International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 07, July 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A SECURE FRAMEWORK FOR DATA EXODUS IN THE CLOUD

Mr.J.V.Krishna[1], Dr. G.Apparao Naidu[2], Dr. Niraj Upadhayaya[3]

[1]Working as Assoc. Professor & HOD, CSE Dept. at SVIST, Krishna Dist. (India)

[2]Working as Professor, CSE Dept., J.B.Institute of Engineering and Technology, Hyderabad. (India)

[3]Working as Professor, CSE Dept.& Principal,J.B.Institute of Engineering and Technology, Hyderabad. (India)

ABSTRACT

Cloud computing has gained a lot of significance in very short span of time as it offers the flexibility, security and promptness. Cloud computing is opted by many big organizations to have a prompt response to their clients located globally without any disruption. As the growth in this platform is enormously high the main concern which comes into picture is security issue. We propose a system which is more robust to the environment and thus will carry out the complete process in the secure and efficient manner with data exodus in the cloud.

Keywords: Cloud Computing; Disruption; Robust; Exodus.

I. INTRODUCTION

Cloud Computing is the process of sharing the data across globe and storing large amount of data which a normal server cannot withhold. Cloud computing is delivering the data to the client as and when the request reaches the server. Cloud can deliver both software and infrastructure as a service. The name resembles the shape of cloud as we cannot set the maximum size for cloud, in the same manner there is no limit for the storage of data. Cloud Computing takes care about the information stored in the cloud by assigning the task to TPA (Third Party Auditor). Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) across the network. Evolution of cloud computing is the broader concept of converged infrastructure and shared resources. Cloud Computing is the technology which has gained a lot of importance in the current day market, because of the demand in the market the other way there is a big risk which is the concern with security. Cloud definition in general resembles to the real time cloud that we see in the sky i.e. there is no boundary or end point to the cloud storage. Cloud computing stores large amount of data related with many companies and TPA who is actually considered to the cloud person acts as a mediator for client and company.

International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 07, July 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

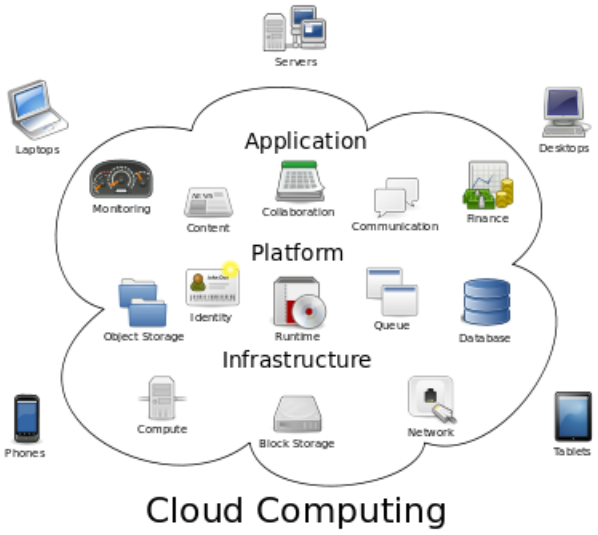

Fig 1: Cloud Computing Architecture

Cloud Computing is a combination of two technologies, namely Networking and Data Mining. To give the clear picture of the processing unit of Cloud Computing we need to consider an example, everyone accesses Gmail accounts for sending and receiving mails with attachments. Suppose there was an Excel sheet attached with the mail and sent to other user, in this scenario when the user who receives the mail does not have MS-Office installed in his system and also without downloading that file the user can read that Excel file in Gmail Server itself, the reason is that Google server maintains MS-Office and because of which users can read the files without downloading it. This overall process we can admit to Cloud Computing. Another concept which uses Cloud Computing architecture is social networking website "Facebook". Facebook is a social networking site which connects many users worldwide. A user who has an account with facebook the user id is generally gmail or yahoo or rediff mail id. The reason is that, any server is limited with a maximum bandwidth and if that limit crosses there is a chance that the user may not get the actual data which was requested. To overcome this problem the facebook has integrated the concept of Cloud computing i.e. account in facebook can have the credentials from other domains in the technology world like yahoo, gmail. The internal process that happens here is that all the databases related to these companies are kept in a common place and TPA is responsible for authenticating any user while logging in. In this project, we focus on the data exodus in the cloud. As there are many users accessing the cloud the main issue comes with the security for the data when data is migrated. In the existing system applications are built with many encryption schemes like Prediction Based Encryption. PBE is a combination of IBE (Identity Based Encryption) and ABE (Attribute Based Encryption). In IBE, an identity is taken from the input only like for an input "abc@mph.com" the encryption key will be abc and during the decryption when the user gives the key that will be compared from the input data only and on match the user can get the data requested. In the similar manner ABE is a kind of encryption scheme where it considers the attribute matching with the data. Say suppose the user has uploaded a file which corresponds to a specific department then key given to that file will surely be related with that department, purpose of doing so it to have a security to the data in the way that it can be accessed by genuine people only. As both these techniques are not providing

the expected security to safety level, we are going to have a system that can ensure security to the data present at cloud or even during the migration time.

II.RELATED WORK

Our implementation will have a technique that will make sure about the security and the safety of the data present at cloud. In the implementation of the proposed work, firstly a study is made on the Prediction based encryption technique that is actually lacking with the security because of the key selection factors. To overcome this drawback, with the PBE we are proposing a new technique i.e. Plain Cipher Encryption (PCE) and this technique involves two stages for converting data into cipher text. First it generates the key based up on the user data upload, i.e. taking the help of Random class available with the utility package where a series of random numbers will be generated and using each of these random numbers a character will be selected from the given set of characters. In this manner, a key will be selected by the application and thus given back to the user for that file which was being uploaded. Next the application moves to second step where the data will be encrypted i.e. converting the plain data to the cipher text. In the process of encrypting data, each character will be taken and its corresponding ASCII value will be taken and that value will be multiplied with a mathematical number and encoded with a special symbol for clear separation of data units. Here we are giving out the sample manipulations for the above process.

2.1 Key Generation Process

```
Char ch[]={‘A’,’B’,’C’,’R’,’W’,’Q’};
Random r=new Randm();
int i=r.nextInt();
int j=r.nextInt();
int k=r.nextInt();
int l=r.nextInt();
char ch1=ch[i];
char ch2=ch[j];
char ch3=ch[k];
char ch4=ch[l];
String key=ch1+ch2+ch3+ch4;
```

Key is the variable that stores the encryption key and that will be utilized for the process of Data Migration in the Cloud. As the key alone will not

be sufficient for the data security, we need to employ the data encryption scheme that will convert the data into cipher text,

2.2 Steps for Encrypting Data.

1. Read the data into a string variable
2. Data must be broken into characters and each character ,must be converted into its equivalent ASCII value
3. Running the loop converting the value into a new value and appending it with a special character
4. Finally an encrypted value will be retrieved in this step.

When above four steps are followed we can convert the plain data into cipher text and thus we are achieving good cover to complete data and thus it is made available for the user to do further processing like uploading it to cloud.

Coming with the uploading process, data is initially uploaded by data owner which in turn will get uploaded to middle ware server which is nothing but the Virtual server present in between the cloud and the company. Whenever company uploads the data it will initially get loaded onto the virtual server and from there when client feels the data is perfect then finally migrates it to cloud. Data encryption is required during the process of migration from virtual server to cloud. Cloud is a common place where data belonging to all clients will be stored. As the storage area is common we are employing the encryption scheme to safeguard the data.

During the download time, the reverse process needs to be employed with which the client or data user can take the data from the cloud. All the clients belonging to the company will be given the key well before hand through their own convenient manner.

2.3 Decryption Process to Fetch the Data

1. Initially the user needs to enter the key shared by the data owners.
2. Once the key matches with the specified file, the decryption technique will load the data.
3. Data loaded will be broken into pieces based upon the special character that was taken during the encryption time
4. Each data unit will be then be divided by the mathematical number
5. Once a number is divided and collected it will then be converted back to its corresponding ASCII value and data will be gathered.

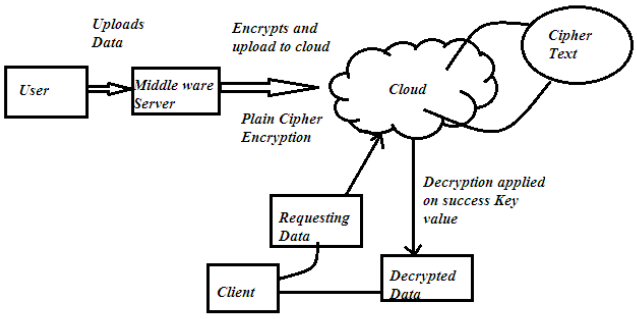

Fig 2: Flow of the Application

III. CONCLUSIONS

As the cloud computing is fastest growing technology in IT world today, the most important thing to be taken into consideration is the security. To overcome this problem with the many existing encryption techniques we employed a new algorithm that is minimizing the security threat and thereby increasing the efficiency of the application and thus enabling many companies to depend on the cloud architecture for storing and migration of their company data from and within cloud. Thus overall paper gives an idea about the cloud importance, its current stand in the market and the way to secure data present in the cloud.

Our future work on this would be to have dynamic support to the clients where they can have an audit check on the cloud with the help of liner programming and public auditability to cross verify whether the data is as it has to be or is it tried to be modified.

REFERENCES

[1]. S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2]. J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3]. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4]. M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[5]. R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[6]. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7]. M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-hive/macros/latex/contrib/supported/IEEEtran/

[8]. FLEXChip Signal Processor (MC68175/D), Motorola, 1996.

[9]. "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[10]. A.Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

AUTHOR DETAILS

	**J V Krishna** working as a Associate Professor & HOD, Department of Computer Science & Engineering at SreeVahini Institute of Science & Technology, Tiruvuru, Krishna Affiliated to JNTUK, A.P, India.
	**Dr. .ApparaoNaidu,** Professor, CSE Dept, J.B.Institute of Engineering & Technology(Autonomus) Moinabad, Hyderabad, T.S., India.
	**Dr.NirajUpadhayaya,** Principal &Professor,CSE Dept, J.B.Institute of Engineering & Technology(Autonomus) Moinabad, Hyderabad, T.S., India.