ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on effective method for Detecting Leakage of Data in Cloud Computing Environment

Poonam R. Panchwatkar[1], Mukta Khirwadkar[2]

M. Tech Student, Dept. of CSE., G.H. Raisoni College of Engineering, Nagpur, India[1]

Assistant Professor, Dept. of CSE., G.H. Raisoni College of Engineering, Nagpur, India[2]

ABSTRACT: Now a days the internet plays a vital role in human daily life , similarly now in organizations also internet technologies plays very important role. It's like there is no work can complete without internet technologies. As we know our India is converting into a Digital India. Similarly now file sharing on cloud environment is important. As we all know Cloud is nothing but the huge space where we can store anything or any type of data. Because of internet use and sharing data on cloud the time gets more utilized. The organization increases their efficiency, takes less time for transferring the data from one place to another place. Though this concept is very efficient and useful there are some other hostile actions too. While transferring the data, the data may gets damage by the person who is misdeed. This concept is known as leakage of data In the work, we aspire a technique for providing more security to our issue data leakage. Here our priority is to provide more security to data and figure out the person who is misdeed, who has leaked the data. Finding the misdeed is big challenge for us.

KEYWORDS: Cloud computing, encryption algorithm and decryption algorithm, Allocation strategies, Data distribution.

I. INTRODUCTION

In the recent structure of business, data leakage is large problem as essential organizational data should secure from unconstitutional access. It is occur by chance the secret organizational data which is distribution to the unconstitutional entities . It is not necessary that unconstitutional means it is planned. The unplanned data leakage is also the part of unconstitutional. The principal is to secure the essential data from getting misused by unconstitutional use. Essential data means the copy right details, functional details etc.

In more organizations, the essential organizational data has been shared to one or more than one stakeholder which are not from the same organizational site. Because of this it is tough to find out a person who is responsible for the misdeed, who emanate the data. My aim is to find out the evil and when the data will be leaked by the evil. To implement the project here I will be used some symmetric, asymmetric cryptographic algorithms to provide the security. The cryptography concept includes plain text, cipher text, encryption, decryption and key generation. These terms are discussed in below :

- Plain Text – Plain text is the text which is written by the sender to the receiver. The normal text and a readable text is a plain text.
- Cipher Text – It is the text which is not readable to anyone else other than the receiver.
- Encryption – The conversion of plain text into the cipher text by using the public key or private key is known as encryption.
- Decryption – Conversion of cipher text into the plain text, readable text by using the key is known as decryption.
- Key – Key is the secret text which is formed by the alpha numeric text, numeric text or by special symbols.

In the structure of business sometimes the data have to share with the third party for some purpose like for any enhancement or for some another operations. The third party may be from same organization or from different

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

organization. Now a days sharing of data is became a problem where the people are afraid of data leakage. To avoid the data leakage and finding out the evil I will used the watermarking technique. Watermarking technique is used to provide the authentication. This method used for images and more secure for transferring the data.

In the business structure after sharing of the data with the another party, merchant who share the data finds the same data in unconstitutional region. If this type of situation occurs then the probability to judge that from where the data is leaked. For example, one child of age 6 years steal the chocolates from chocolate box but in his/her hand I saw only 1 chocolate is remaining so he/she can denied, but I caught him/her with many chocolates then he/she will not be able to denied. Similarly, if I will find the person with maximum clues then its enough to say that person is guilty.

II. RELATED WORK

The system which are in exist they had some drawback. In the previous system only comparison is done to find out the misdeed. These system uses the water marking technique for figure out the data leakage. Here in proposed model will find which type of data is going to be leaked and who is responsible for the leakage, the place or location from where the data is leaked. [1] neerajkumar, et al. In this paper they have done the comparison of cryptographic algorithms rsa,aes and des based on encryption time and decryption time. In this they uses the bell-lapadula for data confidentiality and biba-integrity model for protection of data integrity. Here, they introduced a technique which provides the more security towards the problem of data leakage. [2] rohit pol, et al. In this paper they introduces location strategies. They uses guilty model analysis to check the interaction match. Here they only introduces the concept for finding the leakage. They gives the future scope to find out more location strategies and finding the guilty. [3] rupeshmishra, et al. In this, perturbation and watermarking technique is used. They had use some algorithms like distribution algorithm for data distribution logic, agent detection algorithm. They invents some data allocation strategies. Here they only shows that, there is a possibility to detect person who is responsible for a leak, according to overlapped data with the leaked data and the data of other stakeholders. [4]hitendragarg, et. Al. The proposed watermarking algorithm is found powerful opposition to the distortion attacks. The proposed model shows the result opposed to cropping attack which occurs because of repeated insertions of watermark information in different segments of 3-d mesh. [5] suneetaagrawal, et al. In this paper they proposed a non-blind, secure and tough watermarking algorithm. This algorithm is based on geometrical properties of 3d mesh object. [6] sranjithakumari, et. Al. In this paper they shows that encryption is main part in communication of data. In this they research on folloing encryption algorithms aes, des and rsa using lsb substitution technique which provides more security. [7] dr v palanisamy, et. Al. In this paper they proposed that the which encryption algorithm is better on the basis of different parameters such as key value, computational speed and tenability here they concluded, in symmetric algorithm aes algorithm is better and rsa algorithm better in the asymmetric encryption algorithms. [8] ethambiraja et al. In this paper a deep study has done of various encryption algorithms. They are many encryption algorithms had been introduced by many authors like symmetric encryption, asymmetric encryption. Symmetric encryption such as aes, des, 4rc, 6rc,etc. These encryption algorithm generates a key and each key is used for one round. Each key has its own functions. Each key is used in one round according to the algorithm to encrypt and decrypt the plain text of size 512-bits. The text is transfer with the help of x-or gate, and gate.

III. PROPOSED ALGORITHM

In the analysis phase I have read all the requirements of users. There are lots of things I found which I have to consider as a user. Here I analyse that there are many ways from where the data can be leaked by different types of unconstitutional person. From the analysis of requirements I decided to provide more security to data. Because of this there are less chances to leaked the data or damage the data. For providing the security I will use the AES or RSA algorithm which are good at symmetric and asymmetric encryption, decryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

IV. PROJECT PLAN

The project plan is as follows

- File access will be mapped with user or user id.
- User credential will be encrypted.
- File folder will be maintained on the server.
- The files in the file folder will saved with their logical name and the physical name will be different from the logical name.
- User will be able to view only accessible files by the logical name of file.
- The user uploaded files will be maintained separately first as a temporary files.
- Main file content will only update, if user is authorised.
- If the user is not authorised to update then request comes to admin, alert will generate and updated text will be stored separately.
- All file history will be saved in tables.
- The terminal details will capture for each transaction.
- Here I am maintaining the files on cloud to access files, user has to identify himself/herself then only he/she will be able to view files with logical name.
- User id, file id and date will be saved in the form of image in the background after that only file will get download.

V. SIMULATION RESULTS

The Fig.1.shows the architecture of system that how system will work,where the files will get submitted when constitutional and unconstitutional user upload the files. Which user is authorized and who is misdeed where it will get shown. All these is explained in this fig. The Fig.2.explain as a flowchart for working of system. Admin login, User login, file uploading this structure shows.

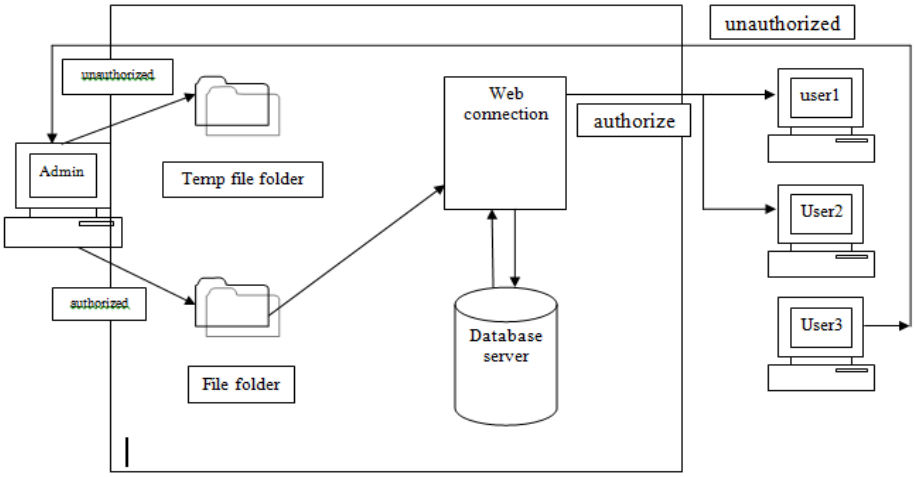

Fig.1.System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

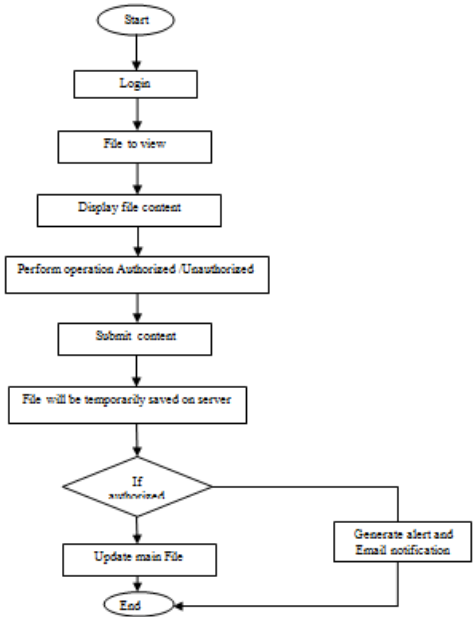

Fig. 2. Flowchart of System

VI. CONCLUSION AND FUTURE WORK

This technique will gives the security to data leakage into the system and also use of select cloud service. The technique will find out the data leakage in the cloud computing environment. The use of encryption and decryption algorithm will provide the more security data. By applying some algorithms we try to detect the culprit who leaks the data. This technique has made system more efficient and secured for the use into the organizations of data leakage.Which will be able to figure out the culprit or a person who is the misdeed. The system will also be able to provide the security to essential data of organization. The future work may consist of increasing the detection level for finding the misdeed by providing other techniques.

REFERENCES

1. Neeraj Kumar, Vijay Katta, Himanshu Mishra and HitendraGarg.Detection of data leakage in cloud computing environment. 2014 Sixth International Conference on Computational Intelligence and Communication Networks.
2. Rohit Pol, Vishwajeet Thakur, RuturajBhise, and A Kat. Data leakage detection. *International Journal of Engineering Research &Application*, 2(3):404–410, 2012.
3. Rupesh Mishra and DK Chitre. Data leakage and detection of guilty agent. *International Journal of Scientific & Engineering Research*, 3(6),2012
4. HitendraGarg and SuneetaAgrawal. Uniform repeated insertion of redundant watermark in 3d object. In *Signal Processing and IntegratedNetworks (SPIN), 2014 International Conference on*, pages 184–189.IEEE, 2014.
5. Hitendra GARG and Suneeta AGARWAL. A secure image based watermarking for 3d polygon mesh. *SCIENCE AND TECHNOLOGY*, 16(4):287–303, 2013.
6. B Padmavathi and S RanjithaKumari. A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution technique. *International Journal of Science and Research*, 2(4), 2013.
7. AL Jeeva, Dr V Palanisamy, and K Kanagaram. Comparative analysis of performance efficiency and security measures of some encryption algorithms. *International Journal of Engineering Research and Applications(IJERA) ISSN*, pages 2248–9622, 2012.
8.] EThambiraja, G Ramesh, and Dr R Umarani. A survey on various most common encryption techniques. *International journal of advanced research in computer science and software engineering*, 2(7):226–233, 2012.
9. M´aireMcLoone and John V McCanny. Efficient single chip implementation of sha-384 and sha-512. In *Field-Programmable Technology,2002.(FPT). Proceedings. 2002 IEEE International Conference on*, pages 311–314. IEEE, 2002
10. David Elliott Bell. Looking back at the bell-la padula model. In *ACSAC*, volume 5, pages 337–351, 2005.
11. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Performance comparison of the aes submissions, 1999.
12. HamdanAlanazi, BB Zaidan, AA Zaidan, Hamid A Jalab, M Shabbir, Yahya Al-Nabhani, et al. New comparative study between des, 3des and aes within nine factors. *arXiv preprint arXiv:1003.4085*, 2010.
13. Aman Kumar, SudeshJakhar, and Sunil Makkar. Distinction between secret key and public key cryptography with existing glitches. *IndianJournal of Education and Information Management*, 1(9):392–395, 2012..
14. D Elliott Bell and Leonard J La Padula. Secure computer system: Unified exposition and multics interpretation. Technical report, DTIC Document, 1976.