ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Multi Owner Data Access with a Novel Access Privilege Mechanism

Sudhakar D [1], Asha S [2]

Assistant Professor, Dept. of Computer Science, Bishop Appasamy Arts and Science College, Coimbatore, India[1]

M.Phil Scholar, Dept. of Computer Science, Bishop Appasamy Arts and Science College, Coimbatore, India[2]

ABSTRACT: Data storing and sharing is an imperative functionality in distributed networks. This proposes a secure and reliable multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. The proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners directly. The size and computation overhead of encryption are constant and independent with the number of revoked users. The proposed system authenticates the multi owner data content through device. This provides secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. The framework consists of two algorithms which are as follows. One for initial creation of public key-cryptography and another for aggregating, validating the key for decryption. The first algorithm enables the framework to generate an optimal and unique key that used to encrypt and authenticate the users on the file sharing. This uses an improved public key cryptography as the base, which is known as a public cryptographic algorithm. And the second algorithm allows remote communication for key verification with less overhead in key authentication. The proposed system ignores the rekeying overhead in the distributed multi owner data environment. This provides rigorous security analysis, and performs extensive simulations to demonstrate the efficiency of the scheme in terms of storage and computation overhead.

KEYWORDS: Multi Owner, Authentication, key, Aggregation, Cryptography algorithm

I INTRODUCTION

The term “cloud”, as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. “Cloud computing” was coined for what happens when applications and services are moved into the internet “cloud.” Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications.

1.1 DATA STORAGE IN CLOUD

Cloud Storage is a crucial service of cloud computing, that permits information house owners (owners) to maneuver data from their native computing systems to the cloud. More and additional house owners begin to store the information within the cloud. However, this new paradigm of information hosting service additionally introduces new security challenges. Data owners would worry that the information can be lost within the cloud.
This is because information loss might happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take. Sometimes, cloud service suppliers could be dishonest. They may discard the data that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

haven't been accessed or seldom accessed to save the cupboard space and claim that the information area unit still correctly hold on within the cloud. Therefore, house owners have to be compelled to be convinced that the information area unit properly holds on within the cloud. Traditionally, house owners will check the information integrity based mostly on two-party storage auditing protocols. In cloud storage system, however, it is inappropriate to let either facet of cloud service providers or house owners conduct such auditing, as a result of none of them can be sure to give unbiased auditing result. During this scenario, third-party auditing could be a natural choice for the storage auditing in cloud computing. A third-party auditor (auditor) that has experience and capabilities can do a additional economical work and persuade each cloud service suppliers and house owners. For the third-party auditing in cloud storage systems, there are units many necessary needs that are projected in some previous works.

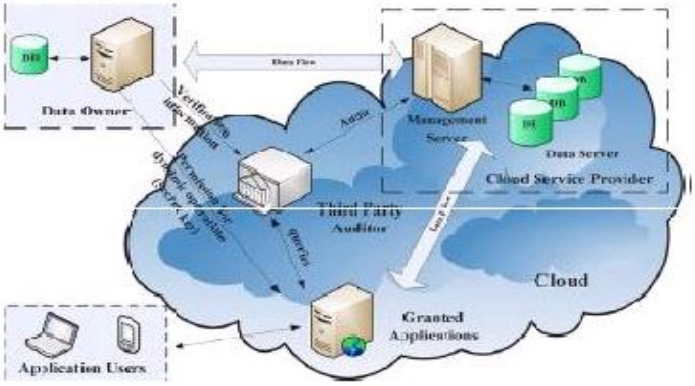

Fig 1: Data storage in cloud

The auditing protocol ought to have the subsequent properties:
1) Confidentiality: The auditing protocol ought to keep owner's information confidential against the auditor.
2) Dynamic auditing: The auditing protocol ought to support the dynamic updates of the data within the cloud.
3) Batch auditing: The auditing protocol ought to even be able to support the batch auditing for multiple house owners and multiple clouds.

II RELATED WORK

Security-mediator (SEM) model is proposed in [1] decouples the anonymous protection mechanism from the provable data possession mechanism via the use of security mediator. Our solution not only minimizes the computation and bandwidth requirement of this mediator, but also minimizes the trust placed on it in terms of data privacy and identity privacy. The efficiency of our system is also empirically demonstrated. [2] discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This study pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. The study [3] addresses the problem of building a secure cloud storage system which supports dynamic users and data provenance. Previous system is based on specific constructions and does not offer all of the aforementioned desirable properties. Most importantly, dynamic user is not supported. We study the various features offered by cryptographic anonymous authentication and encryption mechanisms; and instantiate our design with verifier-local revocable group signature and identity based broadcast encryption with constant size cipher texts and private keys. In the paper [4] The problem of key management in an access hierarchy has elicited much interest in the literature. The hierarchy is modeled as a set of partially ordered classes (represented as a directed graph), and a user who obtains access (i.e., a key) to a certain class can also obtain access to all descendant classes of her class through key derivation. Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. We present a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multi-prover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. [5] To improve security and save the fee, the cloud service providers will add some security countermeasures, such as offline backup. To restrict malicious and frequent access, PCS will require the clients to input the corresponding verification code. After that, the clients can perform the integrity checking protocol. This means that every client has to perform the integrity checking protocol by him. [6] Propose the concept of PPDP. Then, we give the PPDP system model and the formal PPDP security model. Taking use of the bilinear pairings and some difficult problems, we design an efficient PPDP protocol. In our PPDP design, we add the phase of Check Tag to resist the malicious clients. Our PPDP protocol is provable secure. Through security analysis and performance comparison, our PPDP protocol is shown secure and efficient. [7] In this paper, we proposed an efficient and inherently secure dynamic auditing protocol. It protects the data privacy against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, rather than using the mask technique. Thus, our multi-cloud batch auditing protocol does not require any additional organizer. This batch auditing protocol can also support the batch auditing for multiple owners. On the other hand, this method, they let the server compute the proof as an intermediate value of the verification, such that the auditor can directly use this intermediate value to verify the correctness of the proof. Therefore, our method can greatly reduce the computing loads of the auditor by moving it to the cloud server. [8] It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks [10] proposed an algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to assign these nodes ID numbers. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trusted central authority.

III PROPOSED SYSTEM

This introduces a new key aggregation scheme which is named as MAFS (Multi Authority File Security) technique, which collects the keys from all owners and creates an aggregated key for data decryption.
Unlike the previous works, the average size and time of rekeying messages have been avoided. So the communication overhead and time factors are considered here.
The proposal develops a three-step scheme for MAFS implementation.

- The first one is initial key generation for both single owner data and multi owner data group. The first algorithm can generate a key-tree that corresponds to the optimal key-tree obtained by mathematical analysis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

- The second step of the mechanism in MAFS, is an optimal key-tree maintenance and aggregation algorithm for multi owner data.
- The second scheme eliminates the existing re-key and key alteration processes.
- The third step of the scheme is the Device based authentication scheme, which helps to gather the encrypted keys from the device and aggregates together for decryption.
- Finally this performs the crypto process using the aggregated (sum up) key. This technique is named as Multi_Key Cryptography (M_KC). The Multi_Key is referred the proposed MAFS scheme which is mentioned above.

In M_KC, users encrypt a message not only under a public-key, but also under an adjunct of cipher text called class. That means the cipher-texts are further categorized into different classes.
The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key can have an aggregate key which is as compressed as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher-text classes.
The main objective of the Multi_Key cryptography is to review public-key cryptography and aims to demonstrate the confidentiality and sender-authentication. These above can be achieved simultaneously with public-key cryptography.
The proposed system utilizes the Public-key cryptography system, which is also known as *asymmetric-key* cryptography. In the proposed crypto scheme Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the aggregated key and the private key. With the proposed aggregated key cryptography, all parties interested in secure communications publish their private and aggregated keys. The proposed system follows different phased to implement the authentication.

1. **Setup Phase**

This is the first phase of all applications which contains the user registration, login. The user can register in the cloud by providing their desired user id, password. Based on the registration request the server performs the following process.

- **key generation**

Cloud Client can register with the user name and their own password. Security is enhanced to the user by providing secure secret key which is generated by the server known as cloud server. Key generation is based on Random Function
This module executed by the data owner to setup an account on an untrusted server.
KeyGen: executed by the data owner to randomly generate a public/master-secret key pair.
The system performs **key-Generation algorithm**.

2. **Multi owner data accessing phase**

This module helps to deal with the multi data owner details such as use rid, owner's details, unique mobile numbers and email id. The system will perform authentication based on the data owner id and key details.

3. **Client Process phase**

- **Upload data**

User **is** allowed to upload data in the cloud server by dynamic operation. The data which is to be upload is encrypted by the user using keys and then uploaded in the Cloud Server.

- **Encrypt data**

The proposed system uses an asymmetric key cryptographic algorithm which uses aggregated key for both encryption and decryption. User data is encrypted and then stored in the server. When user retrieves their data back encrypted data is decrypted and then data is provided by server.
The system performs **key-aggregate encryption scheme** for encryption and key aggregation.

- **Message phase**

The user enters user ID (id) and specifies the document which they need to download. The mobile program sends encrypted message to the owners when accessing the commonly shared data through telecommunication service provider (TSP)
The message phase begins when the user sends a request to the server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

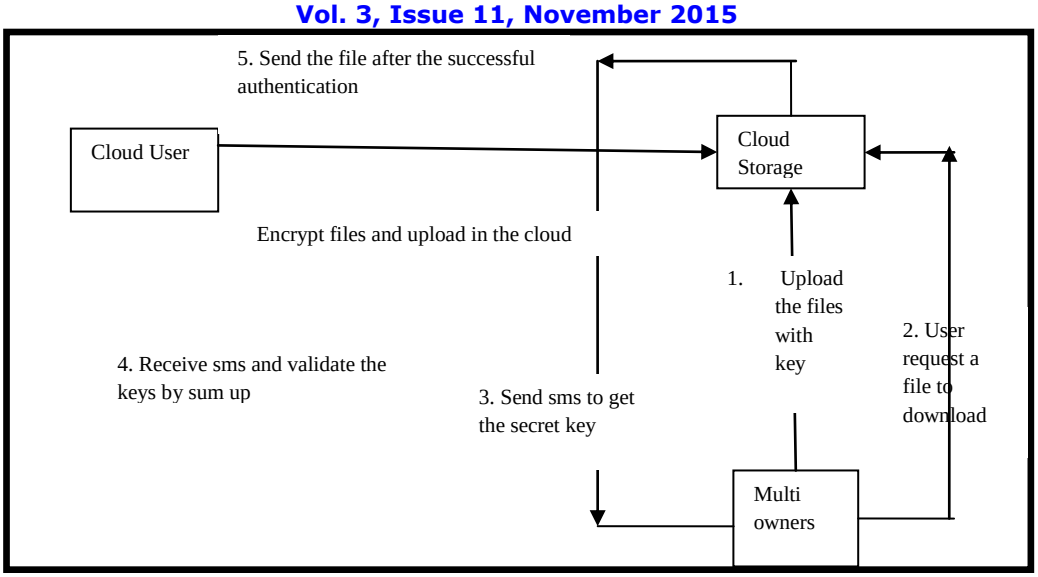

Fig 2: Flow Chart of the proposed system

4. **Server verification phase**

Server can decrypt and verify the authenticity of the registration SMS and then obtain with the shared key. Server also compares the source of received SMS.

Through a un trusted browser, The user uses her cell phone to produce a one-time password, e.g.,, and deliver necessary information encrypted with to server via an SMS message.

The system performs **key-verification scheme** for key aggregation and verification

The system performs **session based key verification method** for session validation

5. **Accessing service phase**

The accessing module provides the authentication to access the data. So the module receives the request form a user, and sends a password message to all its owner. The owners should forward the message along with their keys, which are provided already by the server. Here the session will be initiated; the user should send the message with in a particular time. After receiving the messages from all owners of the account, the system performs the transaction. Acknowledgement will be send to all owners after successful completion of transaction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

3.1 Multi_Key Encryption Process:

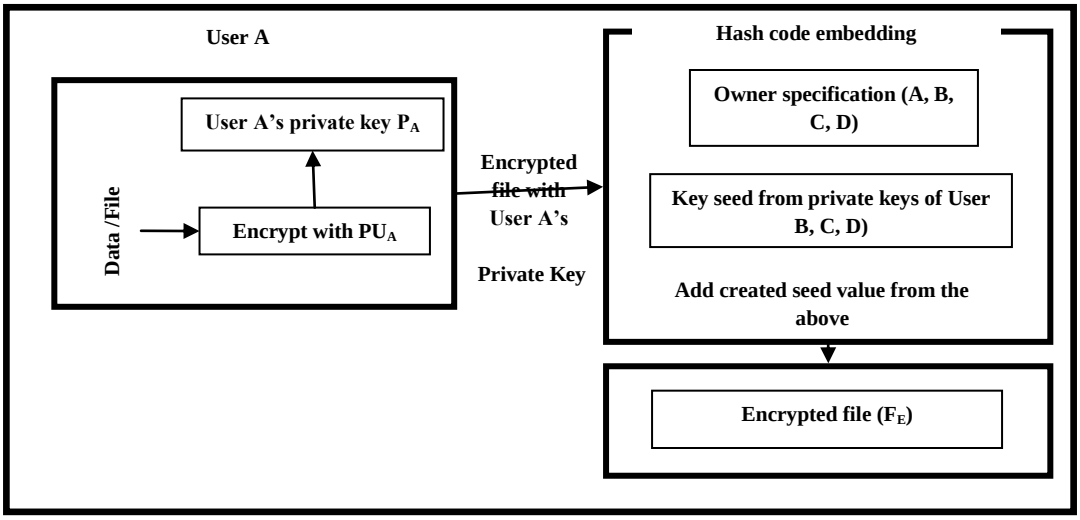

Fig 3: Encryption process

The above diagram represents the encryption process using the Multi_Key crypto phase. This follows the public key cryptography model, where the file can be encrypted using the private key.

3.2 Multi_Key Decryption Process:

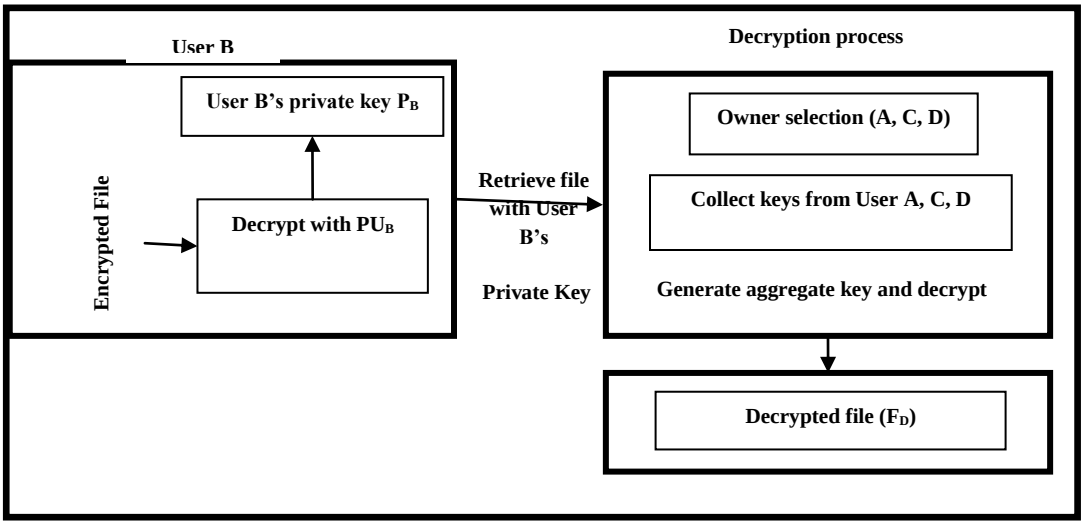

Fig 4: Decryption Process

The above diagram represents the decryption process using the Multi_Key crypto phase. This follows the public key cryptography model, where the file can be decrypted using the aggregated key. For each file the authentication has been verified with the owner's private keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

IV.RESULTS AND DISCUSSION

To evaluate the performance of the proposed MAFS schemes, computational and execution time are considered.The results chapters prove the proposed system is outperformed than the existing techniques. This considered the verification delay and aggregation key creation delay for deployed data on the cloud in the process of retrieval. Encryption and key generation and verification delay are specified below.

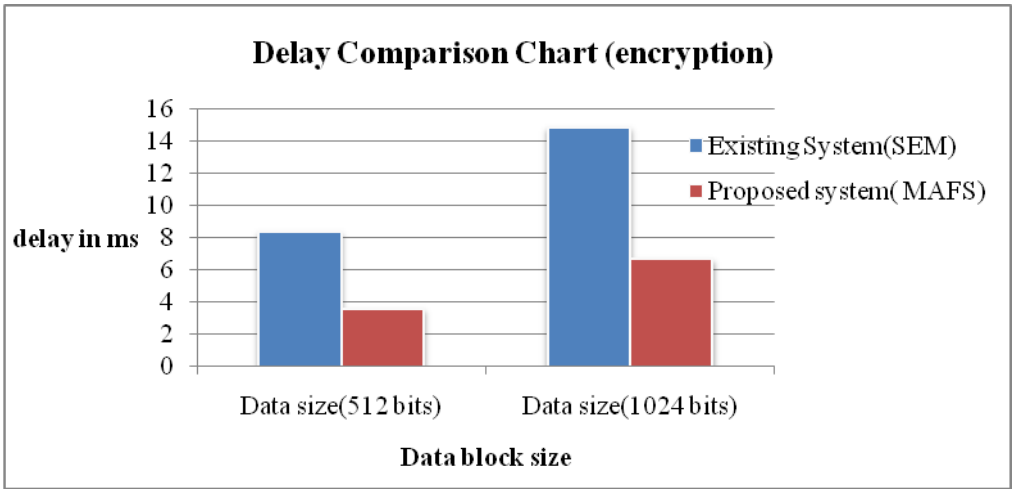

Fig: 5 Delay Comparison chart

The above delay comparison chart indicates the execution time for the algorithm to produce cipher texts and corresponding keys before storing the data.

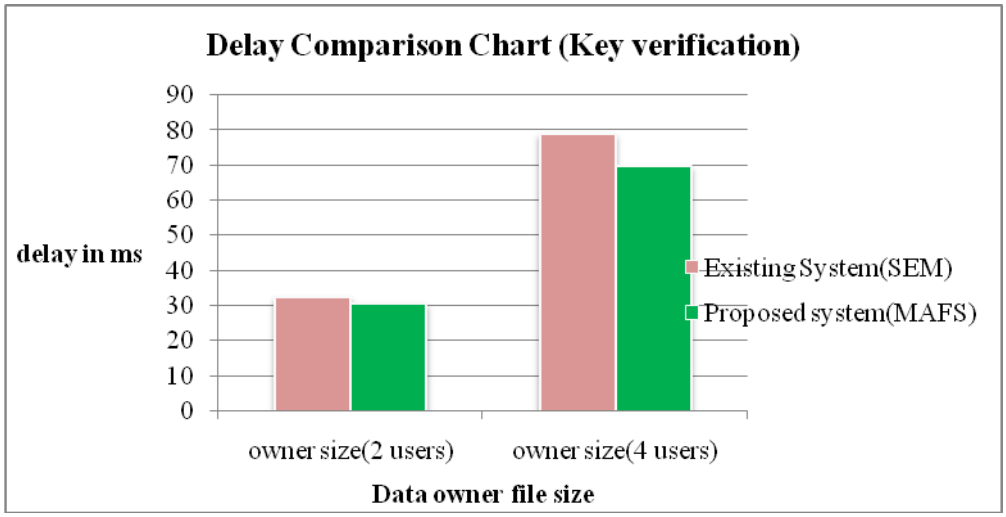

Fig: 6 Delay Comparison chart

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

The above delay comparison chart indicates the execution time for the algorithm to produce normal texts from the cipher data and corresponding keys before storing the data.

V CONCLUSION AND FUTURE WORK

In this work, we have provided a new privacy based multi owner file access system called as MAFS. During user data accessing in the cloud computing to achieve the file access the authentication is established to guarantee data confidentiality, ownership and data integrity. This is achieved by exchanging the sms with the data owners and validate in the server side. User privacy is enhanced by sending the unique key via sms and aggregate them in the cloud server about the users' access desires. Forward security is realized by the session identifier sms to prevent the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications where there are many owners are there for one file.

In the future this concept can be improved to provide better cost optimized output whenever users access the multi owner files. And also the future work can be as the improvised encryption algorithm process.

REFERENCES

[1] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.
[2] Title: A Break in the Clouds: Towards a Cloud Definition Author: Luis M. Vaquero, Luis Rodero-Merino , Juan Caceres, Maik Lindner Telefonica Investigacion y Desarrollo and SAP Research Madrid, Spain, EU and Belfast, UK, EU
[3] S.S.M. Chow,C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.
[4] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.
[5] Zhu, Yan, et al. "Cooperative provable data possession for integrity verification in multicloud storage." *Parallel and Distributed Systems, IEEE Transactions on*23.12 (2012): 2231-2244.
[6] Wang, Huaqun. "Proxy provable data possession in public clouds." *Services Computing, IEEE Transactions on* 6.4 (2013): 551-559.
[7] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *Parallel and Distributed Systems, IEEE Transactions on* 24.9 (2013): 1717-1726.
[8] Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." *Parallel and Distributed Systems, IEEE Transactions on* 22.5 (2011): 847-859.
[9] Wang, Cong, et al. "Toward secure and dependable storage services in cloud computing." *Services Computing, IEEE Transactions on* 5.2 (2012): 220-232.
[10] Dunning, Larry A., and Ray Kresman. "Privacy preserving data sharing with anonymous id assignment." Information Forensics and Security, IEEE Transactions on 8.2 (2013): 402-413.