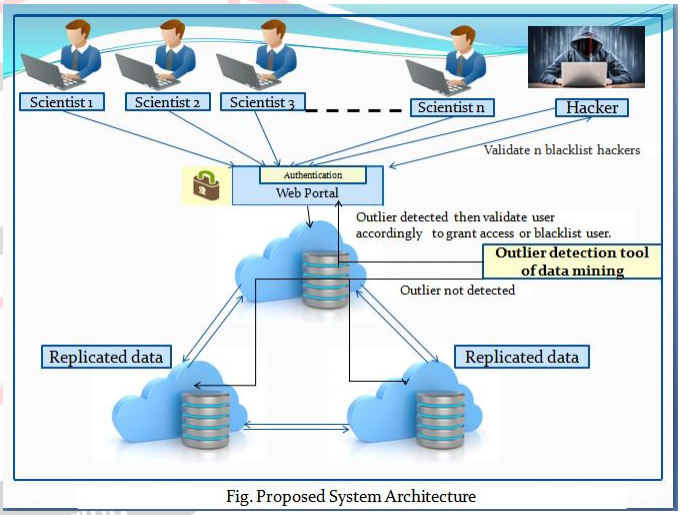

Fig. Proposed System Architecture

- The proposed architecture consists of a main server, 'n' number of clients, outlier detection tool of data mining, authentication and two replicated servers. Since the satellite data is very sensitive, it becomes very important to recover this data over a short period.
- If the user is an authorized person, then he/she can upload, access, change, modify or delete data in the main cloud server. In the main server, this data undergo outlier detection. If no outlier is detected and user has log out his/her account, the data is replicated immediately.
- But if the user is an unauthorized person(hacker) and gets illegal access to cloud by using login credentials of an authorized person, then the outlier detection can help

 DOI : 10.18231/2454-9150.2018.0090

in recovering data which the hacker might have tried to manipulate.

- In outlier detection method, when the data is detected to be outlier, it sends a notification for user validation via security questions. If the user fails to answer right, then the user is blocked for any further process. The modification done to data is replaced with replicated backup data.
- Infrastructure of cloud can also get damaged due to natural disaster such as flood, fire, earthquake, power outage, etc. Recovery of data can be achieved by ceasing the use of damaged server and automatically replacing it with replicated server at different geographical location.

A. Advantages of The Proposed System

a. High data Reliability.
b. Increase Availability and Performance.
c. Fault Tolerance.
d. High Security.
e. Role based Access.
f. Data Consistency

IV. MODULE DESIGN

This project having Five Modules

1. Authentication
2. Session
3. Replication
4. Outlier Detection
5. Types of disaster

1. Authentication

Customer verification is the procedure by which clients safely get to cloud benefits by trading a Digital Certificate. The advanced Certificate is to a limited extent seen as your 'Computerized Id' and is utilized to cryptographically tie a customer's personality to an exceptional computerized endorsement. The Digital Certificate would then be able to be mapped to a customer record and used to give get to control to arrange assets, web administrations and sites. Similarly as cloud supplier need to control which singular customer approach system and assets, cloud supplier likewise should have the capacity to recognize and control the cloud et to. Executing gadget validation implies just cloud, with fitting qualifications can get to , convey, work on organize.

2. Session

A session is storing client specific information for a constrained time frame. Session comprises of Session ID with customer data. A Session ID or Session token is exceptional identifier of that site relegates to a particular client for some foreordained length of time or session to monitor guest movement.

3. Replication

Replication is the way toward making a reproduction of something. On the cloud, the information has been recreated in it's altogether and put on another cloud is called cloud mirroring or cloud replication. Utilizing replication, the intermittent electronic outfreshing/duplicating of information starting with one cloud then onto the next cloud, so all clients in cloud network who are accessing the cloud network continually share a similar level of data if any kind of calamity happen.

4. Outlier Detection

Outlier Detection is the way toward identifying and subsequently barring anomalies from a given arrangement of information. An anomaly might be characterized as a bit of information or perception the goes astray definitely from the given standard of informational collection or or average of data set. An exception might be caused just by shot, however it might likewise show estimation blunder or that the given data set has a heavy tailed distribution. For fundamental cloud information, the outlier detection tool are utilized to identify the anomaly. In this outlier detection event if outlier is discovered then at that point the cloud supplier send notification or message to researcher/customer for validation purpose. The client should respond to validation questions within 5 minutes. If this information is considered as substantial information then data is replicated in cloud. If client is not able to answer those security questions then this information won't get imitated and this client will be blacklisted.

5. Types of Disaster

- **Natural disaster:**

Infrastructure of cloud can also get damaged due to natural disaster such as flood, fire, earthquake, power outage, etc.

➢ **Action taken for recovery by proposed System.**

Recovery of data can be achieved by ceasing the use of damaged server and automatically replacing it with replicated server at different geographical location.

- **Man made attacks:**

1. **The C99 shell Attack:**

The c99 shell is an electronic web based shell customized in PHP. It e.g. permits erasure, migration and copying of documents, has worked in implies for changing the record authorizations and so on. Assist it bolsters associations with different machines, brute-forcing FTP passwords and permits to interface with SQL-Databases and issue commands.

 DOI : 10.18231/2454-9150.2018.0090

➢ **Action taken for recovery by proposed System.**

Outlier detection will detect hacker and validation via security questions will be performed to blacklist hacker. Recovery of data can be achieved by ceasing the use of crashed server and automatically replacing it with replicated server.

2. A Denial-of-service attack :

It is a security event that happens when an assailant makes a move that prevents legitimate users from accessing targeted PC frameworks, gadgets or other system assets. Denial-of-service (DoS) assaults ordinarily surge servers, frameworks or systems with activity so as to overpower the casualty assets and make it troublesome or inconceivable for honest to goodness clients to utilize them. It crashes a server. goodness clients to utilize them. It crashes a server.

➢ **Action taken for recovery by proposed System.**

Recovery of data can be achieved by ceasing the use of crashed server and automatically replacing it with replicated server.

3. A SQL Injection attack :

It comprises of addition or "injection" of a SQL query by means of the information from the customer to the application. A fruitful SQL injection adventure can read sensitive information from the cloud, change cloud information (Insert/Update/Delete),executes administrative operations on the database recoup the substance of a given record introduce on the cloud document framework and now and again issue summons to the working framework. SQL injection assaults are a sort of infusion assault, in which SQL commands are injected into information plane contribution to impact the execution of predefined SQL charges.

➢ **Action taken for recovery by proposed System.**

Primary Defenses:

Use of Prepared Statements (with Parameterized Queries).
Use of Stored Procedures.
White List Input Validation.
Escaping All User Supplied Input.

Additional Defenses:

Enforcing Least Privilege.
Performing Whitelist Input Validation as a Secondary Defense.

6. Brute Force Attack :

A programmer utilizes a PC program or content to endeavor to sign in with conceivable watchword blends or possible password combinations, generally beginning with the most straightforward to-figure passwords. (So simply think: if a programmer has an organization rundown, he or she can without much of a stretch figure usernames. On the off chance that even one of the clients has a "Password123", he will rapidly have the capacity to get in.). It doesn't utilize a rundown of passwords; rather, it goes for attempting every single conceivable blend in the watchword space. Once the hacker gets login credentials using this attack he/she may get access to cloud data.

➢ Action taken for recovery by proposed System.

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. Captcha prevents automated attacks used by brute force attack.

*5. **Dictionary Attack***

A programmer utilizes a program or content to attempt to login by cycling through mixes of regular words. From Wikipedia: "interestingly with a beast constrain assault, where an expansive extent key space is sought methodically, a dictionary assault tries just those conceivable outcomes which are destined to succeed, commonly gotten from a rundown of words for example a dictionary (hence the phrase dictionary attack). By and large, lexicon assaults succeed in light of the fact that many individuals tend to pick passwords which are short (7 characters or less, for example, single words found in word references or basic, effortlessly anticipated minor departure from words, for example, adding a digit."Once the programmer gets login accreditations utilizing this assault he/she may access cloud data.

➢ **Action taken for recovery by proposed System.**

The most obvious way to block dictionary attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. Captcha prevents automated attacks used by brute force attack.

6. **Keylogger Attack:**

A programmer utilizes a program to track the greater part of a client's keystrokes. So toward the day's end, everything the client has written—including their login IDs and passwords—have been recorded. A key logger assault is unique in relation to a beast power or lexicon assault from multiple points of view. Not the minimum of which, the key logging program utilized is malware (or an all out infection) that must first make it onto the client's gadget (regularly the client is deceived into downloading it by tapping on a connection in an email). Keylogger assaults are additionally unique in light

 DOI : 10.18231/2454-9150.2018.0090

of the fact that more grounded passwords don't give much security against them. Once the hacker gets login credentials using this attack he/she may get access to cloud data.

➢ **Action taken for recovery by proposed System.**

The free version of Zemana and SpyShelter only provides encryption for your keystrokes, which means that although the attacker will be able to log your keystrokes, they'll be presented to him in a scrambled and unreadable format.

V. Conclusion

This specialized paper exhibits a down to earth replication based information recuperation strategy. The proposed framework detects unauthorized user using outlier detection tool to cease unauthorized modification of cloud data. Productivity of information recuperation is expanded by utilizing two replicated server in the event of manmade or natural disaster. Strong Consistency, High Availability of information using replication while still maintaining high performance and Security using outlier detection makes this proposed system of incredible use when contrasted with existing framework.

REFERENCES

[1] Liang Zhao, Sherif Sakr, Anna Liu "Cloud data management" -2004

[2] YUN YANG, WENHAO LI, DONG YUAN – 2014 "RELIABILITY ASSURANCE OF BIG DATA IN THE CLOUD 1ST EDITION "

[3] Eleni Palkopoulouy, Dominic A. Schupke, Thomas Bauscherty, "Recovery Time Analysis for the Shared Backup Router Resources (SBRR) Architecture", EEE ICC 2011.

[4] Vijaykumar Javaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[5] Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki, Kazuo Ichihara, Performance Evaluation of a Disaster Recovery System and Practical Network Applications in Cloud Computing Environment, International Journal on Advances in Networks and Services, Volume 4, Issue 1 & 2,2011.

[6] Manish Pokharel, Seulki Lee, Jong Sou Park, "Diaster Recovery for System Architecture using Cloud Computing", 10th Annual International Symposium on Applications and the Internet, 2010.

[7] Vijaykumar Javaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), 2011, "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[8] E. Hand, "Head in the clouds", Nature, Vol. 449, NO.24, pp. 963-970, 2007.

[9] Disaster Recovery Strategies with Tivoli Storage Management, C. Brooks, M. Bedernjak, I. Juran, J. Merryman, IBM/Redbooks, November 2002.

[10] Z.W. Xu, H.M. Liao, et. aI., "The Classification Research of Network Computing System", Journal of Computing Machine, Vol. 18, NO.9, pp.1509-1515,2008.

 DOI : 10.18231/2454-9150.2018.0090