*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

# DATA SECURITY IN DECENTRALIZED CLOUD COMPUTING

**C.Anuradha[1], R.Kavitha[2], T.Shiva sai Krishna[3],V.Kowshik[4]**

[1,2]Asst Professor, Department of CSE, Bharath University
[3,4]UG Student, Department of CSE, Bharath University,Chennai,TN,INDIA a

**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 datawhile 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.

**Key words:** Cloud computing, Security, Private keys, public keys, fine-grained access control

## 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 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**)** 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**.**

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

**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. 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.

**Deployment of cloud**

**Services**

Cloud services are typically made available via a private cloud, community cloud, 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 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, 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 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

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

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 and Ivan, we present new re-encryption schemes thatrealize 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 onthe 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.

**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 invalidand 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.

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

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 specification**

**Hardware specification**

System **:** Pentium IV 2**.**4 Ghz

Hard Disk **:** 40 GB

Floppy Drive **:** 1**.**44 Mb

Monitor **:** 15 VGA Colour

Mouse**:** Logitech

RAM**:** 512 Mb

**Software specification**

Operating system **:** Windows 10

Coding Language :JAVA/J2EE

IDE**:**Eclipse

Backend**:** SQLyog

**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**.**

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

**Design structure**

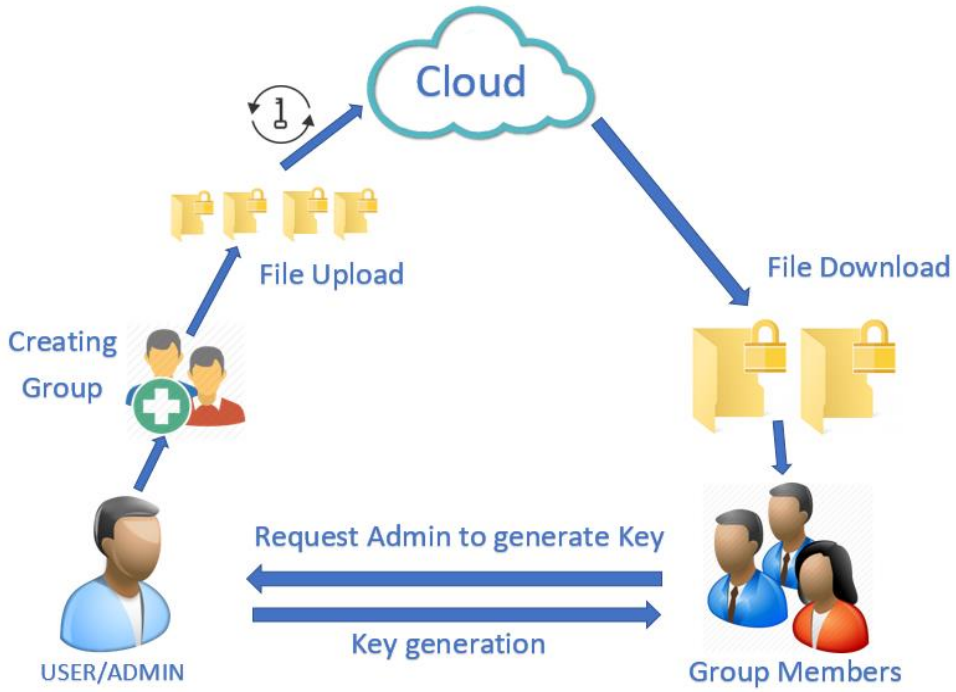
**Input design**

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**.**

**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

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

**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

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

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

**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 collusionscheme 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 collusionscheme 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. Boneh, D**.**, and Boyen, X**.** Short signatures without random oracles and

2. the sdh assumption in bilinear groups**.** Journal of Cryptology 21, 2 **(**2008**)**, 149–177**.**

3. Boyen, X**.**, and Waters, B**.** Full-domain subgroup hiding and constant-size group signatures**.** In Lecture Notes in Computer Science, PKC 2007 **(**2007**)**, pp**.** 1–15**.**

4. Chai, Z**.**, Cao, Z**.**, and Lu, R**.** Efficient password-based authentication and key exchange scheme preserving user privacy**.** In Lecture Notes in Computer Science, Wireless Algorithms, Systems, and Applications **(**2006**)**, vol**.** 4138, pp**.** 467–477**.**

5. Erdogmus, H**.** Cloud computing**:** Does nirvana hide behind the nebula? IEEE Software 11, 2 **(**March-April 2009**)**, 4–6**.**

*International Journal of Modern Agriculture, Volume 9, No. 4, 2020*
*ISSN: 2305-7246*

6. Foster, I., Zhao, Y., Raicu, I., and Lu, S. Cloud computing and grid computing 360-degree compared. In Proceedings of Grid Computing Environments Workshop, GCE'08 (Austin, TX, 2008), pp. 1–10.

7. Gellman, R. Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. Tech. rep., February 2009. http://www.worldprivacyforum.org.

8. Goldwasser, S., Micali, S., and Rivest, R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal of Computing 17, 2 (1988), 281–308.

9. Hartig, K. What is cloud computing? website, April 2009. http://kevinhartig.sys-con.com/.

10. Hasan, R., Sion, R., and Winslett, M.

11. Introducing secure provenance: problems and challenges. In Proceedings of ACM workshop onStorage security and survivabilit, StorageSS'07 (Alexandria, Virginia, USA, October 2007),pp. 13–18.

12. Kaufman, L. M. Data security in the world of cloud computing. IEEE Security & Privacy 7, 4 (July-Aug.2009), 61–64.

13. Liang, X., Cao, Z., Shao, J., and Lin, H. Short group signature without random oracles. In Lecture Notes in Computer Science, ICICS 2007 (2007), pp. 69–82.

14. Lin, X., Sun, X., Ho, P.-H., and Shen, X. GSIS: a secure and privacy-preserving protocol for vehicular communication. IEEE Transactions on Vehicular Technology 56, 6 (2007), 3442–3456.

15. Lu, R., Lin, X., and Shen, X. Spring: Asocial-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In The 29th IEEE International Conference on Computer Communications (INFOCOM 2010) (San Diego, California, USA, March 2010).

16. Lu, R., Lin, X., Zhu, H., Ho, P.-H., and Shen, X.ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In The 27th Conference on Computer Communications (INFOCOM 2008) (Phoenix, Arizona, USA, April 2008), pp. 1229–1237.

17. Lu, R., Lin, X., Zhu, H., and Shen, X. Spark: a new vanet-based smart parking scheme for large parking lots. In The 28th Conference on Computer Communications (INFOCOM 2009) (Rio de Janeiro, Brazil, April 2009).Lynch, C. A. When documents deceive: Trust and provenance as new factors for

18. information retrieval in a tangled web. Journal of the American Society for Information Sciene and Technology 52, 1 (2001), 12–17.

19. Mei, L., Chan, W., and Tse, T. A tale of clouds:Paradigm comparisons and some thoughts on research issues. In Proceedings of Asia-Pacific Services Computing Conference, APSCC'08 (Yilan, Dec.2008), pp. 464–469.

20. Shoup, V. Oaep reconsidered. Journal of Cryptology 15, 4 (2002), 223–249.