HYBRID DATA BACKUP TECHNIQUES FOR CLOUD COMPUTING

1Trupti A Thakkar, 2Assistant Professor Jwalant B Baria

[1]Student, [2]Assitant Professor
[1]Computer Engineering, Government Engineering College
Modasa, India.

Abstract - When data is being stored on our local server, for any reason our data gets lost or data is crashing and our data is not maintained so we need to back up the data so that our data is protected. And data protection is not maintained for any reason while backing up data, data protection is maintained and for the complexity of time and complexity of implementation, these two methods are designed for data backup storage, cloud computing, security. We have a combination of ECC algorithm and PVFS2, we will increase the accuracy of this data and reduce the complexity of time and implementation, which will ensure the accuracy of the data while backing up the data and reduce the time and execution time.

Keywords - Data Backup, Security, Data Recovery, ECC.

I. Introduction

Cloud computing more powerful, cheaper, and can be accessed anywhere anytime. Cloud computing delivers software (application) as a service, infrastructure as a service, and platform as a service. Examples are Amazon's EC2 Google's App Engine, Microsoft Azure , IBM Smart Cloud etc. Cloud backup has different services such as software as a services, Platform as a services and infrastructure as a services. Cloud computing has different models such as public cloud, private cloud and Hybrid Cloud. Its Based on five attributes:- 1)shared Resources 2) Massive Scalability 3) Elasticity 4) Pay AS you go 5) Self provisioning of resources.

In this scenario the research paper gives different Technique such as Cold and Hot back-up technique, ERGOT(Efficient Routing Grounded on Taxonomy), PCS(Parity Cloud Services), REN(Rent Out of Rented Resources), Linux box, SBA(Seed Block Algorithm),HSDRT(High Security Distribution and Rake Technology). Problems like security, data security, time and implementation complexity, privacy security issues are my top priority for keeping data security and security intact. The complexity of time is keeping the complexity and precision of the implementer which will solve the problem of data backup**.**

II. Literature Review

2.1 Cloud Computing Security Challenges & Solutions @ 2018 IEEE

In [1] paper describe the different cloud services model such as a IaSS, PaaS and Seas', and deployment model such as private model, public model and hybrid model.

Three factors has been considered for the cloud system security are Confidentiality, Integrity and availability.

2.2 **Cloud Computing: Fundamentals and Research Issues @ 2017 IEEE**

In [2] initial segment of this paper, a short conversation of essentials of distributed computing are introduced. Distinctive distributed computing conversation in Such as advantaged of distributed computing highlights of distributed computing hindrances of distributed computing, arrangement model and administrations models. In addition, all the issues of distributed computing are likewise talked about in this paper.

2.3 Security Algorithms in Cloud Computing @2017 International Journal of Computer Science Trends and Technology (IJCST*)*

In [3] Paper Data can be changed by third party while transferring .
The major issues related to data security include data integrity, data availability, data confidentiality, privacy, transparency of data and control over data where data resides.

There are various aspects for providing data security such as by providing access controls and encryption methods.

On the side of client, they should look into the security measures related to data that what are the security techniques are provided by cloud provider.

There are different security-based existing algorithms in which AES , DES , Triple- DES, Blowfish Algorithm, RSA , Diffie- Hellman Key Exchange. These algorithms are not secure, there is need to enhance the security of algorithms.

2.4 Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud @2017 International Journal of Engineering Science and Computing(IJESC)

In [4] paper There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms.

DES and AES are mostly used symmetric algorithms as they are relatively more secure. DES is quite simple to implement than AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithm. RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms in cloud. But the security algorithms which allow linear searching on decrypted data are required for cloud computing, which will take care about the safety of the data.

There is a large scope of improvement in this field of research. We can use cryptography in numerous places in order security in cloud.

2.5 Data Recovery Through Indexing in Cloud Computing @2018 IEEE

In [5] paper reason for the recuperation strategy is to assist client with collecting data from any reinforcement server when the server neglects to give the information to the client. Loads of recuperations components are utilized to recoup the information in the cloud, for example, HSDRT, ERGOT, LINUX BOX, PCS, COLD and COLD/HOT reinforcement procedure.

However, there are a few confinements in those procedures, for example, usage multifaceted nature, security issues and recovery time is high. In this paper utilizing Seed square calculation (SBA) evacuate the issues of information recuperation of the information reinforcement it can expel the space of an information however security issue can't be understood.

2.6 Backup of real time data and Recovery using cloud computing @2016 International Journal of Engineering Development and Research (IJEDR)

In [6] paper there are various calculations, for example, PCS, HSDRT, ERGOT, Linux Box, Cold/Hot reinforcement procedure. Are now characterized for late back-up and recuperation strategies that have been created in distributed computing space. The accompanying survey shows that none of these procedures can give best exhibitions under all conditions, for example, cost, security, low usage multifaceted nature, excess and recuperation in limited capacity to focus time.

2.7 Research and Implementation of Data Storage Backup @2018 IEEE

Technique/Methods/Algorithms:-Data Backup, System Backup & Application Backup

In [7] paper, increasingly more significantly, reinforcement strategies are adaptable, reinforcement substance are sheltered and dependable, and reinforcement and recuperation is simple and advantageous. The reinforcement technique can be information reinforcement, framework reinforcement, application reinforcement, and so forth. The information stockpiling and reinforcement framework is situated to the application's database, business framework, and center server and actualizes capacities, for example, information stockpiling, information reinforcement and recuperation, framework reinforcement and recuperation, and application reinforcement and recuperation.

2.8 triviback: A Storage-Efficient Secure Backup System @2017 IEEE

Technique/Methods/Algorithms:- Full Back-up, Incremental Back-up, Differential Back-up

In [8] paper Conventional backup tools like duplicity do support encryption/authentication and deletion of obsolete data, but come with a trade-off between flexibility and storage efficiency by distinguishing three types of backups: Full backups contain (compressed) copies of all backed up data at a specific point of time, differential ones contain only differences to a respective full backup, and incremental backups contain differences to any other backup (including incremental ones). Deletion of a backup, thus, implies deletion of all depending backups, requiring existence of storage-intensive full backups in practice.

2.9 A Review on Data Back-up Techniques for Cloud Computing @2014 International Journal of Computer Science and Mobile Computing (IJCSMC)

Technique/Methods/Algorithms:- SBA , PCS, HSDRT, SBBR

In [9] paper various procedures for PCS, Linux Box, HSDRT, SBA(Seed Block Algorithm) , ERGOT, SBBR, CBSRS(Cold Backup Service Replacement Strategy) and so on. Various issues of information reinforcement and recuperation for Cloud Computing, for example, keeping up the expense of usage and execution complexities as low as could reasonably be expected. Anyway every last one of the reinforcement answer for Cloud Computing can't accomplish all the issues of remote information back-up server with less extra room.

2.10 Efficient Data Backup Technique for Cloud Storage @2018 International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

In [10] paper we propose a proficient information reinforcement procedure Seed Block Algorithm (SBA) for distributed storage and making sure about back-up documents put away at remote server with Advance Encryption Standard (AES) Algorithm.

In this paper a strategy is recommended that license clients to store their information particularly onto the principal cloud server, when the File is put away at cloud server the AES method scrambles such record. Because of any explanation if any document gets erased, the SBA alongside the Help of AES get back that record from remote area where the reinforcement documents are put away.

2.11 Research and Implementation of a Data Backup and Recovery System for Important Business Areas @2017 IEEE

In [11] paper studies mainly focus on the availability and reliability without fully considering the confidentiality in the backup operation and recovery operation.

In this paper, through strong authentication, access control, security audit and other means, we design and implement a kind of data backup and recovery system for the military, national defence and other important fields considering the high confidentiality demand of information technology in modern military and national defence fields.

This paper is organized as follows. The first part is the introduction and the background. In section 2, we come to the design of the system and the third part is about the implementation of the system. Except to satisfy the reliability and availability and many fields require, the system can meet the higher data confidentiality requirements which come from the military and defence fields.

III. System Flow Diagram

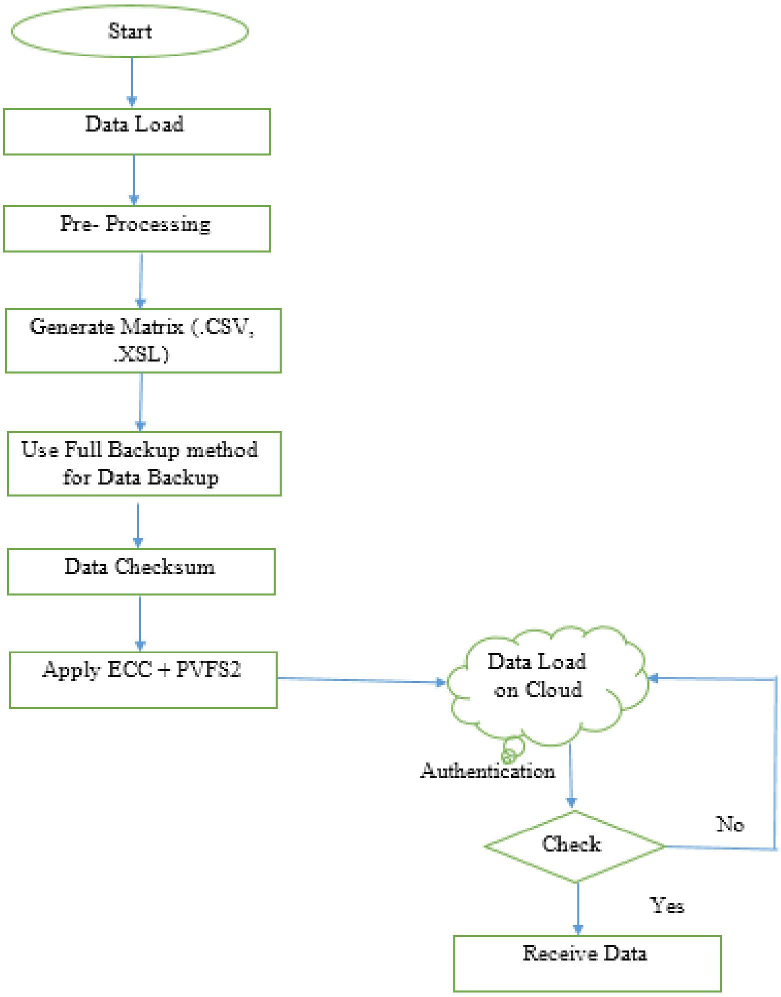

Fig. 3.1 System Flow Diagram

IV.CONCLUSION

- With the combination of the ECC algorithm and PVFS2, I will increase the accuracy of this data and reduce the time and implementation complexity, which will ensure the accuracy of the data while backing up the data and reduce the time and execution time.

REFERENCES

[1]SRIJITA BASU, ARJUN BARDHAN, KOYAL GUPTA,PAYEL SAHA, MAHASWETA PAL,MANJIMA BOSE, KAUSHIK BASU,SAUNAK CHAUDHURY, PRITIKA SARKAR "CLOUD COMPUTING SECURITY CHALLENGES & SOLUTIONS-A SURVEY" 978-1-5386-4649-6/18/$31.00 ©2018 IEEE

[2] Suyel Namasudra , Pinki Roy , Balamurugan Balusamy "Cloud Computing: Fundamentals and Research Issues" 978-1-5090-4799-4/17 $31.00 © 2017 IEEE

[3]T.Ramaporkalai " Security Algorithms in Cloud Computing" ISSN: 2347-8578 2017

[4]Rishav Chatterjee1, Sharmistha Roy2 "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud "ISSN 2321 3361 © 2017 IJESC

[5] Mr.Gadhave Hanmant Pandurang , Miss.Chavan Suvarna Bhimrao, prof .pravin chothe," Data Recovery Through Indexing in Cloud Computing"

[6] 1Karishma Nadhe, 2Sushma Somani "Backup of real time data and Recovery using cloud computing" ISSN: 2321-9939 2016

[7] Yongmin Zhao, Ning Lu "Research and Implementation of Data Storage Backup" 2018 IEEE

[8] Dominik Leibenger, Christoph Sorge "triviback: A Storage-Efficient Secure Backup System" 2017, Dominik Leibenger. Under license to IEEE. DOI 10.1109/LCN.2017.100

[9] Somesh P. Badhel, Prof. Vikrant Chole "A Review on Data Back-up Techniques for Cloud Computing" 2014 IEEE

[10] Yogesh Gite, Ankush Pawar, Dr. Shashikant Ghumbre "Efficient Data Backup Technique for Cloud Storage" ISSN (Online) 2394-2320 2018

[11] Jianping Zhang, Hongmin Li ":- Research and Implementation of a Data Backup and Recovery System for Important Business Areas" 978-1-5386-3022-8/17 $31.00 © 2017 IEE DOI 10.1109/IHMSC.2017.209