© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Enhancement of Cloud Data Security by Multi-Cloud Data Encryption and Decryption

Bhaskar Marapelli
Lecturer, Department of Software Engineering, College of Computing and Informatics, Wolkite University

ABSTRACT

Everyday trillion bytes of data are generated, 90%of which has been created in the last two years alone, from this it can predict the amount of data that will be generated in future. It is necessary, to introduce some techniques for providing security such a huge amount data and to deal with limitation of 'Cloud Security'. Such cloud security can be used 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: Multi-Cloud Data Encryption and Decryption, Cloud Data security.

I. INTRODUCTION

A. E 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 software (SaaS) and infrastructure (IaaS) 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. 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's fundamentally the same as the utilization of best-of-breed applications from various designers on a PC, as opposed to the defaults offered by the working framework merchant. It is acknowledgment of the

way that nobody supplier can be everything for everybody. Various issues also present themselves in a multi-cloud environment. Security and governance is more complicated, and more "moving parts" may create resiliency issues.

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.

D. Present Multi-cloud architecture for cloud computing

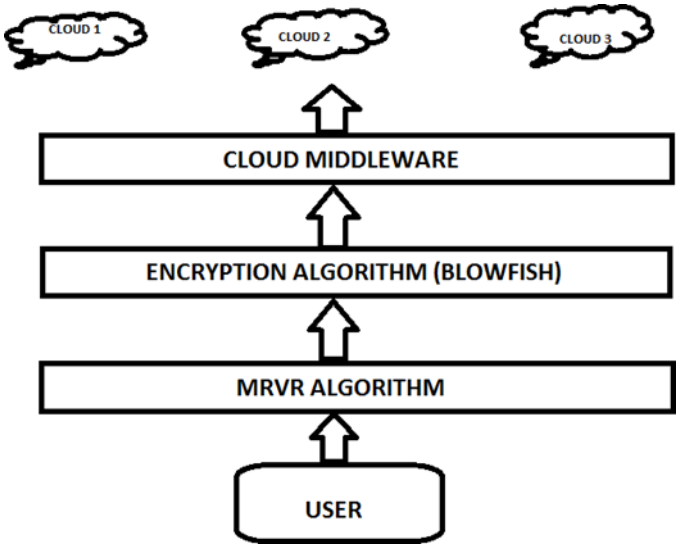

Figure 1. Present Architecture for Cloud Computing

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

Table 1. 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

III. LITERATURE SURVEY

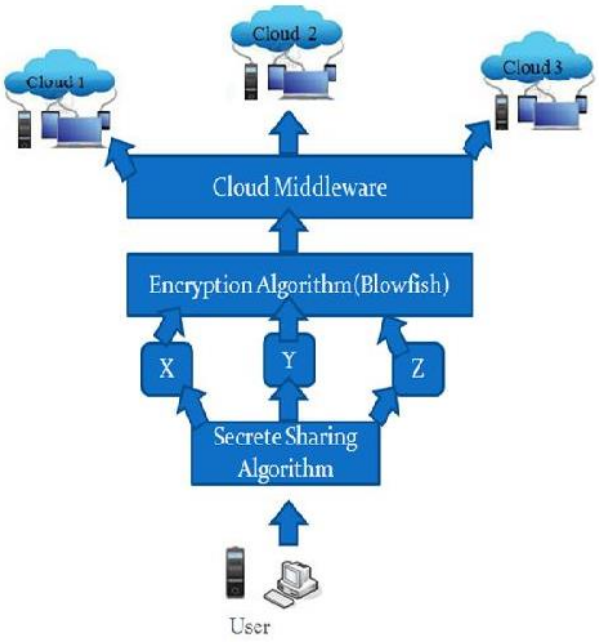

Figure 2. Proposed Architecture for Cloud Computing

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

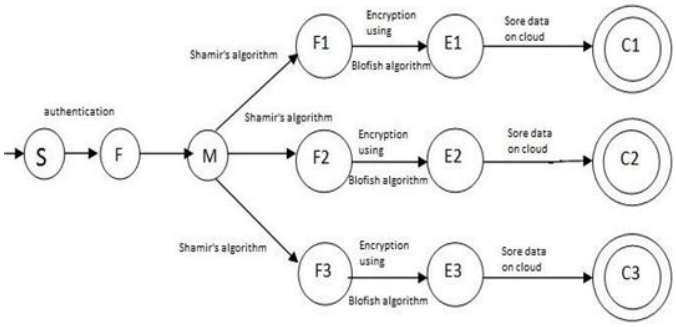

Figure 3. Uploading of Data from User

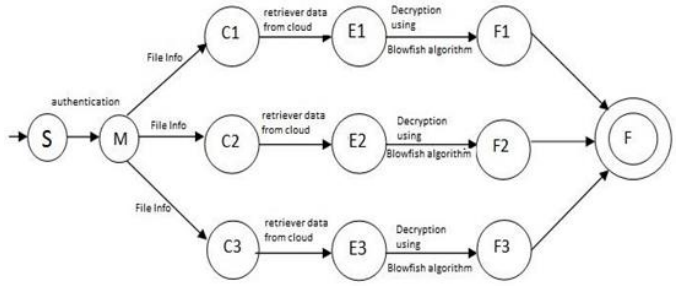

Figure 4. Retrieving of Data from Cloud

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 usage 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. REFERENCES

[1]. Y. Zhu and H. Hu, "agreeable provable information ownership for respectability check in multicloud capacity", IEEE exchanges on parallel and dispersed frameworks, Vol. 23, 2012, pp. 2231-2244.

[2]. G. Ateniese, R. Consumes, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Tune, "Provable information 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, "Proficient remote information ownership checking in basic data frameworks", IEEE Transactions on Knowledge and Data Engineering, Vol. 20, 2008, pp. 1034 - 1038.

[4]. Juels and B. Kaliski, "PORs: Proofs of retrievability for huge records", In ACM CCS '07, 2007, pp. 584-597.

[5]. R. Curtmola, O. Khan and R. Consumes, "Strong Remote Data Checking", in fourth ACM StorageSS, 2008, pp.63-68.

[6]. B. Srinivas, Shoban Babu Sriramoju, "A Secured Image Transmission Technique Using Transformation Reversal" in "International Journal of Scientific Research in Science and Technology", Volume-4, Issue-2, February-2018, 1388-1396 [Print ISSN: 2395-6011 | Online ISSN: 2395-602X]

[7]. B. Srinivas, Shoban Babu Sriramoju, "Managing Big Data Wiki Pages by Efficient Algorithms Implementing In Python" in "International Journal for Research in Applied Science & Engineering Technology (IJRASET)", Volume-6, Issue-II, February-2018, 2493-2500, [ISSN : 2321-9653]

[8]. Shoban Babu Sriramoju, "Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol 6, Issue 12, December 2017, DOI 10.17148/IJARCCE.2017.61212 [ISSN(online) : 2278-1021, ISSN(print) : 2319-5940]

[9]. Shoban Babu Sriramoju, " Review on Big Data and Mining Algorithm" in "International Journal for Research in Applied Science and Engineering Technology", Volume-5, Issue-XI, November 2017, 1238-1243 [ISSN : 2321-9653], www.ijraset.com

[10]. B. Srinivas, Gadde Ramesh, Shoban Babu Sriramoju, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 1692-1697, [ISSN(ONLINE): 2395-1052]

[11]. B. Srinivas, Gadde Ramesh, Shoban Babu Sriramoju, "An Overview of Classification Rule and Association Rule Mining" in "International Journal of Scientific Research in Computer Science, Engineering and Information Technology", Volume-3, Issue-1, February-2018, 643-650, [ISSN : 2456-3307]

[12]. Shoban Babu Sriramoju, "OPPORTUNITIES AND SECURITY IMPLICATIONS OF BIG DATA MINING" in "International Journal of Research in Science and Engineering", Vol 3, Issue 6, Nov-Dec 2017 [ISSN : 2394-8299].

[13]. Dr. Shoban Babu Sriramoju, Prof. Mangesh Ingle, Prof. Ashish Mahalle "Trust and Iterative Filtering Approaches for Secure Data Collection in Wireless Sensor Networks" in "International Journal of Research in Science and Engineering" Vol 3, Issue 4, July-August 2017 [ISSN : 2394-8299].

[14]. Dr. Shoban Babu, Prof. Mangesh Ingle, Prof. Ashish Mahalle, "HLA Based solution for Packet Loss Detection in Mobile Ad Hoc Networks" in "International Journal of Research in Science and Engineering" Vol 3, Issue 4,July-August 2017 [ISSN : 2394-8299].

[15]. Shoban Babu Sriramoju, "A Framework for Keyword Based Query and Response System for Web Based Expert Search" in "International Journal of Science and Research" Index Copernicus Value(2015):78.96 [ISSN : 2319-7064].

[16]. Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].

[17]. Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].

[18]. Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2014 [ISSN : 2249-4510]

[19]. Mounica Doosetty, Keerthi Kodakandla, Ashok R, Shoban Babu Sriramoju, "Extensive Secure Cloud Storage System Supporting Privacy-Preserving Public Auditing" in "International Journal of Information Technology and Management" Vol VI, Issue I, Feb 2012 [ISSN : 2249-4510]

[20]. Shoban Babu Sriramoju, "An Application for Annotating Web Search Results" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[21]. Monelli Ayyavaraiah, "Nomenclature of Opinion Miningand Related Benchmarking Tools" in "International Journal of Scientific & Engineering Research" Vol 7,Issue 8, February 2018, [ISSN 2229-5518]

[22]. Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198

[23]. Ajmera Rajesh, Siripuri Kiran, " Anomaly Detection Using Data Mining Techniques in Social Networking" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1268-1272 [ISSN : 2321-9653], www.ijraset.com

[24]. Siripuri Kiran, Ajmera Rajesh, "A Study on Mining Top Utility Itemsets In A Single Phase" in "International Journal for Science and Advance Research in Technology (IJSART)", Volume-4, Issue-2, February-2018, 637-642, [ISSN(ONLINE): 2395-1052]

[25]. Shoban Babu Sriramoju, "Multi View Point Measure for Achieving Highest Intra-Cluster Similarity" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 2,Issue 3,March 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[26]. Shoban Babu Sriramoju, Madan Kumar Chandran, "UP-Growth Algorithms for Knowledge Discovery from Transactional Databases" in "International Journal of Advanced Research in Computer Science and Software Engineering", Vol 4, Issue 2, February 2014 [ISSN : 2277 128X]

[27]. Monelli Ayyavaraiah, "Review of Machine Learning based Sentiment Analysis on Social Web Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 4,Issue 6,March 2016 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[28]. Ajay Babu Sriramoju, Dr. S. Shoban Babu, "Study of Multiplexing Space and Focal Surfaces and Automultiscopic Displays for Image Processing" in "International Journal of Information Technology and Management" Vol V, Issue I, August 2013 [ISSN : 2249-4510]

[29]. Dr. Shoban Babu Sriramoju, "A Review on Processing Big Data" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol-2, Issue-1, January 2014 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]

[30]. Monelli Ayyavaraiah, " A Study on Large-Scale Cross-Media Retrieval of Wikipedia Images towards Visual Query and Textual Expansion" in "International Journal for Research in Applied Science and Engineering Technology", Volume-6, Issue-II, February 2018, 1238-1243 [ISSN : 2321-9653], www.ijraset.com

[31]. Ramesh Gadde, Namavaram Vijay, "A SURVEY ON EVOLUTION OF BIG DATA WITH HADOOP" in "International Journal of Research in Science and Engineering", Vol-3, Issue-6, Nov-Dec 2017, 92-99 [ISSN : 2394-8299].

[32]. Namavaram Vijay, S Ajay Babu, "Heat Exposure of Big Data Analytics in a Workflow Framework" in "International Journal of Science and Research", Volume 6, Issue 11, November 2017, 1578 - 1585, #ijsrnet

[33]. Ajay Babu Sriramoju, Namavaram Vijay, Ramesh Gadde, "SKETCHING-BASED HIGH-PERFORMANCE BIG DATA PROCESSING ACCELERATOR" in "International Journal of Research in Science and Engineering", Vol-3,

Issue-6, Nov-Dec 2017, 92-99 [ISSN : 2394-8299].

[34]. Namavaram Vijay, Ajay Babu Sriramoju, Ramesh Gadde, "Two Layered Privacy Architecture for Big Data Framework" in "International Journal of Innovative Research in Computer and Communication Engineering" Vol 5, Issue 10, October 2017 [ISSN(online) : 2320-9801, ISSN(print) : 2320-9798]