INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON PRIVACY PRESERVING AND SCALABLE DATA SHARING FOR P2P CRYPTOGRAPHIC STORAGE IN CLOUD

MS. SHWETA A. DHAWALE[1], DR. H. R. DESHMUKH[2], PROF. O. A. JAISINGHANI[3], PROF. S. V. KHEDKAR[3]

1. PG Scholar, Dept. of Computer Science and Engineering DRGITR, Amravati
2. HOD, Dept of CSE & IT, DRGITR Amravati
3. Asstt. Prof. Dept of Information Technology, DRGITR Amravati

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Cloud has gained popularity in the IT Services and infrastructure by speeding up the rate of outsourcing the services of the organization. Cloud computing as an emerging technology contains both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. Cloud Computing has gained popularity in both research and industrial communities. Cloud computing outsource their computational services to the users as well as the organizations, users can gain the services as well as the resources whenever they want and they can release the resource if they are no more needed. A P2P Cloud allows organizations or even individual to build a computing infrastructure out of existing resources, which can be easily allocated among different tasks. P2P cloud storage is usually a combination of cloud computing and peer-to-peer computing mechanism, where it can offer and provide huge computing, storage services and at the same time it lowers the economic cost of the real time users**.**

Keywords: Cloud, Cryptographic Storage

Corresponding Author: MS. SHWETA A. DHAWALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Shweta A. Dhawale, IJPRET, 2016; Volume 4 (9): 1269-1275

PAPER-QR CODE

INTRODUCTION

Cloud provides the method of storing the data the resources and data safely and remotely on the cloud. Cloud Computing is the emerging trend in delivering the services to the user and also to the IT organizations.

Cloud computing is the technology which allows user to access the services remotely outsourced by the cloud. The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. User choose the service from the list and take the resource to get their work done, once they have completed utilizing the resource they release their resource of the future use. Cloud Computing offers the end user with variety of services from hardware to the application with pay per use basis.

In P2P Storage cloud the most security mechanism used in data access privilege, where we determine which type of data can be accessed by the users. To achieve this we propose a technique of encryption which make use of public key cryptography technique and another mechanism used is the user revocation which is used to revoke the access permission of the user to retrieve the data in the P2P storage cloud.

I. LITREATURE REVIEW

Much related work was done in the field of cloud computing to achieve the desire result.

The following paper shows the related work in the field.

- **Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing**

The Paper was published by Shucheng Yu_, Cong Wang†, Kui Ren†, and Wenjing Lou_Dept. Of ECE, Worcester Polytechnic Institute,

Email: {yscheng, wjlou}@ece.wpi.edu.

The paper was based on the Cloud where the attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption was used to make the data secure. This paper shows the concept of encryption of data and key management where the keys are distributed under user privilege so that the data can be decrypted by the user using the assigned key.

- **Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing**

The paper was published by Rongxing Lu†, Xiaodong Lin‡, Xiaohui Liang†, and Xuemin (Sherman) Shen†

This paper uses the concept of again the encryption to make data secure from the unauthenticated or unauthorized user.

- **Cipher text-Policy Attribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization Brent Waters _University of Texas at Austin**

This paper makes the use of encryption technique called as Cipher text-Policy Attribute Encryption (CP- ABE) which is the interactive cryptographic assumptions in the standard model where the record of the patent is partitioned into a hierarchal structure and each part or portion is encrypted with its own matching key.

- **Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data**

This paper was published by Vipul Goyal Omkant Pandey*y* Amit Sahai*z* Brent Waters

In this Paper more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored

II. EXISTING SYSTEM

Since Cloud is used to store data on the cloud and Protection of the data on the cloud is a risk for cloud service provider as well as to the cloud user. Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to users. Once the user get the keys they can download he data without any interruption and also the data can be accessed by the unauthorized user as well.

In the existing system there was the issue of data being tampered or the key may get hacked. Any unauthorized user not being the part of the system can download any of the data without the permission of the data owner.

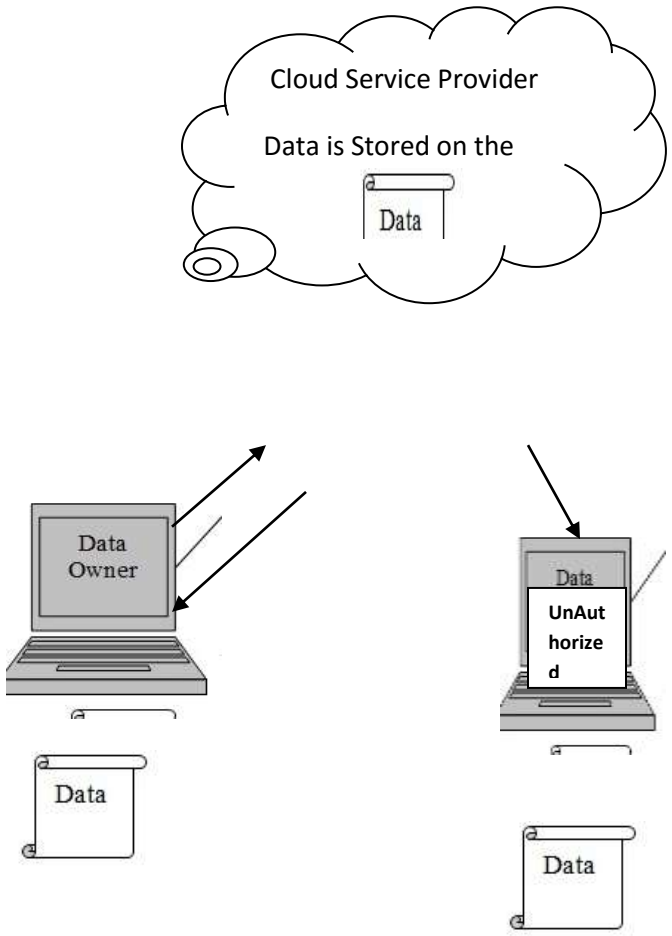

Fig: Overview of Data Stored on Cloud without any Security.

III. SECURITY

Because of the various security issues and threats to the data on the cloud, there is the need of data security. Data uploaded in the cloud can be tampered and modified. To help prevent the data loss or unauthorized access data uploaded on the cloud must be encrypted by the cryptographic algorithm these algorithms may be symmetric or asymmetric.

IV. PROPOSED SYSTEM

In order to overcome the drawbacks, we require a new secure architecture where data is secure .According to literature, lack of trust, efficiency, and scalability in user authentication and access processes are challenging issues in cloud-based environments. Therefore, an efficient and scalable authentication algorithm has been proposed and evaluated according to

defined parameters. The proposed model was designed by using two encryption algorithm concepts.

Firstly the data owner normally encrypt the original plaintext into ciphertext where it uses symmetric encryption using Secret Key The most important factor in dealing with this process is the attributes of the user. Once it successfully completed, another encryption, is applied again on the same data by the same data owner to enforce the security of the data. Now the original information is available in the P2P storage cloud.

If a user comes into existence for the data which resides in the P2P storage cloud, the decryption mechanism takes place where user attribution of the Authenticated user is checked. Once all the information which is needed to perform the decryption is successfully verified and guaranteed, the decryption takes place using the secret key of the user. The original data is retrieved by the user

V. Problem Analysis

Generally Data is Stored on the cloud to help share the data between the user remotely. The cloud is also used to backup the entire important document which will be needed in the future. Sharing or Storing data is one of the most significant function of the cloud whereas on the other hand storing the data also involves risk of data being tampered or sharing the data involves the risk that the data is being accessed by the unauthorized person to help prevent this risk issues we have designed the system in such a way that it does not involve any risk and the data owner will rely on the cloud before storing the data or after the storage.

VI. Conclusion and Future Scope

Security is a crucial aspect for providing a reliable environment and then the user authentication and access control enable the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. In this paper we have suggested a model with strong user authentication system where user have to introduce a confirm identity of his own and once the application confirms its identity then the user is allowed to use the services provided by the cloud. Most of the issues are observed in the cloud computing environment like authentication and network security which intensively affect the growth and popularity of using the cloud. Many issues which affect the single customer indirectly affect action of many other users that make the user experience bad about using the cloud computing environment. At the same time we have also tried to develop the system which will guarantees

high integrity and security to the cloud users by providing the encryption scheme which will help to maintain confidentiality of data.

Hence in future we will concentrate on the strategies to develop a new mechanism to help secure the data and also try to enhance the security level and also improve the resource sharing capacity of the cloud along with the reduction in the data tampering and data leakage. A secure cloud computing environment depends on several security solutions working harmoniously together. However, in our studies we did not identify any security solutions provider owning the facilities necessary to get high levels of security conformity for clouds. Thus, cloud providers need to harmonize security solutions from different places in order to achieve the desired security level.

VII. REFRENCES

1. S.IShaik Hussain, PG Scholar, V. Yuvaraj, Assistant Professor “A SECURE DATA ACCESS CONTROL METHOD USING AES FOR P2P STORAGE CLOUD”, IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICJJECS) 978-1-4799-6818-3/15/ ,2015

2. Faraz Fatemi Moghaddam Faculty of Computer Science and IT, Shiva Gerayeli Moghaddam Faculty of Computing, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi, Shirin Dabbaghi Varnosfaderani “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments”, 2014 IEEE Region 10 Symposium 978-1-4799-2027-3/14/$31.00 ©2014 IEEE

3. Nelson Gonzalez1*, Charles Miers1,4, Fernando Red´ıgolo1, Marcos Simpl´ıcio1, Tereza Carvalho, Mats N¨aslund2 and Makan Pourzandi “A quantitative analysis of current security concerns and solutions for cloud computing” Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, **1**:11

4. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL 25, NO. 2, FEBRUARY 2014.

5. Zhuge, T. Holz, C. Song, 1 Guo, X. Han, and W. Zou. Studying malicious web sites and the underground economy on the Chinese web. In Workshop on the Economics of Information Security, June 2008.

6. J. Bethencourt, A.Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,"inProc.2007 TEEESymp.SP, Taormina,Ttaly,pp. 32 1-334.

7. Camenisch, M. Dubovitskaya, andG.Neven, "Oblivious transfer with access control," in Proc.16th ACM ConfCCS, New York, NY, USA, 2009, pp.I31-140.
8. M. Kavitha Margret,"International journal of advanced research in computer engineering and technology", vol.2, 2013.
9. S. Al-Riyami and K. Paterson, "Certificate less public key cryptography, In Proc. ASTACRYPT2003, C. - S. Laih, Ed. Berlin,Germany: Springer,LNCS2894,pp.452-473.
10. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation,"inProc.5thASTACCS, New York, NY, USA, 2010, pp.261-270.
11. R. Gennaro, C. Hazay, and J. S. Sorensen. Text search protocols with simulation based security in 13th International Conference on Practice and Theory in Public Key Cryptography, pages 332-350, 201O.
12. Curtmola, R. , Garay, 1, Kamara, S. , Ostrovsky, R. : Enhancing Detinition and Efficient Constructions using Searchable Symmetric Encryption In: 13th ACM Conference on Computer and Communications Security, pp. 79-88 (2006)
13. Boneh, D., Lynn, B. , Shacham, H. : Generate Short signatures Using weil pairing. Tn: Boyd, C. (ed.) ASTACRYPT 2001. LNCS, vol. 2248, pp. 514-532. Springer, Heidelberg (2001).
14. Go1dreich, 0., Micali, S., Wigderson, A. : How to play any mental game. In: 19th ACM Symposium on Theory of Computing, pp. 218-229 (1987)
15. Yao, A. c. : Protocols for secure computations. Tn: 23rd IEEE Symposium on Foundations of Computer Science, pp. 160-164 (1982)
16. A.J. Choudhury, P. Kumar, M. Sain, L. Hyotaek, and H. Jae-Lee, “A Strong User Authentication Framework for Cloud Computing,”in *Proc. IEEE Asia-Pacific Services Computing Conference (APSCC)*, Jeju Island, South Korea, 2011, pp.110115.
17. C. Tien-Ho, Y. Hsiu-lien, and S. Wei-Kuan, “An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing,” in *Proc. 5th FTRA International Conference Multimedia and Ubiquitous Engineering (MUE)*,Loutraki, Greece, 2011, pp.155-159
18. L. B. Jivanadham, A.K.M.M Islam, Y. Katayama, S. Komaki, and S. Baharun, “Cloud Cognitive Authenticator (CCA): A Public Cloud Computing Authentication Mechanism,” in *Proc. International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, Bangladesh, 2013, pp. 1-6.