RESEARCH ARTICLE OPEN ACCESS

A Virtualized Cloud for storing Mobile data with Location"- A Review

Deepika Bhatia *, Amol rangari**, Vishal wakodikar***
*(Department of Computer Science, JIT, Nagpur , India-11
** (Department of Computer Science, JIT, Nagpur , India-11

ABSTRACT-
Cloud computing is one of the latest developments in the IT industry also known as on demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. National institute of standard and technology defines as a model for enabling convenient, on-demand network access to a share pool of configurable computing service (for example, networks, servers, storage, applications and services) that can be provisioned rapidly and released with minimal management effort or services provider. Cloud computing is no longer a buzzword today. In addition, it changes and improves the way we uses the computing platform. In today's world, there is a huge increase in the mobile data. This requires large volume of data storage devices to store this large amount of data. Therefore, usually consumer prefers to store large amount of private data in cloud. Unfortunately, if mobile will be lost, stolen or damaged it leads to the loss of all important and private data then there should be some mechanisms to take back-up of the data, and provide the data. Although many backup and recovery techniques have been proposed during last few years in the computing domain; however, real world scenarios remain a challenge. In this review paper, we focuses on the various techniques of back-up and recovery on cloud computing.
Keywords **-** Cloud, Encryption, Data Recovery, Backup etc.

I. INTRODUCTION

The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud Computing is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash strapped IT departments that are wanted to deliver better services under pressure.When this cloud is made available for the general customer on pay per use basis, then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud. But having many advantages for IT organizations cloud has some issues that must be consider during its deployment. The main concern is security privacy and trust. These issues arise during the deployment of mostly public cloud because in public cloud infrastructure customer is not aware where the data store & how over the internet. In this paper security privacy & trust issues of cloud computing are reviewed.

II. RELATED WORK

The In our literature survey, we found many techniques that are having their unique ways to create backup and recovery. Broadly speaking, all those techniques focus on three different aspects, such as cost controlling, data duplication and security issues. Each of the technique has the complete focus on their aim of backup and recovery. Further, we detail few recent techniques HSDRT [1], PCS [2], ERGOT [3], Linux Box [5], Cold and Hot back-up technique [6].
In 2012 ,Kruti Sharma, Kavita R Singh[3], proposed differences between the work of different authors as below:-

Table-1 Comparison between Various Techniques of Back-Up and Recovery

S.No	Approach	Advantage	Disadvantage
1	HSDRT[1]	• Used for Movable clients like laptop, Smart Phone	• Costly • Increase redundancy
2	Parity Cloud Service[2]	• Reliable • Privacy • Low cost	• Implementation • complexity is high
3	ERGOT[4]	• perform exact-match retrieval • Privacy	• Time complexity • Implementation complexity
4	Linux Box[5]	• Simple • Low cost for implementation	• Required higher bandwidth • Privacy • Complete server Backup at a time
5	Cold /Hot Back-up	• Triggered only when failure	• Cost increases as data increases

1) Cold and Hot Backup Service Replacement Strategy (CBSRS) [6]

In Cold Backup Service Replacement Strategy (CBSRS) recovery process, it is triggered upon the detection of the service failures and it will not be triggered when the service is available. In Hot Backup Service Replacement Strategy (HBSRS), a transcendental recovery strategy for service composition in dynamic network is applied [6]. According to the availability and the current state of service composition before the services interrupt, it restores the service composition dynamically. During the implementation of service, the backup services always remain in the activated states, and then the first returned results of services will be adopted to ensure the successful implementation of service composition. On Comparing HBSRS with the CBSRS, it reduced service recovery time. However, because backup services and original services are executed at the same time, the recovery cost increases accordingly.

2) Linux Box

Another technique to reduces the cost of the solution and protect data from disaster. It also makes the process of migration from one cloud service provider to other very easy. It is affordable to all consumers and Small and Medium Business (SMB). This solution eliminates consumer's dependency on the ISP and its associated backup cost. A simple hardware box can do all these at little cost named as simple Linux box which will sync up the data at block/file level from the cloud service provider to the consumer. It incorporates an application on Linux box that will perform backup of the cloud onto local drives. The application will interface with cloud on a secured channel, check for updates and sync them with local storage. The data transmission will be secure and encrypted. After a valid login, the application secures the channel using IP Security and in-flight encryption techniques. The application then interacts with the application stack at the cloud service provider and does a onetime full backup. During subsequent check, it backs up only the incremental data to the local site. The limitation we found that a consumer can backup not only the Data but Sync the entire Virtual Machine[5] which somehow waste the bandwidth because every time when backup takes place it will do back-up of entire virtual machine.

3) Efficient Routing Grounded on Taxonomy (ERGOT)

Efficient Routing Grounded on Taxonomy [4] is a Semantic-based System for Service Discovery in Distributed Infrastructures in cloud computing. In our survey, we found a unique way of data retrieval. We made a focus on this technique as it is not a back-up technique but it provide an efficient retrieval of data that is completely based on the semantic similarity between service descriptions and service requests. It also exploits both coarse-grain service functionality descriptions and at a finer level. ERGOT is built upon 3 components. These components include:

1) A DHT (Distributed Hash Table) protocol, which we use to advertise semantic service description annotated using concepts from ontology,
2) A SON (Semantic Overlay Network), enables the clustering of peer that have semantically similar service description. The SON is constructed incrementally, as a product of service advertising via DHT,
3) A measure of semantic similarity among service description [4]. DHTs and SONs both networks architectures have some shortcomings. Hence, ERGOT combines both these network Concept. The ERGOT system proposed semantic-driven query answering in DHT-based systems by building a SON over a DHT. An extensive evaluation of the system in different network scenarios demonstrated its efficiency both in terms of accuracy of search and network traffic. DHT-based systems perform exact-match searches with logarithmic performance bounds, however does not go well with semantic similarity search models.

4) Data Block Recovery:

When a data block is corrupted, it can be recovered using the parity block provided by the PCS server and encoded data blocks provided by other nodes in the parity group. Assume that the n-th data block in nodei , Bin, has been corrupted. Nodei sends a recovery request message to the PCS server. On receiving the recovery request message, the PCS server identifies to which VDPG the node belongs to and reads the corresponding parity block, Pn. Then, it generates a temporary random block, r, and a temporary parity block, Pr, for recovery process. When the size of the VDPG is even, Pr = Pn r. Otherwise, Pr = Pn. The PCS server sends Pr along with the list of nodes that will send their encoded data block to nodei for recovery along with the IP address of nodei to all other nodes in the group. If there are any off-line nodes, the PCS server sends the message when they become on-line. On receiving the message, each node generates their own encoded data block, E, by XORing the n-the data block with r (Ej = Bin r, for each node j VDPG, j i) and sends to nodei. Then, the nodei recovers the corrupted data block by Bin = PrE1··· Ei-1 Ei+1··· E |VDPG|. (1) Note that the

whole virtual disk corruption can be recovered by iterating the above data block recovery process.
Apart from its best performance given by the algorithm discussed above PCS somehow lags behind in providing perfect solutions to backup and recovery due to some limitations. These limitations are [2]: first one is that, the recovery process cannot finish if one or more participating nodes are not online at the recovery time. Second limitation is that, PCS is based on Markov process and calculate Mean time failure. More important finding in our literature survey is that the effect of the individual disk reliability varies.

III. NEED FOR BACK-UP IN CLOUD COMPUTING

- Imagine having infinite, secure storage for your backup data at reasonable price.These are just some of the reasons why people aremoving their data to the cloud.
- The cloud can also handle tasks that normally require hardware anddownloadable software.
- Servers, for instance, are now hosted in the cloud.Companies like Google, host their applications inside the cloud. GoogleDrive, Vimeo, Flickr, Wordpress, and Widgetbox are just a few sample.

IV. DIFFERENT USES OF CLOUD

a)Media storage and playback

We don't have to always reprint photos, download MP3s, or hoard movies. Picasa, Spotify, Netflix, Sound cloud, and other services make media available on various devices through the web.

Fig 1: Cloud infrastructure

b)System back up and restore

Some operating systems provide cloud backup and restore services in case your device crashes or is stolen, or your datasomehow gets deleted.

c)Banking and finance

Personal finance services like Mint and Page Once, make it easier for you to monitor expenses, pay bills, or view portfolios in different currencies.

d)Social media and communications

We can also communicate and mingle through the cloud. Networking sites like Facebook and Twitter have apps you can use. Instant messaging (IM) and voice services like Google Voice and Skype also let you call and chat via the web instead of the usual phone services.

e) Note-taking and bookmarking

Copying links is old school with apps like Ever note and Instapaper that let you save and bookmark notes in a few clicks.

f) Remote Data Back-up Server

Remote Data Backup server is a server which stores the main cloud's entire data as a whole and located at remote place (far away from cloud). And if the central repository lost its data, then it uses the information from the remote repository. The purpose is to help clients to collect information from remote repository either if network connectivity is not available or the main cloud is unable to provide the data to the clients. As shown in Fig 1, if clients found that data is not available on central repository, then clients are allowed to access the files from remote repository.

The Remote backup services should cover the following issues:

1) Privacy and ownership.
2) Data security.
3) Reliability.
4) Cost effectiveness.
5) Appropriate Timing.

1) Privacy and ownership

Different clients access the cloud with their different login or after any authentication process. They are freely allowed to upload their private and essential data on the cloud. Hence, the privacy and ownership of data should be maintained; Owner of the data should only be able to access his private data and perform read, write or any other operation. Remote Server must maintain this Privacy and ownership.

2)Data security

The client's data is stored at central repository with complete protection. Such a security should be followed in its remote repository as well. In remote repository, the data should be fully protected such that no access and harm can be made to the remote cloud's data either intentionally or

unintentionally by third party or any other client we are using login password for data security.

3) Reliability

The remote cloud must possess the reliability characteristics. Because in cloud computing the main cloud stores the complete data and each client is dependent on the main cloud for each and every little amount of data; therefore the cloud and remote backup cloud must play a trustworthy role. That means, both the server must be able to provide the data to the client immediately whenever they required either from main cloud or remote server.

4) Cost effectiveness

The cost for implementation of remote server and its recovery & back-up technique also play an important role while creating the structure for main cloud and its correspondent remote cloud. The cost for establishing the remote setup and for implementing its technique must be minimum such that small business can afford such system and large business can spend minimum cost as possible.

5) Appropriate Timing

The process of data recovery takes some time for retrieval of data from remote repository as this remote repository is far away from the main cloud and its clients. Therefore, the time taken for such a retrieval must be minimum as possible such that the client can get the data as soon as possible without concerning the fact that remote repository is how far away from the client. There are many techniques that have focused on these issues. In forthcoming section, we will be discussing some of recent techniques of back-up and recovery in cloud computing domai

V. CONCLUSION

CLOUD CAMP-provides the most easiest way to store the private data of users mobile with the features of security, cost effesctive, reliable and easy to maintain by the user.

An android based mobile application for backup and restore of mobile data. It provides easy way to access the data, central storage of data, store the data locally and then upload it onlin,requirement of local storage reduced, information can be useable even after changing the mobile devices.The main and important applications of this project is it also provide the Gps .This application is more useful in any workplace and offices. In this paper, we presented detail review of most recent back-up and recovery techniques that have been developed in cloud computing domain. Detail review of this paper shows that these techniques have its own advantages and disadvantages which are summarized in the Table-1. All these approaches are able to provide best performances under all uncontrolled circumstances such as cost, security, low implementation complexity, redundancy and recovery in short span of time.

VI. FUTURE SCOPE

- In future plans we are extending our application so that it can be used on multiplatform such as Windows OS, Symbian S60.and we use it as Business Sharing Application.
- We can also add some more advanced encryption techniques for password protection.

ACKNOWLEDGEMENT

We wish to avail this opportunity to acknowledge our profound in debtedness and extend our deep sense of gratitude to our guide Mrs. Deepika Bhatia for their valuable guidance profound advice and encouragement that has feel to the successful completion of this research.

REFERENCES

[1] Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, Inzai-shi, Chiba,Kazuo Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications,2010, pp 256-259.

[2] Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 2011.