© 2018 IJSRST | Volume 4 | Issue 3 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
29th January 2018
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur, Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

Single to Mlticloud Security (By Parts)

Harshal S. Wankar, Gaurav Jasutkar, Arati Chipate
Anjuman College Of Engineering And Technology, Department of Computer Science and Engineering, Sadar Nagpur , Maharashtra, India

ABSTRACT

Cloud computing is largely viewing technology in software industries. It is adopted as service program, where users can remotely depot their data into the cloud so as to take advantage of on-demand high quality services from a shared set of manageable computer devices. Cloud computing offers large benefits to its users, But it also remain with a set of problems and unpredicted decision which security is the biggest concern. Now days cloud computing is very beneficial to its user for shearing a data with other without threating by unwanted user access. To access the security level on cloud storing data partition of data is done. The partition of data is not the final storage in cloud it just a middle step of process. The parts of data is get encrypted with secret shearing schema are used to restrict the unwanted access to the restricted data. The secret shearing schema is also get upgraded by adding Shamir's secret shearing concept in it. Threshold secret sharing schema in which all the participants are needed in reconstruction phase this is required for reconstruct the secret. With these in feature easy data outsourcing with the help third party storage service providers. It has a considerable potential as similar process for traditional silo computing. The Shamir's secret shearing schema is help to store the parted data in the different cloud with proper rearrangement method with it. The threated data from one cloud get corrupted or loss but the original data can be recover with other clouds data. Data encryption, threshold secret shearing schema, Shamir's secret shearing algorithm is the mainly used for the securing data outsourcing. In this paper Shamir's secret shearing schema with the utilization of partition of data is used in multi cloud environment.

I. INTRODUCTION

The main goal of this project is to increase the security of cloud database for cloud computing community with third party utilization. These kind of security is achieved by implementing Shamir's secret shearing algorithm with the addition concept of data partition before algorithm performance. The data parts get separate implementation of Shamir's secret shearing algorithm which again get divided into parts on the bases of Shamir's algorithm. The Shamir's use data encryption for better security by making the double time divided data into the unreadable format. In this system the encrypted data get stored into the different cloud for higher security provision. It can improve the performance with fast processing of data in clouds. It get better in MULTI – CLOUD environment.

- Better performance
- Fast data Service

- Increase

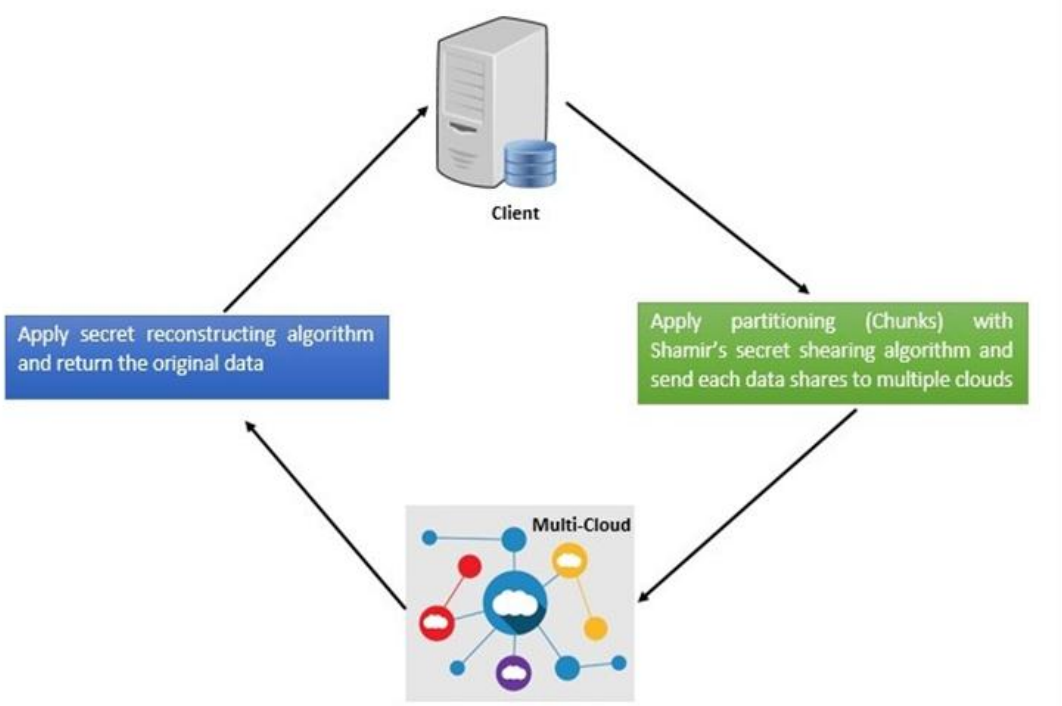

Figure 1. Block Diagram of Secret Shearing algorithm

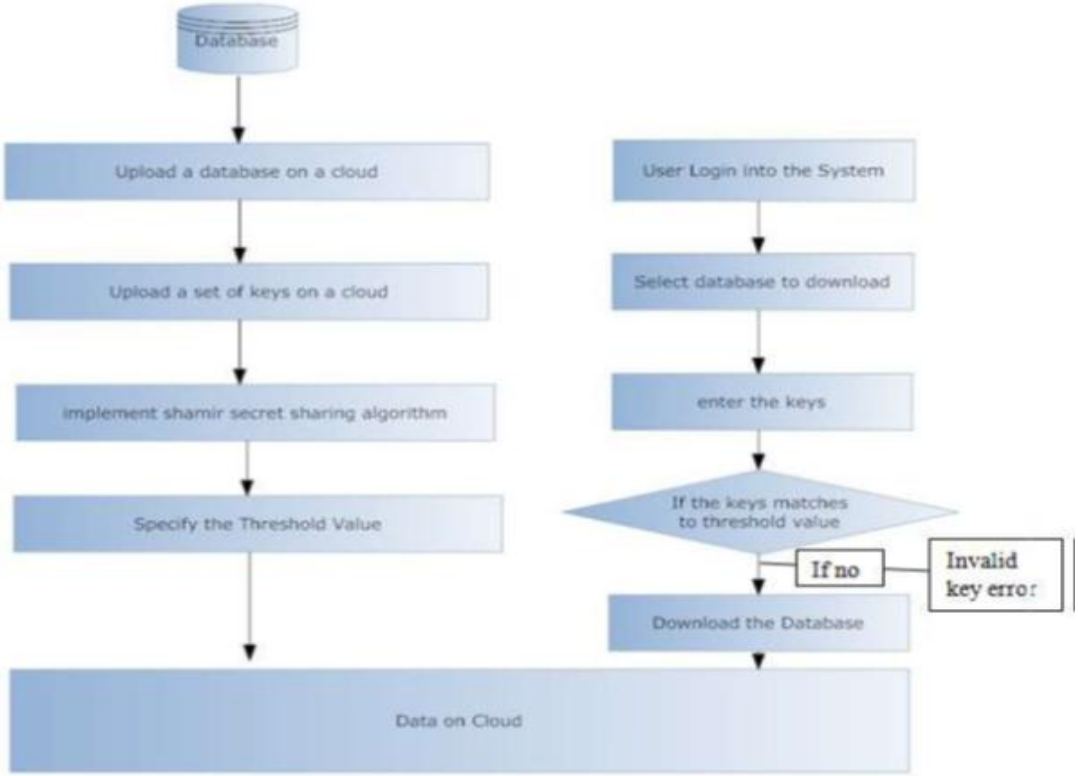

Figure 2. Architecture Design

II. MULTI-CLOUD

Multi-Cloud is a collection of several clouds. In a single cloud infrastructure if the data in single cloud get corrupted then there is a loss of data is occur. Multi-Cloud environment solve this problem by containing the data in multiple cloud if one cloud data is get corrupted then it can be recover from the other clouds. The replication of data in multiple clouds can save the loss of data fact. So when one cloud get attack by the threat then it data can be save with its replication in other cloud.

2.1 CLOUD SERVICE MODELS

- IAAS – Infrastructure as a service should fulfill the essential characteristics to support cloud services. It is built using a shared pool of computing resources, such as virtual compute, virtual storage, operating systems and virtual network.
- PAAS – Platform as a service is within IAAS. Within the PaaS model, customer's area unit supplied with associate degree package, artificial language execution setting, database, and internet server. They're not concern with the price and management within the hardware and package layers. PaaS is that the use of cloud computing to supply platforms for the event and use of custom applications. The PaaS solutions embody application style and development tools, application testing, versioning, integration, readying and hosting, state management, and different connected development tools.
- SAAS - Software-as-a-Service could be a computer code distribution model during which applications are hosted by a vender or service supplier and created accessible to customers over a network, usually the net.

III. SHAMIR'S SECRET SHEARING ALGORITHM

The Shamir's secret shearing algorithm is divide the data into the parts and after that it encrypt the data. Stored the encrypted data into the multiple clouds.

3.1 MATHEMATICAL DEFINITION

The goal of the algorithm is to divide the data DATA into n pieces (PART1, PART2, PART3, PART4 ….. PARTn) so that,

1. Retrieving any k or more PARTi pieces makes PART easily computable.

2. Retrieving any k-1 or fewer PARTi pieces leaves PART thoroughly undetermined.

The above scheme is known as threshold (k, n). If k=n, then all pieces are available for reconstruction of DATA. The objective of Adi Shamir's secret sharing algorithm algorithm is that, k points are enough to define a polynomial of degree k-1.

Example, 2 points are sufficient to define a line.

Choose an approximate k-1 coefficients c0, c1, c2, c3….ck-1 in H, and let c0 = S, where S is the Secret data which is going to be stored in cloud. Build the polynomial $H(z) = c0 + c1z1 + c2\ z2+……+ck-1zk-1$. Then n points are defined, for example set i=1,2….n to retrieve (i, H(i)) . A pair is formed with input to the polynomial and output.

Given any subset of k of these pairs, using interpolation the coefficients of the polynomial can be found and the constant term a0 is the secret.

SHAMIR'S APPROACH

The secret is divided into pieces by considering an approximate degree polynomial

$H(z) = c0 + c1z1 + c2\ z2+\ldots\ldots+ck\text{-}1zk\text{-}1$

In which $c0 = S$, $S1 = H(1)$, $S2 = H(2)$,……, $Sn = H(n)$ and represent each share as a point

$(zi, G(zi) = yi)$

IV. TECHNOOGY

HARDWARE REQUIREMENT

1. Processor - Pentium-iii
2. Speed - 1.1GHz
3. RAM - 256 MB(min)
4. Hard Disk - 20 GB
5. Keyboard - standard keyboard

SOFTWARE REQUIREMENT

- ✓ Operating system – windows xp
- ✓ Front end – HTML,JAVA,JSP
- ✓ Script – java script
- ✓ Database – MYSQL
- ✓ Ellipse - Oxygen

V. CONCLUSION

- This study is carried out to design single and multi-cloud using secret key sharing algorithm which will result in deduction of the cost for the physical infrastructure, reducing the cost entry and execution as well as the response time for various associated applications.
- Also the disadvantages of single cloud and advantages of multi-cloud were addressed in this paper.
- Customer do not want to lose their private information as a result of malicious insiders in the cloud.