International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211
Volume 10, Issue 1, January-2022, Impact Factor: 7.429, Available online at: www.ijaresm.com

Secure Multi-Clouds Database: A New Approach to Provide Security in Cloud Computing

Dr. Varsha S. Tondre

Brijlal Biyani Science College, SGB Amravati University, Amravati, MS. India

---

ABSTRACT

Cloud computing is a type of computing that shares computing resources on the internet. It means "A type of Internet-based computing", which provides different types of services to users such as servers, storage space, and devices through the Internet. "Single cloud", may lead to security problems like service availability failure, data loss. There might also exist a possibility of malicious insiders in a single cloud. Bessani [1] presents multi-cloud or cloud-of-clouds that decreases security risks in cloud computing. This paper focuses on multi-cloud to enhance security by dividing reliability, trust, and security among multiple cloud providers.

This paper proposed a new model of "Secure multi-cloud database framework" which is based on multi-cloud providers rather than the single cloud provider. This framework compromises with Shamir's secret sharing approach, Byzantine Fault Tolerance in a multi-cloud computing environment, and also applies MDE (Model-Driven Engineering).

Keywords – Multi-cloud, Secret sharing algorithm, Byzantine Agreement protocols, Byzantine fault tolerance, Model-driven engineering.

1. INTRODUCTION

Users can access cloud services everywhere at any time. Hence, the use of the cloud has increased in the IT sector and organizations. Both the small as well as large organizations store their critical data in the cloud service provider rather than store data on their own server. Cloud users encounter numerous security lapses in cloud storage due to flaws in software and hardware. Their important requirement is data security. Constructing a highly secured and reliable cloud system has become a critical research issue.

The multi-cloud also called cloud-of-clouds, aims at reducing the risk of service availability failure, corruption of data, loss of privacy, and the possibility of malicious insiders in the single cloud. Using a multi-cloud environment, cloud users never face a lack of availability of a service or a resource at any point in time and could prevent potential loss.
Any faults in cloud computing are called Byzantine faults. This fault can be caused by any malicious attack or operator error. The proposed model of Byzantine agreement protocols detects Byzantine faults before causing any bad impact on the system.

Many vendors deliver a Platform as a service, which provides the components that they require to develop applications and operate applications over the network. Different vendors provide different platforms, if an application is built to deploy on one platform cannot switch to other platforms, then it results in a critical issue called vendor lock-in. As a solution to this problem, this paper proposed a framework that works as a runtime environment for the development and execution of an application based on Model-Driven Engineering (MDE).

The latter half of this paper is organized as below:
Section II describes the basic architecture of our model, Section III explains the algorithm used in our model i.e. Secret sharing algorithm, Section IV explains our model with byzantine fault tolerance, Section V illustrates Model-Driven Engineering (MDE), Section VI concludes with the proposed model.

II. Proposed Model:

2.1. Secure Multi-cloud database model(SMCDM):

SMCDB provides database storage in a multi-cloud service provider. It uses a database management system to manage and control the transaction between the clients and service providers. SMCDB contains three layers first presentation layers, which contains the user's browser and HTTP server, second application layer contains servlet engine and third layer i.e. is management layer contains DBMS and database, service provider.

SMCDB preserves the security and privacy of data by applying multi shares techniques on multi-cloud providers.

2.2.SMCDB Data flow:

Sending data procedure (Fig.1):

a) A user sends a query by using a user interface and a web browser through an HTTP request.
b) The user's query will be sent through the HTTP server to a Servlet Engine by an application request.
c) When the query arrives at the data source, the DBMS will manage this query and send it to the CSP.
d) After the result of the query is returned to the DBMS, the DBMS returns this query result to the Servlet Engine and then the HTTP server returns the result of this query to the user interface again.

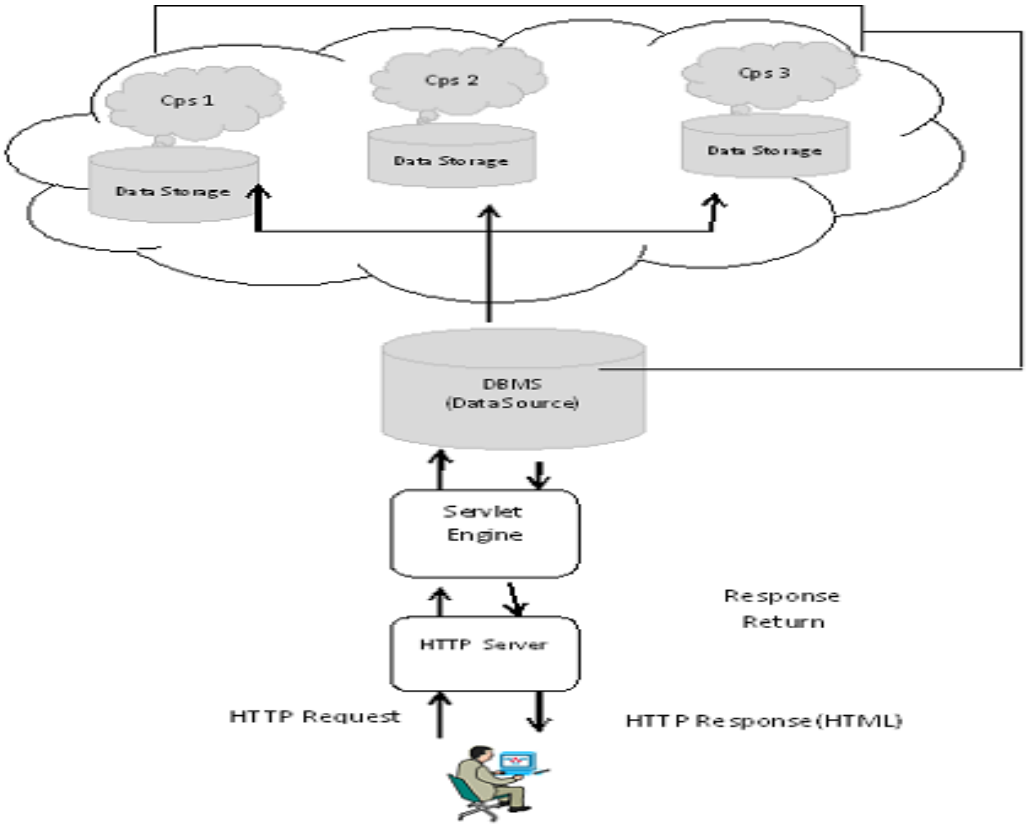

Figure 1: A General Overview of Multi-Cloud.

3. Algorithm Used:

3.1.Shamir's Secrete sharing algorithmstrategy:

The secret sharing technique was proposed by Adi Shamir [2][3]. In this technique, a secret or piece of data is distributed among a group of n participants. This method allows a subset of participants to reconstruct secrets rather than all n participants to reconstruct secrete. But any less subset k participants out of n shares cannot obtain secrete.

- Consider secreting S divide into n shares S1, S2….Sn in such a way that:
  – Knowledge of any ≧k shares can reconstruct the secret value S.
  – Knowledge of any ＜k pieces cannot get sufficient information to reveal the secret value S.

Where k is shares or subset of n shares recover the secrete.

- This scheme is called as (k, n) threshold scheme. If k equals n then all participants are required together to reconstruct the secret. But k-1 shares give no information of secrete.

- Definition: A (k, n)- threshold scheme is a method in which a message S is shared among a set of n participants such that any subset consisting of k participants can reconstruct the secrete S, but no subsets of a smaller size can reconstruct S [4].

- Suppose we want to use (k, n) threshold scheme to share our secret S where k < n.

Let us consider if k=3 then any three people could reconstruct polynomial and obtain secrete. If we use the polynomial of degree k-1, there is no way that a k-1 person can obtain information about the message with only their data.

Therefore, k people are required to obtain the message.

3.2. General Data Flow Scenario:

1. First, the DBMS component receives a request from a user.
2. Next, it divides the received data that the client wants to hide from an untrusted cloud provider, into n shares or chunks.
3. After dividing the data into 3 shares and storing them in different CSPs, the database management system generates a random same degree polynomial function, one for each CSP and creates the shares which are distributed to the defined cloud providers.
4. In order to retrieve data the user's querymust reachthe DBMS and DBMS should rewrite the query again to retrieve the result from the relevant share from CSP.
5. Once the data is received from the multi-cloud, DBMS computes the secret value of the coming result and sends it to the concerned requester client (Fig. 2).

4. Byzantine Fault Tolerance:

In previous research [1], the Byzantine fault tolerance strategy and its protocol were explained. Now, BFT is implemented in the proposed model to detect Byzantine faults in multi-cloud computing. Computing system faults, ranging from accidental crash faults to arbitrary faults, are often called Byzantine.

In the BFT which has three clouds centrally controlled by the cloud manager, the cloud manager is responsible for sending a sequence of user's requests to the clouds. The BFT consists of three components:

a) First, the cloud manager is responsible for sending queries from the cloud to a client and applying Shamir's Secrete sharing approach, also responsible for retrieving voting results from the clouds before sending them to the client.
b) Second, communication protocol offers BFT, which communicates with clients and the cloud for requests.
c) Third, the cloud side is responsible for performing the client queries on Shamir's data (the hidden data by Shamir's secret sharing approach) before sending responses to the cloud manager (Fig. 3)

The Majority voting was applied on the retrieved results from the multi-clouds to the voter unit inside the cloud manager to find out whether a cloud is faulty or not.

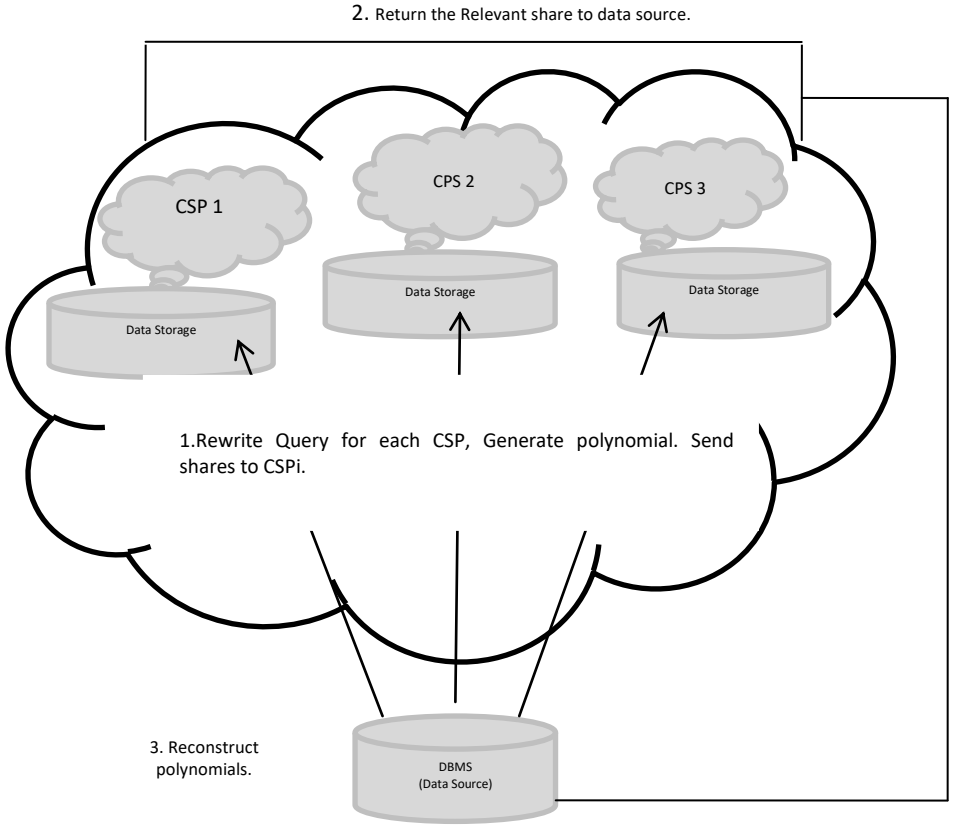

Fig. 2:Procedure between DBMS/CPS [3].

5. Model-Driven Engineering (MDE):

In our proposed model, the development and execution of an application are based on Model-Driven Engineering (MDE), to avoid vendor lock which provides portability between different platforms and allows the developer to

develop an application with the same design but still move towards a different platform. MDE helps developers to port applications from one platform to other platforms without understanding different cloud platforms by switching software development from design to deployment [6].

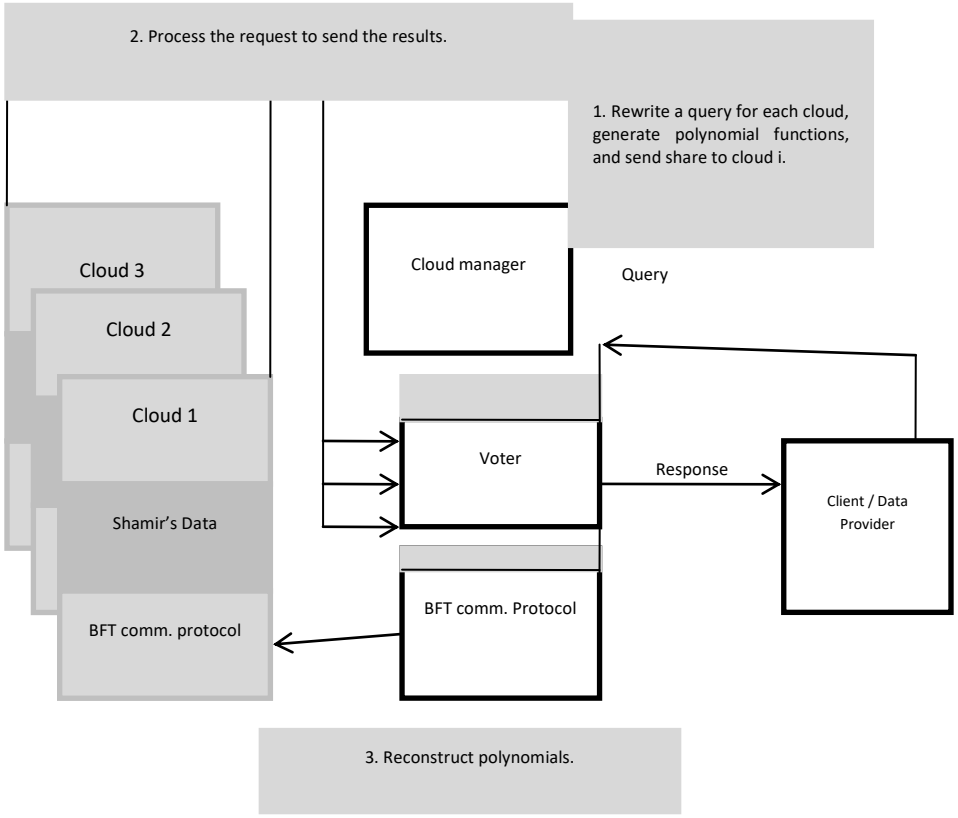

Fig. 3: BFT Overview [4].

1. Intruder hacked cloud provider password and they are able to access all instances and resources. But in our model, if a hacker hacks one cloud's password or even two cloud's passwords, they still need to hack the third cloud to know the secret, which is most difficult.
2. Replicating data into multi-cloud using a secret sharing algorithm may reduce the risk of data intrusion and increase data integrity.
3. Proposed model improves the flexibility of cloud storage.
4. Because of the replication technique, if one of the clouds may be fails then the alternative cloud is able to perform users operations.
5. This framework provides the portability of applications from one platform to other.
6. If one of the cloud failures still user retrieves data from other cloud providers.
7. By using Secrete sharing approach data is secured and easy to maintain a large database with security.

Limitations:

1. This proposed model allows users to switch from one platform to another by the same design implemented on a different platform. But this model could not protect user design from malicious attacks when moving from one to another platform.
2. Using Shamir's secret scheme, there is the complexity of computing to reconstruct secrets.

CONCLUSION

It is clear that security issue is much important in the cloud environment. This issue causes many problems for a customer of cloud computing. Every user wants data security while using the cloud, there might be a failure due to various Byzantine failures in the software, hardware, or attacks from malicious insiders.

The model presented in this paper relies on a novel approach that combines Byzantine Agreement protocols along with Shamir's secret sharing approach to detect a Byzantine failure in the multi-cloud computing environment as well as to ensure the security of data stored within the cloud. MDE helps to automate the translation from design into the

implementation which addresses the vendor lock-in problem.

In this work, to mitigate the threats facing cloud storage, we extended the cloud data storage to include multiple service providers, where all cloud storage represents a different service provider.

REFERENCES

[1] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
[2] Md KausarAlam, Sharmila Banu K, ,"An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds",International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.
[3] Venkatarao Matte1, L. Ravi Kumar2, "A New Framework for Cloud Computing security using Secret Sharing Algorithm over Single to Multi-Clouds.", International Journal of Computer Trends and Technology, volume 4, Issue8, August 2013.
[4] Mohammed A. AlZain, Ben Soh and Eric Pardede, "MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.
[5] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences, 2012.
[6] I. Sapthami , P. Srinivasulu, B. Murali Krishna, "A Novel Approach to Cloud Computing Security over Single to Multi Clouds", Journal of Engineering Research and Application,Vol. 3, Issue 5, Sep-Oct 2013, pp. 636-640.
[7] Mohammed A. AlZain, Ben Soh and Eric Pardede, "A Byzantine Fault Tolerance Model for a Multi-Cloud Computing", IEEE 16th International Conference on Computational Science and Engineering, 2013.
[8] W. Trappe and l.C. Washington, Introduction to Cryptography with Coding Theory, Pearson International Edition, 2006.
[9] Nacha ChondamrongkulPunnarumulTemdee, "Multi-Cloud Computing Platform Support with Model-Driven Application Runtime Framework", 13th International Symposium on Communications and Information Technologies, 2013.
[10] R. Kondabala, M. Arathi , "Multi Cloud Computing Security", International Journal of Engineering Research and Sports Science, Vol. 1, Issue 6, June 2014.
[11] MonaliShrawankar, Associate Prof. Ashish Kr. Shrivastava, "Security Threat Solution over Single Cloud To Multi-Cloud Using DepSky Model", IOSR Journal of Computer Engineering , Volume 14, Issue 1, Sep. - Oct. 2013, pp. 71-76.
[12] Prof.V.N.Dhawas,PranaliJuikar,NehaPatekar,NehaLendghar,SushantVartak, "A Secured Cost Effective Multi-Cloud Storage in Cloud Computing", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013..
[13] S. B. Shivakumar, Ramesh B. E., Kavitha G. M., Mala M., "Multi Cloud Architecture for Improved User Experience", International Journal of Inventive Engineering and Sciences, Volume-1, Issue-7, June 2013.
[14] A. Waghmare, R. Patil, P. Mane, S. Bhosale, "Data Storage in Secured Multi-Cloud Storage in Cloud Computing", International Journal of Computational Engineering Research, Vol, 04, Issue 2, Feruary 2014.
[15] T.Kariya, Dr. V.M. Thakre, Dr. V.S. Tondre, "A Review On Multi Cloud Security", Global Journal Applied Social, Political, Sports & Science, 2014, pp. 40-48.