SECURE DATA SHARING AND REMOTE ACCESSING OF FILES IN CLOUD

[1]Pooja Awasare, [2]Priya Bansode, [3]Pankaj Dandge ,[4]Aishwarya Kudale,[5]Seema Shabadi
[1]Student,
[1]Computer Engineering RSCOE,
[1]Savitribai Phule Pune University, Pune, India

Abstract—* *Cloud is being used by much type of users to fulfill their storage needs and sharing requirements. Cloud is one of the emerging techniques in today's era. As there are many cloud service providers in industry it is extremely easy to avail cloud storage. But while doing so users compromise security and privacy of data willingly or unwillingly as these cloud storage services are not very proficient when it comes to data security. We are proposing a system that can overcome these issues. Our system introduces encryption for security of data. As data is stored in encrypted form it will be hard for cloud storage owners also to decrypt the data. By doing so some other problem arrives like searching becomes impossible. For that we are maintaining a keyword database that will be used when user search for a file. User can see graph that will show categories of documents uploaded on cloud. Storage uses on cloud will be traced. There is another unique feature of our system. If user enters # with correct password, system will prevent user from accessing any files and SMS will be sent to emergency contacts of user.

Index Terms—* *Cloud Storage: Access Control, Authentication, Unauthorized Access (e.g. Hacking), Database Processing, Privacy,Security.

I. INTRODUCTION

Cloud as an emerging technique in today's era is being used by many types of users to fulfill their storage needs along with sharing requirements. Now days, it is extremely easy to avail cloud storage, due to abundant availability of cloud service providers. But on the other hand, these cloud storage services are not very proficient when it comes to data security and the users have to compromise security and privacy of data. . We are proposing a system that can overcome these issues. Firstly our system introduces encryption for security of data .It will be hard for cloud storage owners also to decrypt the data, as data is stored in encrypted form. Due to such things, some other problem arrives like searching becomes impossible. For that we are maintaining a keyword database that will be used when user search for a file. User can see graph that will show categories of documents uploaded on cloud. Storage uses on cloud will be traced. There is another unique feature of our system. If user enters # with correct password, system will prevent user from accessing any files and SMS will be sent to emergency contacts of user.

II. RELATED WORK

Protecting user's data is an essential task in current systems. Researchers are proposing approaches and solutions to maximize the confidentiality of users data. Study of different types of algorithm like AES, RSA, Blowfish and distinguishing between them to recognize which algorithm is best suitable for our system.

LITERATURE SURVEY

1. Enhancing Cloud Computing Security using AES Algorithm

Abha Sachdev
Assistant Professor Department of Computer Science & Engineering ASET, Amity University, Noida, India
Mohit Bhansali
Student Department of Computer Science & Engineering ASET, Amity University, Noida, India
International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April

The above proposed system is a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security. These parameters provided us a better assessment of AES for increasing security.

2. A hybrid security approach based on AES and RSA for cloud data

Bhupendra Kumar1, Jayshree Boaddh2 and Lata Mahawar2
Student, Department of Computer Science, MIT, RGPV, Bhopal1
Assistant Professor, Department of Computer Science, MIT, RGPV, Bhopal2
International Journal of Advanced Technology and Engineering Exploration, Vol 3(17) ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2016.317005

In this paper they have proposed an efficient and secure cloud computing framework which support security for the cloud users and data control is being provided at the cloud user side. The cloud user can use the privilege of inter cloud communication with the data security of AES and RSA security hybridization which will provide four key security. The encryption is provided by the server. Then the receiver cloud can view the request file by applying the four keys. If any malicious behaviour is identified before the cloud user read operation then our document identification bit alert the client and server for the possible attack. So this framework supports secure data inter communication with malicious identification also. In this paper we have designed a secure user cloud framework with the help of AES and RSA algorithms. Our approach provides an authenticated way of entering the cloud user and provides inter clod communication virtualization environment. For data security in inter cloud communication AES and RSA capability are used as the four key security. The key control with the user side protection is the main benefit of our dissertation. Then we have provided the data identification bit control for controlling any malicious behaviour detection.

3. Enhancing Cloud Data Security Using Elliptical Curve Cryptography

Ms. Nikita N Chintawar1, Ms. Sonali J Gajare2, Ms. Shruti V Fatak3, Ms. Sayali S Shinde4, Prof. Gauri Virkar5 Bachelor of Engineering, Information Technology, BSIOTR, Pune, India 1, 2, 3, 4 Professor, Computer Science and Engineering, BSIOTR, Pune, India5

International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016

Elliptic Curve Cryptography provides better security and more efficient performance than the first generation public key cryptography techniques like RSA which is now in use. Although ECC's security has not been completely evaluated, it is expected to come into universal use in different fields in the future. After comparing the RSA and ECC ciphers, the ECC has manifest to complex much less overheads compared to RSA. The ECC has many advantages due to its ability to provide the same level of security using less key size .The future of ECC looks brighter than other algorithms as today's applications

4. Study of Security Requirements in Cloud Computing Environment

Naziya Khan1, Mrs. Asha Khilrani2 M.Tech. Scholar, Department of Computer Science & Engineering, T.I.T. & Science, Bhopal, India 1 Assistant Professor, Department of Computer Science & Engineering, T.I.T. & Science, Bhopal, India

International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, June 2016

As on now cloud is changing the way a user works over the network. It continuously reduces the load on users in terms of cost and complexity. It also lets the organization feel safe about their data against security breaches and fault interruptions. It provides a robust way of serving user through a service based model. In a way to achieve its goal, the changed computing also demands some of modified operation of security control for more protection. In this paper a study of cloud security environment and requirement of cloud security has been explored and address with problem observations.

5. Data Security in Cloud Computing using Encryption and Steganography

Karun Handa, Uma Singh
PG Student, Department of Computer Science & Engineering, Delhi Institute of Technology and Management, Gannaur, India
Asst Professor, Department of Computer Science & Engineering, Delhi Institute of Technology and Management, Gannaur, India
Email: k7handa@yahoo.in
IJCSMC, Vol. 4, Issue. 5, May 2015, pg.786 – 791

It is indeed that cloud computing can prove to be a boon in today's work environment hence this paper deals with data security issues related to cloud computing so that data centres can provide a good environment to keep data. The above mentioned scheme revolves around the problem of data security and with the help of encryption at client side and steganography at server side provides a highly secure model that will not only solve the issue of data safety but also simple in its implementation and hence usage. As per now the above mentioned scheme has been implemented using java. In future, the technique of image compression would be added to improve storage.

6. An Efficient data storage security algorithm using RSA Algorithm

Amandeep Kaur1, Sarpreet Singh2
1Research fellow, Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh
Sahib, Punjab, INDIA
2Assistant Professor, Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh
Sahib, Punjab, INDIA
International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Volume 2, Issue 3, March 2013

This paper presents the implementation of RSA through an encryption and decryption procedures, which are readily available for commercial use. Experiments were conducted on different text sizes. The results obtained in encryption and decryptions of RSA were given in seconds

7. Data Security in Cloud Computing Using Various Encryption Techniques

Shikha Rani Department of IT Chandigarh group of Colleges Mohali, India
pahujashikha@ymail.com
Shanky Rani Department of IT Chandigarh group of Colleges Mohali, India
cecm.infotech.shanky@gmail.com

International Journal of Modern Computer Science (IJMCS) ISSN: 2320-7868 (Online) Volume 4, Issue 3, June, 2016

In this paper proposed scheme is used to provide for en-hancing security on the cloud server. For this we use Blow-fish and MD5 as a hybrid security mechanism. Encryption and decryption is done by Blowfish and MD5 is used for data digestion form which enhances the security .From this we learned the blowfish approach for data security.

8. SECURE CLOUD ENVIRONMENT USING RSA ALGORITHM

P.suresh
Research Scholar,
Department of computer science,H.H The Rajahs college (Autonomous)India
International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072 © 2016, IRJET | Impact Factor value: 4.45 | ISO 9001:2008 Certified Journal |

In this proposed system the performance characteristics of rsa are observed by implement the algorithm for computation. in this paper, RSA was implemented through an asymmetric key algorithm ,encryption and decryption procedure over different key size.

9. A Review Paper on a Hybrid Model of Steganography and Blowfish to Ensure Data Security in Cloud Environment

Amanpreet Kaur*, Er.Khushdeep Kaur Department of CSE, I.K Gujral PTU, Punjab, India
Volume 6, Issue 7, July 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering

In this paper, we have proposed a new security algorithm with efficient use of AES algorithm , steganography and blowfish algorithm.We will be implementing the above proposed work in cloud sim simulation tool.

III. OUR APPROACH

Main objective of the system is to provide easy searching of document on cloud, because when users upload some document on cloud some time it is difficult to find out itself by user. So system provides keyword database functionality for searching particular file. System generates graphical format of uploaded documents which shows type of documents. There is functionality, if anybody force user to login to the system, and if user type # after correct password then system will block and SMS will send to registered contact numbers. User is able to Search file, Upload file, Download file using this system with security and easy search method.

IV. PERFORMANCE

Now days carrying physical document any time and everywhere is difficult to handle so, to minimize use of a physical document and to ensure the authenticity of our document.so this system is implemented.in which user can digitally upload documents on cloud with best features of security. The security features are: Dual Authentication, Password Security, Sharing Document, Traffic control.

V. CONCLUSION

In this paper, we proposed that system provides solution for achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud. Hence the data remain information-theoretically secure against the Cloud provider and other malicious users. In this technique searching of files is managed by the system it provides Graphical representation of file types and the secure sharing of data are provided.

REFERENCE

[1] E. Saleh and C. Meinel, "HPISecure: Towards Data Confidentiality in Cloud Applications," in Cluster,Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, 2013, pp. 605-609.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, et al., "A view of cloud computing," Communications of the ACM, vol. 53, pp. 50-58, 2010

[3] Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, pp. 355-370, 2014.

[4] A. Bessani, M. Correia, B. Quaresma, F. André, and P.Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds," ACM Transactions on Storage (TOS),vol. 9, p. 12, 2013.K. Elissa, “Title of paper if known,” unpublished.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34,pp. 1-11, 2011.

[6] L. Wei, H. Zhu, Z. Cao, W. Jia, and A. V. Vasilakos,"Seccloud: Bridging secure storage and computation in cloud," in Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on, 2010, pp. 52-61

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.