www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13917-13920

Confined Decentralize Cloud Storage Using Authentic Access Contol Scheme

Ms.C.Bindu [#1]***, Mrs.G.Nalini*** [*2]***,***

[#1] M.Phil., Scholar, Department of CS, College, Marudu Pandiyar College under Bharathidasan University.

[*2] Assistant Professor, Department of CS, College, Marudu Pandiyar College under Bharathidasan University.

[1] cspillai1961@gmail.com

[2] nalinigurumurthi@gmail.com

Abstract:- ***Cloud computing multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. This paper implements secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file.***

Keywords:-Decentralize,Attribute,revocation,cloud,outsource **:**

1.Introduction

Cloud computing has become the new buzz word driven largely by marketing and service offerings from big corporate players like Google, IBM and Amazon. Could computing is the next stage in evolution of the Internet. Computing provides the means through which everything from computing delivered to us as a service wherever and whenever we need.

"Could compute has the potential to create irreversible changes in how computers are used around the world". Could computing technology's objective is to move any application stored on a computer to a remote location, eliminating all the standard components, including operating systems and hard drives, which are necessary in today's computers and make them accessible online through a standard browser.

Cloud computing Security, or more simply, could security is an evolving sub-domain of computer security, network security and more broadly, information Security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Even though cloud computing has more benefits. It also has some disadvantage or drawbacks namely High Speed Internet Required, constant Internet connection, limited features, Downtimes, Vulnerability to attack, costs, limited control, Vendor lock – in, connecting peripherals, N/w connections Dependency, No hard drive, Data Security and privacy.

Taking In account of Data Security and privacy we have problems such as Data Breaches, Data Loss, Insecure APIS, Denial of Services, Malicious Insiders, Abuse of cloud services, Insufficient Due Diligence, Shared Technology.

Although the cloud computing infrastructure is generally very secure, it is also a very tempting target for the criminal underground. All public clouds have been engineered with could compute security as one of the top concerns. Any such vulnerability reported or not, in our chosen cloud, might put our entire data at risk.

To eradicate the data security problems Research Process takes place all over the world. This work also focuses on data security using some algorithms. The algorithm has the main objective to increase user's data confidentiality, Integrity and Availability.

The security is maintained from the beginning and do not pave way to the intruders to breach in to the users data. At the first stage, the user has to select his/her on security questions which will be known only to the user.

The second stage involves with generation of the key which is not immediately shown to the accessing user until the user is identified as the loyal user. The keys generated to the user are pubalic key, Private Key, Access key, Renew key.

2.Related work

Cloud Computing, the long – held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their services or the human expense to operate it. The authors gives us the quick review of the obstacles to and opportunities for growth of cloud computing. The top 10 obstacles prescribed by the authors are: Availability of Service, Data Lock – In, Data Confidentiality and Auditability, Data Transfer Bottlenecks, Performance Unpredictability, Scalable Storage, Bugs in Large Distributed Systems, Scaling Quickly, Reputation Fate Sharing, and Software Licensing.[1]

The paper [2] proposes a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the server without knowing the user's identity before storing data. The scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud and addresses user revocation. Moreover, the authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, the paper [3] proposes a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

Paper [4] proposes a solution to the old open problem of constructing a fully Homomorphic scheme. This notion, originally called a privacy homomorphism, was introduced by Rivest, Adleman and Dertouzous shortly after the invention of RSA by Rivest, Shamir and Adleman. Basic RSA is a multiplicatively Homomorphic encryption scheme i.e. given RSA public key pk = (N,e) and ciphertexts $\{\psi_i \leftarrow \pi_i^e \bmod N\}$, one can efficiently compute $\Pi_i \psi_i = (\Pi_i \pi_i)^e \bmod N$, a ciphertext that encrypts the product of the origin plain text.

Attribute based Encryption with key – policy based Encryption scheme utilizes multi-authority attribute-based encryption to encrypt the PHR data[5], so that patients can allow access not only by personal users, but also various users from different public domains with different professional roles, qualifications and affiliations. An important future work will be enhancing the MA-ABE scheme to support more expressive owner-defined access policies.

3.Existing System

The Existing works concern about the data security of the owner user while accessed by the loyal user, when an intruder tries to access the owner's data. The works concentrates over the encryption of the user's document while it is being accessed by the loyal user. The paper focuses only on securing the information which is stored by the user but not the retrieval of the user's file. The algorithm used in the existing system describes the stages in between the first stage and the last stage, which does not have the security over the intrusion of the third person. The goal of stopping the intruder from accessing the user's file is not acceptable and results in failure. To retrieve this, the work should concentrate on securing the file accessing controls. The user must have the satisfaction and confidence that their document is safe enough to be stored in the cloud.

4.Proposed System

Encrypting the document only does not save the user's document from the intruder. We have to improve the security while the intruder tries to access the owner user's document. In this project, we propose a novel approach of issuing level by level security process in which an unnecessary intruder is not allowed into the owner user's cloud. The key manager issues the key only at the last stage in order to ensure that the key is safe enough. We have four different cryptographic keys to protect data files stored on the cloud namely Public Key, Private Key, Access Key and Renew Key.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem there are lot of techniques introduced to make secure transaction and secure storage.

The encryption standards used for transmit the file securely. This assured deletion technique aims to provide cloud clients an option of reliably destroying their data backups upon requests. The encryption technique was implemented with set of key operations to maintain the secrecy. Recently, Susmita ruj [1] addressed Anonymous Authentication [1] for data storing to clouds. Anonymous Authentication is the process of validating the user without the details or attributes of the user. So the cloud server doesn't know the details or identity of the user, which provides to the users to hide their details from other users of that cloud. Security and Privacy protection in clouds are examined and experimented by many researchers. Wang et al. provides storage security using Reed – Solomon erasure – correcting codes. Using homomorphic encryption, [4] the cloud does not know what data it has operated on.

Time – based file assured deletion, which is first introduced in [5], means that files can be securely deleted and remain permanently inaccessible after a predefined duration. The main Idea is that a file is encrypted with a data key by the owner of the file, and this data key is further encrypted with a control key, by a separate key manager known as Ephemerizer[5]). The key manager is a server that is responsible for cryptographic key.

In [5], the control key is time – based, meaning that it will be compsletely removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared without the control key, the data key and hence the data file remain encrypted and are deemed to be inaccessible. Thus, the main security property of file assured deletion is that even if a cloud provider does not remove expired file copies from its storage, those file remain encrypted and unrecoverable. An open issue in the remain encrypted and recoverable. An open issue in the work is that is uncertain that whether time - based file assured deletion is feasible in practice, as there is no empirical evaluation.

Later, the idea of time – based file assured deletion is prototyped in vanish. Vanish a data key into multiple key shares, which are then stored in different nodes of a public peer – to – peer distributed hash table system. Nodes remove the key share that reside caches for a fixed time period, then the file owner needs to update the key shares in node caches – aging mechanisms in the p2p dht, it is difficult to generalize the idea from time based deletion to a fine – grained control of assured deletion with respect to different file access policies.

The paper proposes policy based file access [2] and policy based file assured deletion, for better access to the files and delete the files which are decided no more. The author proposes effective renewal policy for making better approach to renew the policy without downloading the data key and control keys, which is available now a day. Instead, we can add a renew key with each file and download that keys whenever the file needs to be renewed. First, the client was authenticated with the username and password, which is provided by the user. Then the user was asked to answer two security levels with his or her choice. Each security levels consist of 5 user selectable questions. The user may choose any one question from two security levels. The private key for encrypt the file was generated with the combination of username, password and the answers for the security level questions.

After generating the private key the client will request to the key manager for the public key. The key manager will verify the policy matches with the file name then same public key will be generated. With the public key and private key the file will be encrypted and uploaded into the cloud.

If a user wants to download the file he or she would be authenticated. If the authentication succeeded, the file will be downloaded to the user cant able to read the file contents. He or she should request the public key to the key manager. According to the authentication, the key manager will produce the public key to the user. Then the user may decrypt the file using the login credentials given by the user and the public key provided by the key manager. The client can revoke policy and renew the policy due to the necessity.

4.1 Algorithm

We used RSA algorithm for encryption/decryption. This algorithm is the proven mechanism for secure transaction. Here we are using the RSA algorithm with key size of 2048 bits. The keys are split up and stored in four different places. If a user wants to access the file he/she may need to provide the four set of data to produce the single private key to manage encryption/decryption.

4.1.1 File Upload/Download

The client makes request to the key manager for the public key, which will be generated according to the policy associated with the file. Then the client generates a private key by combining the username, password and security credentials. The authenticated client can get the public key. Then the client can decrypt the file with the public key and the private key.

4.1.2 Policy Revocation for File Assured Delation:

The policy of a file may be revoked under the request by the client, when expiring the time period of the contract or completely move the files from one cloud to another cloud environment. Automatic file revocation scheme is also introduced to revoke the file from the cloud when the file reaches the expiry and the client didn’t renew the files duration.

4.1.3 File Access Control:

To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files. To recover the file, the client must request the key manager to generate the public key. With file access control the file downloaded from the cloud will be in the format of read only or write only supported. Each user has associated with policies for each file.

4.1.4 Policy Renewal:

Policy renewal is a tedious process to handle the renewal of the policy of a file stored on the cloud. An additional key named renew key is implemented, which renews the policy of the file stored on the cloud. It can be done using 5 steps.

4.2 Experimental Analysis:

While experimenting the project the time performance, uploading performance and downloading performance are taken in account. The performance of this project was analyzed under various file sizes. The cryptographic operation time is evolved. It supports random time duration for any size of files to download. While uploading the time is not constant. Even for same size file the time taken for uploading differs randomly. The time delay is made eventually to confuse the hacker. It is achieved using different encryption standard. Because of this downloading performance is also not a constant one.

5. Conclusion

As a conclusion, we propose secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption or Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future.

DOI: 10.18535/ijecs/v4i8.53

The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new keys to the files stored in the cloud.

6.Future Scope

In Future the file access policy can be implemented with multi authority based attribute based encryption. Using the technique we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so that the hacker can confuse to identify the algorithm.

References

[1] Michael Arm burst, Armando Fox, Rean Griffith, Anthony D.Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia - "Above The Clouds: A Berkeley View Of Cloud Computing" – UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10,2009.

[2] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak - "Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds", IEEE Transactions on Parallel And Distributed Systems, 2013.

[3] Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou – "Towards Secure And Dependable Storage Sevices In Cloud Computing", IEEE Transactions on Cloud Computing, Aptil – June 2012.

[4] Craig Gentry – "A Fully Homomorphic Encryption Scheme", A Dissertation submitted to the department of Computer Science And the Committee On Graduate Studies Of Stanford University In Partial Fulfillment of the Requirements for the degree of Doctor Of Philosophy, September 2009.

[5] Ming Li, Shucheng Yu, Kui Ren, and Wenjing Lou, "Securing Personal Health Records In Cloud Computing: Patient – Centric and Fine – Grained Data Access Control in Multi – Owner Settings", LNICST 2010

[7] Sonia Jahid, Prateek Mittal and Nikita Borisov, "EASiER: Encryption – Based Access Control in Social Networks with Efficient Revocation", ASIACCS 2011

[8] Fangming Zhao, Takashi Nishide and Kouichi Sakurai, "Realizing Fine – Grained and Flexible Access Control to Outsourced Data with Attribute – Based Cryptosystems",ISPEC 2011.

[9] Weichao Wang, Zhiwei Li, Rodney Owens and Bharat Bhargava, "Secure and Efficient Access to Outsourced Data", CCSW 2009

[10] Melissa Chase, Sherman S.M.Chow, "Improving Privacy and Security in Multi – Authority Attribute – Based Encryption", CCS 2009

[11] Kan Yang, Xiaohua Jia, Kui Ren and Bo Zhang, "DAC – MACS: Effective Data Access Control for Multi – Authority Cloud Storage Systems", Dept of CS, City University of Hong Kong 2013

[12] Sushmita Ruj, Amiya Nayak, Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds", SEECS, University of Ottawa, Canada 2011.

[13] Radia Perlman, "File System Design with Assured Delete", NDSS 2007

Authors Detail:

Ms. **C.Bindu, Completed** her B.Sc (CS) in SASTRA UNIVERSITY and finished M.Sc (CS) in ALAGAPPA UNIVERSITY. She had also completed B.Ed (CS) in PRIST UNIVERSITY and now currently doing M.Phil (CS) in Marudu Pandiyar College under Bharathidasan University.

Mrs.**G.Nalini, M.Sc., M.Phil** is working as an Assistant professor in Marudu Pandiyar College under Bharathidasan University. She had participated in several work shops and international conferences and presented papers.