# A Novel Approach for Ensuring Data Confidentiality in Public Cloud Storage

S. Arul Oli
Research Scholar in Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, India.

L. Arockiam, Ph.D.
Associate Professor in Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, India.

## ABSTRACT
Cloud computing is one of the emerging forms of modern computing due to its many advantages. The security in the cloud data storage has become an important aspect of quality of service. As the number of users is on the tremendous increase, there arise many more issues since users look for the space to store sensitive data in the cloud. Along with variant advantages, the cloud storage has gained lot more advancement in both IT firms and Education fields since 2007. However, it also poses new challenges in creating secure and reliable data storage. Cloud delivers a facility for easy access over insecure or unreliable service providers. This paper addresses the security issues of storing sensitive data in a cloud storage service and this provides the need for the users to store the data in the trusted cloud providers. This proposes a cryptographic technique for cloud storage with encryption and decryption techniques. A novel approach is proposed for security in cloud storage. We also further look for the scheme which would check the integrity of their data and to optimize the mechanism efficiently and effectively.

## Keywords
Cloud Storage; Key Generation System; Security; Confidentiality

## 1. INTRODUCTION
"Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorised persons, processes, or devices." Cloud computing systems provide multiple Internet-based data storage and services. Due to its multiple benefits, which include cost effectiveness and high scalability and flexibility, cloud computing has gained significant achievements recently as a new paradigm for distributed computing for various applications. With the rapid growth of the Internet, service-oriented architecture (SOA) and virtualization technologies, cloud computing leads to the vision of Internet as a supercomputer. However, cloud computing has a major limitation to be broadly adopted due to the serious barrier that current cloud computing systems cannot protect the confidentiality of users' data from their service providers. A recent survey shows that most of cloud users fear that their data is being stolen and misused or tampered.

Data security is always an important aspect of quality of service and it is also a key issue in cloud computing. Due to traditional cryptographic primitives for the purpose of data security protection, it cannot be directly adopted to the environment of cloud. The data stored in cloud is facing different and neoteric challenges. Recently, the importance of ensuring the data security in cloud computing has been highlighted by researchers and enterprises. Cloud storage is built on the network computing environment. There are many benefits to move data into the cloud. For example, users need not care about the complexities of direct hardware management. But since users store their data in the cloud, it means that they will lose control of them and more and more concerns will arise about the data security.

The Security methods have got several advantages. First, it provides secrecy for encrypted data which are stored in public clouds. Second, it offers controlled data access and sharing among users, so that unauthorized users or untrusted providers cannot access or search over data without user's authorization.

Unfortunately, in addition to its advantages, cloud storage brings several security issues. Data confidentiality appears as the biggest concern for users of a cloud storage system. In fact, the clients' data are managed out of their governance. Kamara and Lauter [2], and Chow et al. [3] agreed that encrypting outsourced data by the user is a good alternative to mitigate such concerns of data confidentiality.

Thus, the user preserves the decrypting keys out of sight from the service provider, namely with the user himself. The confidentiality provisioning becomes more complex with flexible data available. It requires efficient sharing of decrypting keys between different authorized users. So that, only authorized users are able to obtain the clear text of data stored in the cloud. In this paper, we describe a new method for improving data confidentiality in cloud storage systems and enhancing dynamic sharing between users. It can be used by an authenticated user for his data storage. A representative solution for ensuring data safety in keeping the encrypted data in cloud storage with two-key encrypted system is introduced with a key generator system in the service provider to avoid any threats in cloud storage.

Our approach is to present a frame work to protect the confidentiality of user's data from service providers and to ensure that service providers cannot access or disclose user's confidential data being processed and stored in cloud computing systems. In this paper, an effective and novel scheme is proposed with key generation system through the service provider in the cloud environment. The generated key is sent to the user through the service provider. One more key is generated with the use of available encryption techniques. By making use of both the keys the data is encrypted. The encrypted data is sent to the service provider. We succeed in storing the encrypted data into the service provider which makes it trustful and secure cloud.

This paper provides the literature review in the chapter 2. The chapter 3 gives the concern for cloud store. Chapter 4 explains the Motivation. Chapter 5 deals with Methodology. The proposed frame work is explained in chapter 6. The paper is concluded in chapter 7 followed by the references.

## 2. LITERATURE REVIEW
Varun Maheshwari, et al [4] proposed a privacy-aware scheme which allowed a user to store data in a cloud. It was to perform database style query on the stored data without using

standard cryptography schemes while maintaining data confidentiality. They used data obfuscation techniques to achieve data confidentiality, and used glyph image to add noise and split the glyph image into small portions. They used another technique called Gaussian and speckle noise to convert the data into images and sent each part of the image to different independent clouds. The limitation here is that the cloud is neither aware of which part of the data it holds, nor knows how many other clouds hold the remaining data.

Krishna P.N. Puttaswamy, et al [5] proposed four methods to improve the data confidentiality at the time of data being stored on third party computing. The first method was to identify all functionally encryptable data for encryption. The sensitive data was to be encrypted without limiting the functionality of the cloud application. The second was to identify all functionally encryptable data in cloud applications. Third was to assign encryption keys for specification of data subsets. It was to minimize key management complexity at the time of ensuring robustness while compromising the key. The fourth method was to provide transparent of data access in order to prevent from malicious clouds at the user device.

Tribhuwan et al. [6] proposed a method to enhance the security of data stored in the cloud by utilizing the concept of homomorphic tokens and distributed verification of erasure coded data. This method attained both the integration of storage correctness insurance and data error locations. They introduced a new two way handshake scheme which is based on the token management method. This method does not work properly for maintaining the integrity and confidentiality of data.

Sato et al. [7] suggested one of the security concerns for cloud that could be summarized as social in security. It was classified into the multiple stakeholder problems, the open space security problem and the mission critical data handling problem. As a solution of these problems, they proposed a new cloud trust model. They considered both internal trusts model and contracted trust model that could control cloud service providers. They presented a model named as "Security Aware Cloud"

Seung-Hyun Seo, et al [8] proposed the mediated certificate-less public key encryption without using pairing operations. While pairing the sensitive data, there arise the key escrow problems. When not paired, the sensitive data are partially decrypted upon the successful authorization and the remaining data are decrypted by the user. This scheme improved the efficiency of encryption of the data which reduced the computational overhead by using pairing free approach. The advantages of this scheme are that the key Generation Center resides at public clouds. It solves escrow problem and revocation problem and assures confidentiality of data stored in public cloud.

Jeong-Min [9] highlighted the recent study model using Key Policy-Attribute Based Encryption (KP-ABE) and Proxy Re-Encryption (PRE). The above-mentioned both models violated the confidentiality of data through merging attack of revoked users in system. This paper proposed a model that would store and divide the data file into header and body. It delegated the decryption right by use of Type-based Proxy re-encryption. It divided data files stored on cloud servers as header and body and had the decryption rights as head (encrypted key using KP-ABE) and body (encrypted message using symmetric encryption).

Shuai Han [10] solved the problem of data storage security using the third party auditor scheme. This third party auditor was inside the cloud storage provider itself against scheme of the third party auditor with the user. This solved the threats of data being lost to certain level.

Abhishek et al [11] have described a trusted cloud storage architecture which applies the specification of the Trusted Computing Group (TCG). TCG is a global industry standard, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. The author had used TPM to encrypt data before storing it to the cloud. And they use Kerberos Authentication service to avoid masquerading, replay attack and eavesdropping. They proposed a module widely for the security of cloud storage. Kerberos is a secured method for authenticating requests for any service and is used to authenticate the end user to the trusted gateway.

Abhishek et al [11] have proposed fully homomorphic encryption schemes that can be used for multi-tier cloud architecture wherein the author, deploy two or more clouds for securing the data stored in an effective manner. They concentrated on the security issues related to cloud data storage and provided an efficient way to secure the same. This 2-tier architecture helped to achieve enhanced performance with less computing power that cloud offered.

Arockiam et al [12] have proposed encryption and obfuscation techniques that are used to protect data from unauthorized users in cloud storage. Encryption is the process of converting the readable form into unreadable form using an algorithm and key. Obfuscation is a process which illegal users do by implementing a particular mathematical function. Encryption and Obfuscation can be applied based on the type of data. Encryption can be applied to alphanumeric and alphabet type of data. Obfuscation can be applied to a numeric type of data. Based on these two techniques data would be more secure and protected from unauthorized access. The proposed techniques can be applied before data being sent to the cloud storage. They proposed three algorithms for securing the data. The first algorithm was used for finding out the type of data. Second algorithm was used for obfuscation which would find out the numeric data type. Third algorithm was used for encryption and it would find out the alphanumeric and numeric type of data. Confidentiality can be used in encryption and obfuscation for cloud storage. These two techniques are used to increase the confidentiality of data. The proposed technique is secure to protect the data in cloud storage.

Monikandan et al [13] have proposed a symmetric encryption algorithm to protect the data stored in cloud storage from the unauthorized access. The proposed technique was converting plain text into the corresponding ASCII code value of each alphabet and the key value ranges between 1 and 256. This technique improved classical encryption techniques by integrating substitution cipher and transposition cipher. Symmetric encryption has the speed and computational efficiently to handle encryption of large volumes of data in cloud storage. The proposed algorithm is used to encrypt the user data in cloud storage and it cannot be accessed by administrators or attackers.

Nesrine Kaaniche et al [14] proposed cryptography scheme for cloud storage, based on an original usage of ID-Based Cryptography. Their solution proposed the following advantages. The first was that the scheme provided secrecy for encrypted data which are stored on public servers. The second was that it offered controlled data access and sharing

among users. So unauthorized users cannot access or search over data without clients authorization. They proposed a technique which is called ID-Based Cryptography (IBC), where each user acts as a Public Key Generator (PKG).

From the above readings, we realize that there are many more techniques to secure the data in users' point of view. At the same time we also realize the number of possible threats which obstruct the security of the data. In order to secure the data, the cryptography techniques are used. The user realizes lot more threats in the cloud storage. So the user needs to be aware of threats before going into storing the data in cloud storage.

# 3. THE CONCERNS FOR CLOUD STORE

Though the cloud computing services have lot more advantages in data storage, the security problem makes users hesitate in trying on the cloud-based data storage services. Both the service providers and the users seek for adequate security in the cloud storage environment. A few requirements must be considered before start of the data the security process.

## 3.1 Data Encryption Storage

The biggest threat in cloud storage is the information leak as the data is in unknown Storage location. If the data is encrypted and stored in the clouds, the risk of data leakage is being reduced. There are two kinds of encryption algorithms. They are the symmetric encryption technology and the asymmetric encryption technology. The former deals with large amounts of data with more efficiency, but the keys must be frequently changed. The latter suits to a small amount of data encryption, but it can be used in many scenes. If the user wants to communicate with others, he just needs to know the public keys of others in advance. One can encrypt data using the public key of other user and only the owner of public key can decrypt the data.

## 3.2 Data Storage Wiping

- Cloud storage providers may share a storage device across multiple customers. For example, user stores the confidential data in the cloud and later the provider deletes that file.
- Another user may store the data but does not write any information on the cloud.
- The user examines the allocated space where the user may have to access to the previously deleted confidential file.
- To prevent this data access cloud based storage device overwrites files contents when a file is deleted.
- Wiping involves overwriting the previous file space with the service of values.

## 3.3 Storage Design

The storage design stage indicates such as redundancy, dynamic and isolation. Redundancy is the most basic measures to protect the data storage security. Dynamic is the user data which often changes leading to data consistency measurements. Isolation is to differentiate the data from its users, so that only the intended user can use their data. These storage designs must be carefully thought about.

## 3.4 Account or Service Hijacking

The service hijacking is explained as an account theft which can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and direct any transactions.

## 3.5 Data Integrity Protection and Prove of Integrity

The data integrity protection is to ensure that the data is correct before storing. And the proof of the data integrity is a service provided by provider, which allows the data users to check whether the data stored in the cloud is complete or not. Both requirements would reduce the business risk caused by data loss or damage.

## 3.6 Protection of Data Availability

Data might be stored in the different devices in cloud environment. If some device or node is a failure, then it could lead to data loss or unavailability. Therefore, the cloud service providers have to ensure the availability of quality.

# 4. MOTIVATION

From the above readings and concerns we realise the importance of security. Security is maintained with confidentiality measures. The confidentiality lies with either user or service provider. While storing the data into cloud, lot more threats and third party and malicious attacks occur in between. By considering all these threats, the user has to send the data to provider.

With one key encryption technique the security of the data would not be possible. It is not safe to encrypt the data either with user side or with provider's side. So the two-key system is proposed in this framework.

# 5. METHODOLOGY

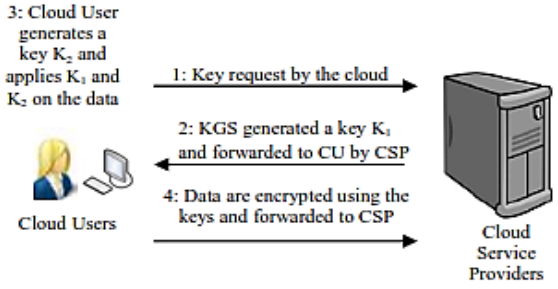


**Figure 1. Encryption Steps**

In this methodology, two-key system is utilized for the confidentiality and security. The key generator system controlled by the service provider generates a key and it is sent to the user through the provider. So, the user generates another key with the encryption techniques. By utilizing both the keys the data is encrypted by using encryption techniques and sent to the service provider for storage. This method serves our purpose of confidentiality. Supposing the data is encrypted with one key generated by key generation system, and then the data is at risk.

# 6. PROPOSED FRAMEWORK

The Figure 2 is the proposed frame work. It gives the detail of the flow of functions. The main frame has two sub parts namely; Cloud User and the cloud service provider. The cloud service provider has got the Key Generation System (KGS), storage system. The KGS is controlled by CSP. The cloud

user wants to be sure of his data being secured. So he needs to protect by encrypting the data.

With one key encryption the data may not be very confidential. So the cloud user requests the key from the CSP. The CSP requests the KGS to generate the key, where the KGS in turn automatically generates the key, K1, and sends back to the CSP. The CSP sends the key to user. Upon receiving key, the user maintains the table to keep track of the key and its source. Now the user generates another key, K2, with encryption techniques. With the use of K1 and K2, the user encrypts the original data. The encrypted data is sent.

The two-key system is used to protect the data from threats like external and internal. The internal threat is that the key generated by KGS could be misused by the provider himself. The external threat is that the single key encryption could be tampered by the third party. In order to safeguard from these threats the two-key system is used. The advantage of this proposed frame work is that with the known KGS the CSP cannot tamper or misuse the data of the user. The user maintains both the keys and the encrypted details in a table. Even if other user wants the data, he has to get the access from the primary user.

This framework also paves the way for another contribution of checking the integrity measures and the optimization of time. The provider also cannot think of misusing the stored data in storage, since he has to know another key K2. In this way the confidentiality of the data is maintained.

## 7. CONCLUSION

In this paper, we described the problem of data security in cloud data storage, which is essentially a paramount concern. In order to ensure the correctness of data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic two key systems. With the use of two key systems the data are encrypted and sent to the provider. The sent data is securely stored on the storage repository. The confidentiality of the data lies with the user since both the keys are protected by the user.By protecting the confidentiality of the data, the security of the data is envisaged. Thus gives the method more effective.

The data storage and its security in Cloud Computing demands lot more challenges to the users and the providers. So it becomes more important in the confidentiality of the data. The challenges to protect the data give lot more orientations and directions with innovative scopes for future research. We envision several possible directions for future research on this area.

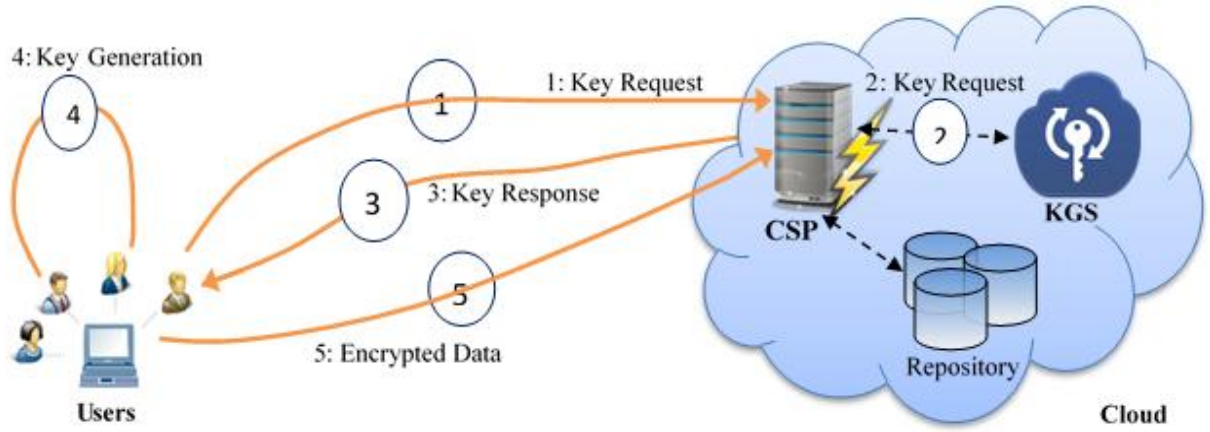


**Figure 2. Request Response for Storage**

## 8. REFERENCES

[1] DoD Trusted Computer System Evaluation Criteria, http: /csrc.nist.gov/publications/history/dod85.pdf

[2] Kamara and K. Lauter, “Cryptographic cloud storage,” in *Proceedings of the 14th international conference on Financial cryptography and data security*, ser. FC’10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 136–149.

[3] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control,” in Proceedingsof the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85–90.

[4] Varun Maheshwari, et al, “Character-based Search with Data Confidentiality in the Clouds”, IEEE, 2012.

[5] Krishna P.N. Puttaswamy, et al., “Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications”, SOCC, 2011.

[6] Tribhuwan, M. R., V. A. Bhuyar, and Shabana Pirzade. "Ensuring data storage security in cloud computing through two-way handshake based on token management." Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on. IEEE, 2010.

[7] Sato, Kanai Atsushi, and Tanimoto Shigeaki. "Building a security aware cloud by extending internal control to cloud." Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on. IEEE, 2011.Sato et al.

[8] Seung-Hyun Seo, et al., “An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”, IEEE, 2013.

[9] Jeong-Min do, “Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments”, IEEE, 2011.

[10] Shuai Han, “Ensuring Data Storage Security through a Novel Third Party Auditor Scheme in Cloud Computing”, IEEE, 2011.

[11] Abhishek, R. M. Tugnayat, and A. K. Tiwari. "Data Security Framework for Cloud Computing

Networks" International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, ISSN 0976– 6375 (Online), pp. 178-181.

[12] Arockiam, L., S. Monikandan, and P. D. Malarchelvi. "Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage." International Journal of Computer Applications 88 (2014).

[13] Monikandan, L. Arockiam, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm." International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) 2.8 (2013): 2278-1021.

[14] Nesrine Kaaniche, Aymen boudguiga, Maryline Laurent, "ID-Based Cryptography for Secure Cloud Data Storage, IEEE Sixth International Conference on Cloud Computing, 2013.

## 9. AUTHOR'S PROFILES

**S. Arul Oli** received his Masters in Computer Science from Bharathidasasn University, Tiruchirappalli, India. Currently, he is a Ph.D research scholar in the department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Cloud Computing. He has atteneded several national and international conferences and workshops.

**Dr. L. Arockiam** is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 26 years of experience in teaching and 19 years of experience in research. He has published more than 213 research articles in the International & National Conferences and Journals. He has also presented 3 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored 3 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010 & 2011 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in college" award for the year 2013 & 2014.