INTEGRATING HETEROGENEOUS DATA ON CLOUD

Deepali Tripathi[1], Dr. N. K. Joshi[2]

[1]Research Scholar, MIMT, Kota, Raj. (India)

[2]Professor, Modi Institute of Mgmt and Technology, Kota, Raj. (India)

ABSTRACT

In this cloud era business undertakings are moving towards distributed computing, the assorted volume and speed of the cloud is required to adapt up to the desires. This paper proposes a model for incorporating heterogeneous information on the cloud, based on security algorithms for Data Encoding, Data Decoding and Load Balancing. For the support of system we also use periodically Monitoring Algorithm that executes periodically to monitor the load and then call balancing algorithm as needed. The paper plans to give an answer for the heterogeneous information joining issue on cloud and information security along with Resource Management. The proposed model focuses on service oriented implementations of various algorithms.

I. INTRODUCTION

As cloud computing is a flexible computing mode, more and more enterprises' application systems are migrated to cloud environment, large amount of business data is stored in different data nodes. Data location and organization are transparent to users, the heterogeneous data is distributed in different cloud node, each node only contains part of the information that users need, so it is necessary to effectively manage the heterogeneous cloud data, forms a giant data pool that masked the distribution, heterogeneity and complexity of the data resource, ensures efficient using of data services in cloud environment, realizes data integration and data operation transparency.

II. PROPOSED MODEL

This paper presents a novel heterogeneous secure data integrity model, the model consists of all the aspects of heterogeneous data collection in cloud environment, including: data resource description, physical and logical storage management and encryption, decryption etc. Meanwhile, this paper presents the main problems of data security in cloud environment and key implementation technologies of the model. This paper gives a good solution for heterogeneous data security management and application in cloud.

The proposed model is consist of basic 2 sub modules.

(i) Upload Module

(ii) Download Module

2.1 Upload Module

This module comes in role when a client is uploading the data on server. It has following steps:

- Creation of separate data base for each client.
- Conversion of uploaded data/file in binary text format.
- Applying Encryption algorithm on Binary Text.
- Storing encrypted data in the database.

Creation of Data Base: In this step when user Registered himself on the server a new separate data base is created on cloud separately dedicated to the particular client.

It results in data separation approach for each user.

Conversion of file: In this step when any type of data (jpg,jpeg,pdf,doc,docx,txt,etc.) is uploaded on the server then data is first converted in binary text format by using conversion algorithm.

2.1.1 Conversion Algorithm

Step 1: First read the file extension and size.

Step 2: Now convert the file into Buffer Byte Stream (HEX Format).

Step 3: Apply Hex to binary conversion concept on the stream.

Step 4: Apply Bit Exchange method on binary stream.

Step 5: Now pass this result to next STEP.

2.1.2 Encryption Algorithm

Step1: Input the text and the key (User id).

Step2: Add the key to the text.

Step3: Convert the previous text to ASCII code.

Step4: Convert the previous ASCII code to binary data.

Step5: Find out One’s complement of the previous binary data.

Step6: Gather each 8 bits from the previous binary data and obtain the Decimal value from it.

Step7: Divide the previous Decimal value by 4.

Step8: Obtain the ASCII code of the previous result divide and put it as one character.

Step9: Obtain the remainder of the previous divide and put it as a second character.

Step10: Return encrypted text.

Storing in the database:

In this step the encrypted text passed by previous step is stored in the database Table as String type data.

Data Base table mainly has three columns

i. Name of the File
ii. Encrypted text
iii. Extension of the file.

So there is no file, no folder and no image exist on the server it only has data base table.

2.2 Download Module

This module comes in role when a client is downloading previously uploaded data from the server. It has following steps:

- Selecting the required data from database.
- Converting data in binary text format using Decryption.
- Converting Binary Text data in required format or file.
- Downloading the data or file on Client Machine.

Selecting the required data: First when client logged in to his account then a table of previously uploaded files is shown to the client and client will select the required data to be downloaded and click on the link. As per client request query is fired and Encrypted text is retrieved from the data base and passes to the next step.

2.2.1 Decryption Algorithm

Step1: Input the encrypted text and the key.

Step2: Loop on the encrypted text to obtain ASCII code of characters and add the next character.

Step3: Multiply ASCII code of the first character by 4.

Step4: Add the next digit (remainder) to the result multiplying operation. (Consider result as Decimal value).

Step5: Convert the previous Decimal value to binary data.

Step6: Find out One’s complement of the previous binary data.

Step7: Gather each 8 bits from the previous binary data and obtain the ASCII code from it.

Step8: Convert the previous ASCII code to text.

Step9: Remove the key from the text.

Step10: Return decrypted data.

2.2.2 Conversion of the Data

Step 1: First read the Decrypted text.

Step 2: Apply Reverse Bit Exchange method on binary stream.

Step 3: Apply Binary to HEX conversion concept on the text.

Step 4: Now write this text in buffer byte format array.

Step 5: Now pass this result to next STEP.

Downloading File to the Client Machine:

Now finally the Buffer Byte Stream array is written to the client machine with the same filename and extension provided by client.

And in this way client will have its data file as it was uploaded. But in the meanwhile this data was not in such format on server as it is to be supposed to. In such a way we have created a new Service for heterogeneous data integrity on Infrastructure of the cloud

But as it is cloud it can have different types of problems regarding the data storage so for this purpose we used two algorithms as additional feature to our model.

2.2.3 Load Balancing Algorithm

Step1: Calculate the current load.

Step2: Now take total data load of data source and calculate average load.

Step3: Now check data load of each node and assign weight to it.

Step4: If data load is greater than average value then migrate the data to the unloaded node.

Step5: Repeat above for each node.

IV. CONCLUSION

The cloud computing platform has very good ability for flexibility but the issues regarding the security of data remains same as it is open for all. But our model provides an additional service layer to the cloud environment which secures every and each type of data uploaded on the server as well as monitoring its load. The model proposed in this paper gives a novel solution to the security issues of data storage on cloud environment. This model is feasible enough to be implemented on any cloud storage regardless of its vendor as it is an additional service layer which ads up the security to the data. More security algorithms and other techniques can be implemented to this model in future.

REFERENCES

Journal References

[1] J. Shute, M. Oancea and S. Ellner, “F1: The fault tolerant distributed RDBMS supporting google's ad business”, Proc of SIGMOD, New York: ACM, **(2012)**, pp. 767-778.

[2] G. DeCandia, D. Hastorun and M. Jampani, “Dynamo: amazon's highly available key value store”, Proc of SOSP, New York: ACM, (2007), pp. 205-220.

[3] K. Shvachko, H. Kuang, S. Radia and R. Chansler, “The Hadoop distributed file system”, Proc. of the IEEE 26th Symp. On Mass Storage Systems and Technologies(MSST), Lake Tahoe: IEEE, (2010), pp. 1-10.

[4] K. C. Birman and G. van Renesse, “Toward a cloud computing research agenda”, ACM SIGACT News, vol. 40, no. 2, **(2009)**, pp. 68-80.

[5] T. Hirofuchi, H. Nakada and H. Ogawa, “A live storage migration mechanism over wan and its performance evaluation”, VTDC'09. Barcelona, Spain: ACM, (2009), pp. 67-74.

[6] D. Tripathi, “Development Trends and Evolution of SOA”, National Conference on Emerging Trends in Mechanical, Electronics and Computer Engineering, April 2010, pp 139-143.

[7] Craig Gentry, A Fully Homomorphic Encryption Scheme, 2009 http://crypto.stanford.edu/craig/craig-thesis.pdf

[8] New encryption method promises end-to-end cloud security, by Kevin McCaney Jun 13, 2013 - http://gcn.com/Articles/2013/06/13/ Encryption -endto-end-cloud-security.aspx?Page=1