iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X1, November 2017- Available at www.ijraset.com

Multi-Cloud for Improving Cloud Data Security

Rucha Dixit[1], Omkumar Pal[2], Abhishek Gaikwad[3], Mahesh Tawaskar[4], Aditya Sankpal[5]
[1, 2, 3, 4, 5] *Research Scholar, KLU & Assistant Professor, JSPM JSCOE Pune,Computer Department, JSPM, JSCOE Pune Savitribai Phule Pune University*

Abstract: Everyday quintillion bytes of data are generated; 90%of which has been created in the last two years alone, from this itcan predict the amount of data that will be generated in future. It is necessary, to introduce some techniques for providing security such ahuge amount data and to deal with limitation of 'Cloud Security'. Such cloud security can bemused nearly in every aspect of cloud environment system. The motive of this paper is to understand how cloud security is prime and the necessity of multi cloud system. This paper also gives a short glimpse of multi cloud security implications in the real world and its role in every field along with challenges and advantages. This paper also explores various techniques, algorithms such as Shamir Secret and Blowfish, systems of multi cloud system in various sectors of digital world.

Keywords: Cloud Data security, Multi-Cloud Data Encryption and Decryption.

I. INTRODUCTION

A. *What is Cloud Computing?*

Cloud computing is simply renting or leasing of resources which is required by an organization. It helps in reducing the infrastructure cost in project. Types of cloud:

1) Public or External Cloud
2) Private Cloud
3) Community Cloud
4) Hybrid Cloud

In the recent years, cloud service gains enormous popularity with the growing of big data. The cloud storage service relieves the burdens of clients on storage management and access control. The cloud service system of current lacks data integrity and data security in multi cloud. The currently widely used clouds include Amazon S3, Google File System, etc. All of them have the common features: a service interface provides centralized management by a global namespace, files are split into blocks or sectors and are stored on remote servers, and the systems are consisted of inter-connected clusters of service nodes.

B. *What is Multi-Cloud Computing?*

Multi Cloud is the use of multiple cloud computing services in a single heterogeneous architecture. For example, an enterprise may concurrently use separate cloud providers for infrastructure (IaaS) and software (SaaS) services, or use multiple infrastructure (IaaS) providers. In the latter case, they may use different infrastructure providers for different workloads, deploy a single workload load balanced across multiple providers (active-active), or deploy a single workload on one provider, with a backup on another (active-passive). There are a number of reasons for deploying a multi-cloud architecture, including reducing reliance on any single vendor, increasing flexibility through choice, and mitigating against disasters. It is similar to the use of best-of-breed applications from multiple developers on a personal computer, rather than the defaults offered by the operating system vendor. It is a recognition of the fact that no one provider can be everything for everyone. It differs from hybrid cloud in that it refers to multiple cloud services rather than multiple deployment modes (public, private). Various issues also present themselves in a multi-cloud environment. Security and governance is more complicated, and more "moving parts" may create resiliency issues. Selection of the right cloud products and services can also present a challenge, and users may suffer from the paradox of choice.

C. *Advantages of Multi-cloud Computing:*

1) It gives multi choices for the Business Organization.
2) It gives more security for the data storage, if the data gets corrupted.
3) It gives flexible switching between different clouds.
4) It is cost efficient.
5) It allows combination of Private and Public Cloud.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X1, November 2017- Available at www.ijraset.com

D. Present Multi-cloud architecture for cloud computing

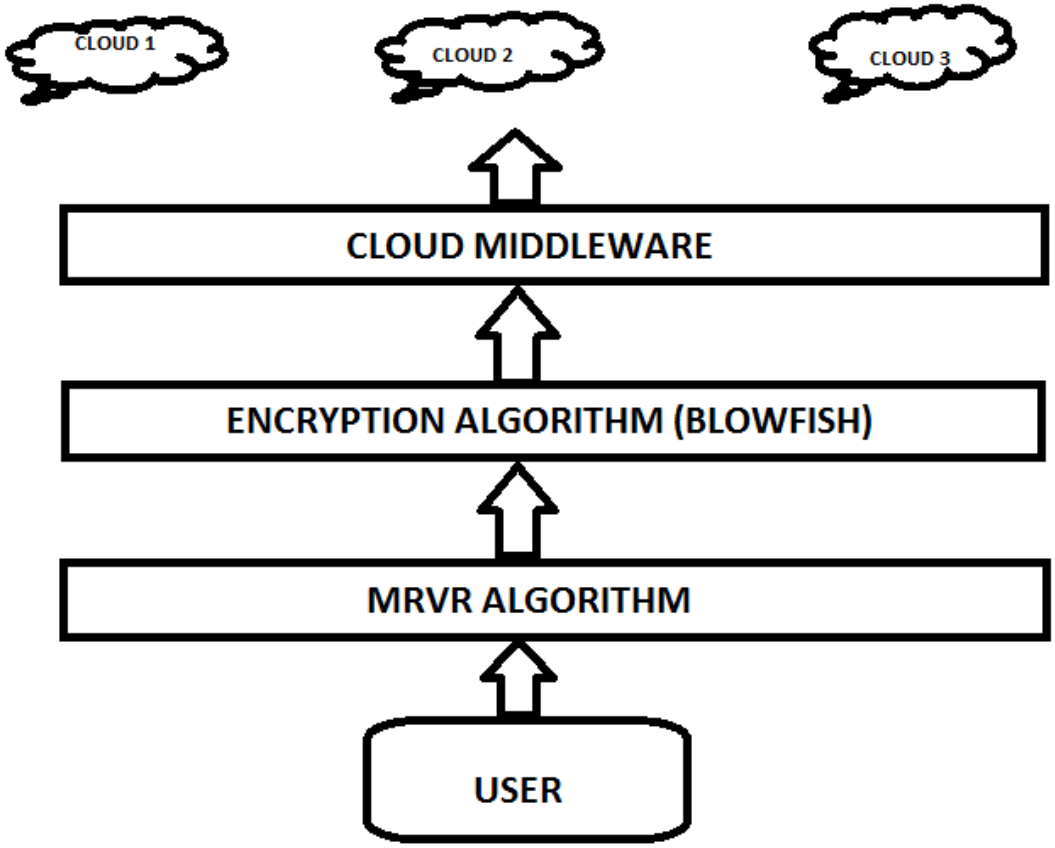


Fig: 1 Present Architecture for Cloud Computing

The present architecture of cloud computing involves MRVR Algorithm and Blowfish Algorithm. The user will upload data into cloud. Further, Data is encrypted with the Blowfish Algorithm and encrypted is send to Cloud Middleware or Auditors. Data is encrypted for increasing security and if data is hacked the hacker will get encrypted data. Lastly, the data is send to different cloud as replicas of encrypted data.

E. Disadvantages of Present architecture

1) Organization has to trust the cloud middleware or Auditors for the security of data.
2) Insider Threat Attack may leak the confidential data from Auditors.
3) Due to this organization may suffer heavy loss or may bankrupt.

II. LITERATURE SURVEY

Paper no.	Techniques/Methods/ Algorithms	Tools	Journal	Year
1	TPA	Data storage, Public auditability, Data dynamics, Cloud computing	IEEE	2011
2	Auditing Protocol,Batch Auditing for multiowner.	Storage auditing, Batch auditing, Privacy-preserving auditing	IEEE	2013

3	Remote Data Checking (RDC)	Data security, Robustness	IEEE	2012
4	Remote data possession checking protocols	Management of computing and information system, Database management	IEEE	2014
5	Pairing based provable multi-copy data possession (PB-PMDP) scheme	Data integrity, Cryptographic protocol	IEEE	2012
6	OPoR	Data Retrievability	IEEE	2015
7	Ranked Merkle Hash Tree, BLS Signature	Authorized auditing, data security	IEEE	2014

Table: 1 Literature Survey

III. PROPOSED ARCHITECTURE

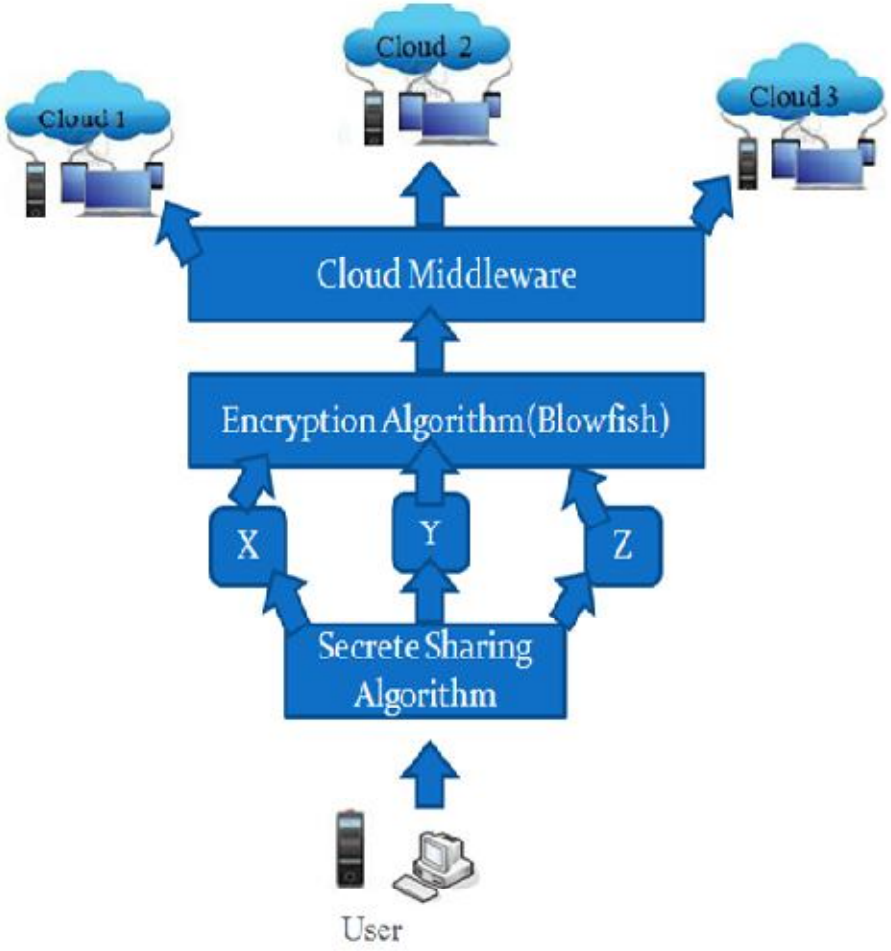


Fig: 2 Proposed Architecture for Cloud Computing

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X1, November 2017- Available at www.ijraset.com

IV. EXPLANATION OF PROPOSED SYSTEM

To improve the Data Security it is necessary and efficient to use combination of Shamir's secret Algorithm and Blowfish algorithm together. It works efficiently and breaks the user data and then encrypt the data hence it provides enhanced security. The working of system is explained in Fig.2.the user data first break into smaller pieces by Shamir Secret Algorithm. Further the small pieces of data is encrypted by Blowfish Algorithm. Lastly, the encrypted small pieces of data is stored in different cloud servers.

A. Shamir's Algorithm:

1) Divide secrete information into parts.

2) Using of some of the parts or all of them are required in order to reconstruct the secret information.

B. Blowfish Algorithm:

1) Blowfish provides a good encryption rate in software.

2) The algorithm is hereby placed in the public domain, and can be freely used by anyone.

C. Advantages

1) Organization should not be fully based on cloud middleware for security.

2) Hacker will get incomplete encrypted information if the server is hacked, and that information is of no use.

3) The data uploaded will be more secured and trustworthy.

V. MATHEMATICAL MODEL OF PROPOSED SYSTEM

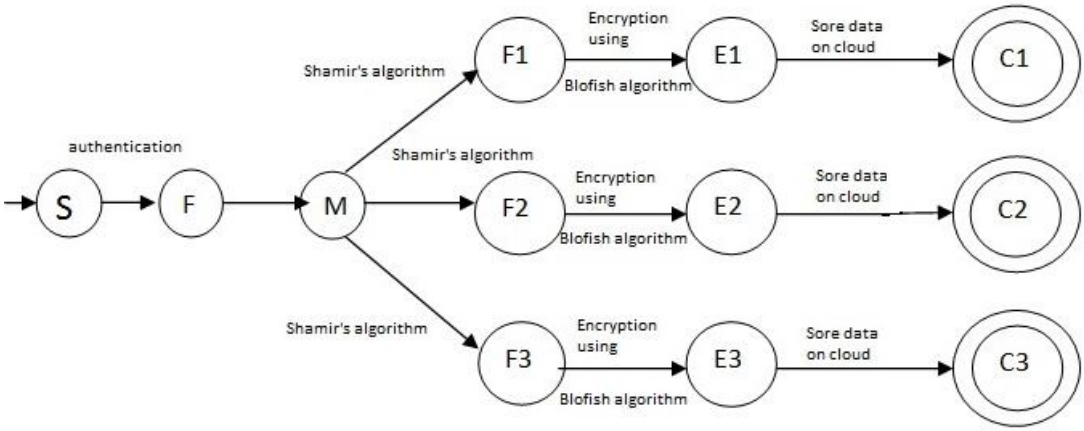


Fig: 3 Uploading of Data from User

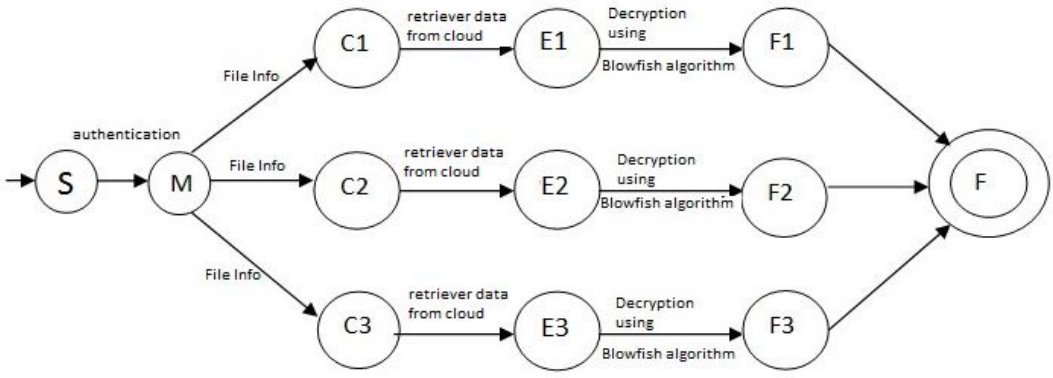


Fig: 4 Retrieving of Data from Cloud

S= Start state
F= Data file
M= Meta file
{F1, F2, F3}= divided file using Shamir's algorithm
{E1, E2, E3}= Encrypted File using Blowfish algorithm
{C1,C2, C3}= different clouds

VI. CONCLUSION

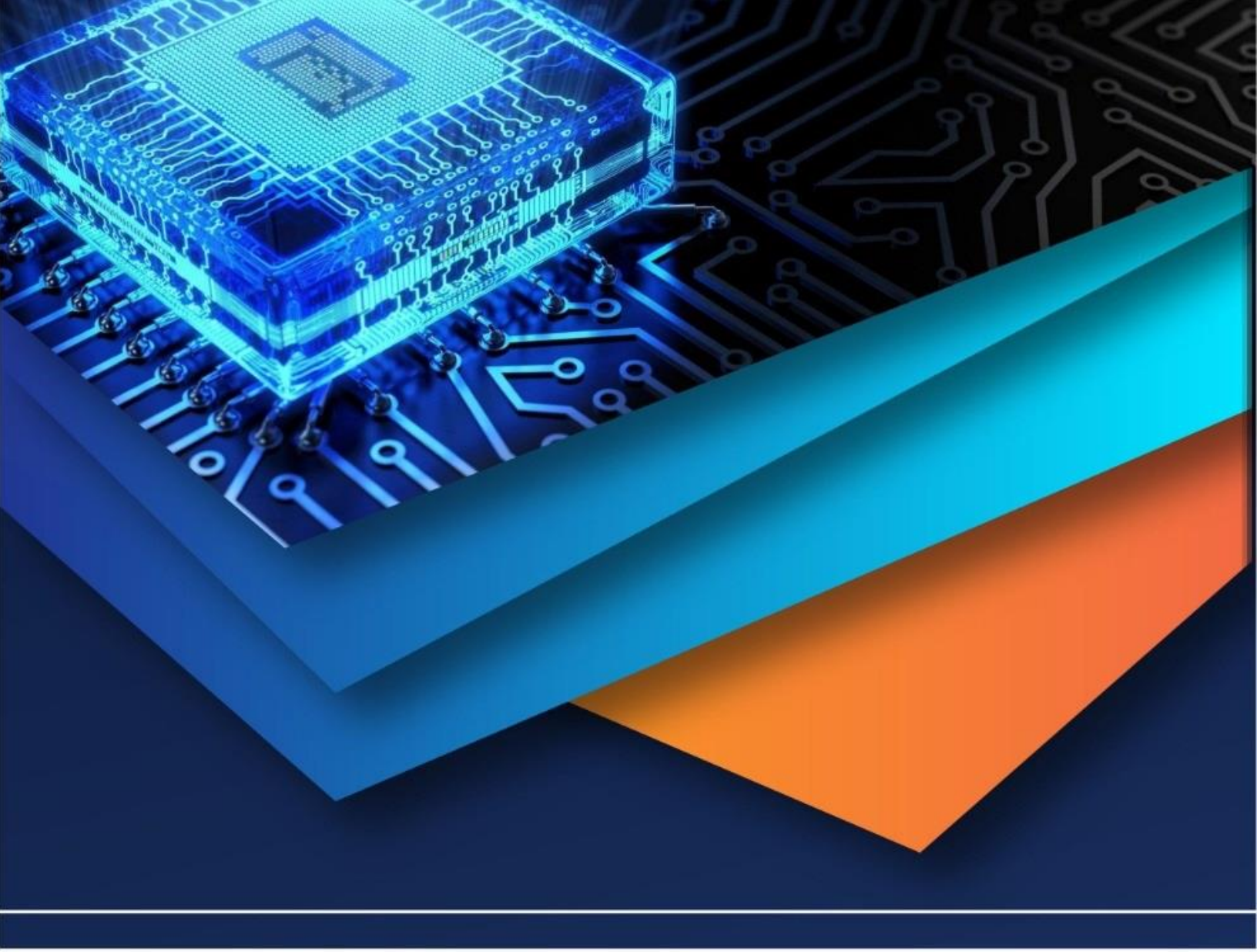
The amount of data generated and stored is vast in multi cloud system. By use of Shamir's secret algorithm and Blowfish algorithm together successfully and enhancing data security and integrity in multi cloud environment. The proposed system provides efficient use of single and multi-cloud storage environment. In order to achieve high security we combine two algorithms i.e. Shamir's secret algorithm. Blowfish algorithm. Overall data integrity, security, availability is maintained. We hope the content discussed in this paper, can be helpful for future analytics.

VII. ACKNOELEDGMENT

Special thanks to our Staff of Department of Computer Engineering, Jayawantrao Sawant College of Engineering & Sciences Hadapsar Pune and Savitribai Phule Pune University in order to support this work.

REFERENCES

[1] Y. Zhu and H. Hu, "cooperative provable data possession for integrity verification in multicloud storage", IEEE transactions on parallel and distributed systems, Vol. 23, 2012, pp. 2231-2244.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possessionat untrusted stores", in ACM CCS '07, 2007, pp. 598-609.
[3] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.- J. Quisquater, "Efficient remote data possession checking in critical information infrastructures", IEEE Transactions on Knowledge and Data Engineering, Vol. 20, 2008, pp. 1034 -1038.
[4] Juels and B. Kaliski, "PORs: Proofs of retrievability for large files", In ACM CCS '07, 2007, pp. 584-597.
[5] R. Curtmola, O. Khan and R. Burns, "Robust Remote Data Checking", in 4th ACM StorageSS, 2008, pp.63-68.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY