Data Security in Decentralized Cloud Computing

[1] C.Anuradha, [2] T.Shiva Sai Krishna, [3] V.Kowshik,

[1] Asst Professor, Department Of CSE, BIHER,

[2] [3] UG Student, Department Of CSE, BIHER,TN,INDIA

Abstract: The cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. we propose a secure data sharing scheme fordynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and private key is valid only once and cannot access the file again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user view in the group.

Keywords : Cloud computing, Security, Private keys, public keys, fine-grained access control.

I. INTRODUCTION

When you store your photos online instead of on your home computer, or use webmail or a social networking site, you are using a "cloud computing" service. If you are an organization, and you want to use, for example, an online invoicing service instead of updating the in-house one you have been using for many years, that online invoicing service is a "cloud computing" service. Cloud computing [1,2,3] refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. For that reason the Office of the Privacy Commissioner of Canada (OPC) [4,5,6] has prepared some responses to Frequently Asked Questions (FAQs). We have also developed a Fact Sheet that provides detailed information on cloud computing and the privacy challenges it presents.

CLOUD COMPUTING

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

CHARACTERISTICS

The characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks[7,8,9,10]. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

II. DEPLOYMENT OF CLOUD

SERVICES

Cloud services are typically made available via a private cloud, community cloud[11,12], public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider.

In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party.

In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

A hybrid cloud[13,14] is a combination of different methods of resource pooling (for example, combining public and community clouds).

Why cloud services are popular

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment[15,16,17], rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop.

Potential privacy risks

While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate.

LITERATURE SURVEY

Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic[18,19,20] primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an un trusted server to authorize file writes. We have built a prototype of Plutus on Open AFS.

This paper presents Sirius, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. Sirius assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Our implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations.

In **1998**, **Blaze, Bloomer, and Strauss (**BBS**)** proposed an application called atomic proxy encryption, in which a semi trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS encryption has been hindered by considerable security risks. Following recent work of Dodis[21,22] and Ivan, we present new re-encryption schemes that realize a stronger notion of security and demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread

and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by Providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice.

DISADVANTAGE

The frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack.

PROPOSED SYSTEM

We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

We propose a secure data sharing scheme which can be protected from collusion attack. Secure is needed to download the file from the group, when user revoked, the key is invalid and cannot used back again to view or download the file, even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.

Our scheme is able to support dynamic groups efficiently, when a user downloads the file from the group, the private keys of the other users do not need to be recomputed and updated.

ADVANTAGES

The users can securely obtain their private keys from group manager without any certificate authorities due to the verification for the public key of the user. It can be protected from collusion attack. When a user downloads the file from the group with the secret key, the secret key of the file key is invalid once, the key will recomputed and updated.

SYSTEM ARCHITECTURE

Design is a multi- step that focuses on data structure software architecture, procedural details, algorithm etc... and interface between modules. The design process also translate the requirements into presentation of software that can be accessed for quality before coding begins. Computer software design change continuously as new methods; better analysis and border understanding evolved. Software design is at relatively early stage in its revolution.

Therefore, software design methodology lacks the depth, flexibility and quantitative nature that are normally associated with more classical engineering disciplines. However techniques for software designs do exit, criteria for design qualities are available and design notation can be applied.

DESIGN STRUCTURE
INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form

for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.

IV. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

SYSTEM MODULES

1. Key Distribution
2. Access Control
3. Data Confidentiality

KEY DISTRIUTION

In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.Group members (users) are a set of registered users that will create their own group and store their own data into the cloud and share them with others.

In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

ACCESS CONTROL

First, group members are able to use the cloud resource for data storage and data sharing.

Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked from the file.

We propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager.

Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users from the file cannot access the cloud file again after they are revoked.

We can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud.

DATA CONFIDENTIALITY

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data.

To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue.

ALGORITHM SPECIFICATION
AES- Advanced Standard Encryption

In order to create such a cryptosystem, one must remember that anything done by encryption must be undone during decryption, using the same key since it is a conventional (symmetric key) system. Thus, the focus is on various invertible operations. One standard technique in using the key is to derive a string somehow from the key and use xor to combine it with the emerging

Key Sizes versus Rounds			
	Key Block Size (Nk words)	Plaintext Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Fig11.1 table

cipher text. Later the same xor reverses this. Otherwise there are ``mixing'' operations that move data around, and ``translation'' (or ``substitution'') operations that replace one piece of data with another. This last operation is usually carried out on small portions of cipher text using so-called ``S-boxes'', which define replacement strings. One set of mixing, replacements, and exclusive-or with a string derived from the key is called a round. Then there will typically be a number of rounds. The AES uses different numbers of rounds for the different key sizes according to the table below. The table uses a variable Nb for the plaintext block size, but it is always 4 words. Originally the AES was going to support different block sizes, but they settled on just one size. However, the AES people (at the NIST) recommend keeping this as a named constant in case a change is ever wanted.

Note:

In This Project we using AES-128 key size for re-encryption process

For the Mathematical Cryptograph Notations:

The input data block is broken into a 4x4 byte array (128-bit key). The initial subkey (derived from the cipher key via key schedule [8]) is XOR'd to the byte array by an AddRoundKey() operation (Nb = block size)

- For each encryption "round"/iteration to n-1 (128-bit, n=10; 192-bit, n=12; 256-bit, n=14):
- Each array byte is substituted using a SubBytes () S-box [7] operation
- A ShiftRows () cyclic shift operation is done on the last three rows of the byte array

V. CONCLUSION

Secure provenance is of paramount importance to the flourish of cloud computing, we formally defined the secure provenance and the corresponding security model in cloud computing. Then, we proposed a concrete secure provenance secure anti collusion scheme based on the bilinear pairings, and used the provable security technique to prove its security in the standard model. Due to its comprehensive security features, the proposed secure anti collusion scheme provides trusted evidences for data forensics in cloud computing and thus pushes the cloud computing for wide acceptance to the public and fine-grained data access control in cloud computing. One challenge in this context is to achieve fine grainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. Proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved.

REFERENCES

1. Kavitha, R. Shelgin, S.,, Sandeep, S. "A study on vulnerability detection of attacks in web security",2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No: 9-12

2. Kavitha, R., Priya, N., Anuradha, C., "Li-Fi science transmission of knowledge by way of light",2017, International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:285-290

3. Kavitha, R..,Priya, N., Anuradha, C., "A novel approach of hybrid cloud",2017, International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue, Page No:299-304

4. Kavitha, G., Kavitha, R., Koushik Subramaniam, Y. "Operating scheme and its shield in mobilephone by utilizing android",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No:129-133

5. Kavitha, R., Kavitha, G."Deconstructing evolutionary programming using ghat",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:213-216

6. Kavitha, R., Kavitha, G., Thakur, K.A. "Helmet mounted heads-up display a rider assistance smart helmet for everyone",2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:411-413

7. Priya, N., Pothumani, S., Kavitha, R,"Merging of e-commerce and e-market-a novel approach",2017,International Journal of Pure and Applied Mathematics,Volume 116,
9 Special Issue ,Page No:313-316

8. Priya, N., Anuradha, C., Kavitha, R" Analysis of various data mining clustering algorithms",2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue,Page No:279-281

9. Kavitha, S., Kavitha, R."DDOS attack and defenses",2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No: 57-61

10. Kavitha, R., Kavitha, G.,"Decoupling byzantine fault tolerance from multi-processors in I/O automata",2017,International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue,Page No:225-228

11. Kavitha, R., Kavitha, G."A development of IPV4 with skilty approach",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:219-222

12. Shelgin, S., Kavitha, R."A cram on bluejacking by OBEX (Object exchange)", Volume 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No:441-445

13. Shelgin, S., Kavitha, R., Sudha, K.L."Identifying credit card fraud using biometric fingerprint techniques",2017,International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue, Page No: 447-451

14.Kavitha, G., Kavitha, R., Jennifer, S."Effectual exploit of digital irrigate tecniques to afford cloud safety marking",2017,International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue,Page No:185-189

15. Kavitha, R., Kavitha, G., Ramya, B."Inpatient monitoring for healthcare data using wireless sensor network",2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:345-350

16. Kavitha, R. "A methodology for improving read-write technologies for dhts",2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page No:93-97

17. Priya, N., Pothumani, S., Kavitha, R."Analysis of data mining using social network", 2017,International Journal of Pure and Applied Mathematics,Volume 116, 9 Special Issue, Page No: 307-310

18. Shelgin, S., Kavitha, R."A study on web application security state",2017,International Journal of Pure and Applied Mathematics, Volume 116,9 Special Issue, Page No:75-78

19. Priya, N., Anuradha, C., Kavitha, R."Analysing storage and processing in enhanced cloud computing with hadoop ", 2017, International Journal of Pure and Applied Mathematics,Volume 116,9 Special Issue,Page No:293-296

20. Kavitha, G., Kavitha, R.,Indhu.G, "Big Data, Cloud, Web of Thing in Healthcare Monitoring Scheme", 2017, International Journal of Pure and Applied Mathematics, Volume 116,8 Special Issue, Page 177-182

21. Kavitha, R., Kavitha, G., "Fuzzy, probabilistic algorithms for online clustering algorithms",2017, International Journal of Pure and Applied Mathematics,Volume 116,10 Special Issue, Page No:207-211

22. Shelgin, S., Kavitha, R., Balasubhakar,"A comparitive study on 5g mobile wireless technology"2017,International Journal of Pure and Applied Mathematics, Volume 116, 9 Special Issue,Page No:81-85