INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

DESIGN OF A SECURE CRYPTO-MECHANISM FOR DATA STORING AND SHARING IN CLOUD ENVIRONMENT

[1]Seema Tahalyani, [2]Dr.S.M.Ghosh

[1]M.tech. (Software Engineering), Department of Computer Science & Engineering, Rungta College of Engineering & Technology. Bhilai, India. E-Mail: seematahalyani@gmail.com
[2]Associate Proffessor,Department of Computer Science & Engineering,Rungta College of Engineering & Technology,Bhilai, India E-Mail: samghosh@rediffmail.com

Abstract: - Data storing and sharing is an imperative utility of Cloud computation. Cloud provides such an environment that it resembles such that users are working on a local network. Cloud serves users with many pros one such merit is that it offers large pool of configurable computing resources that can be shared. This sharing facility is not only limited to resources but also involves data to be shared among users. However data sharing functionality can cause outsourced data to get exposed to many security threats in a shared tenancy environment like that of cloud because client doesn't have direct control over data storage. To secure data in cloud storage many attempts have been made, one such impactful attempt is using a cryptosystem which secure data from malicious attacks. In this paper we are going to propose a secure crypto-mechanism in which encryption process is applied at twofold layer to keep both data and keys secure. Firstly, the proposed designed utilizes both symmetric key cryptography and asymmetric key cryptography for secure data sharing. Secondly, both stored data and keys are encrypted. Further the work checks data integrity before sharing. So that when delegate receives both data and keys they are in encrypted form without any tampering and reach to receivers through an encrypted channel. This process enhances data security in cloud environment. This proposed methodology is an efficient way for scalable and flexible sharing of data.

Keywords: - Cloud computing, cloud storage, data sharing, Cloud security, Encryption, decryption.

I. INTRODUCTION

Each and every day a large amount of data is being generated from various sources and this data has to be stored somewhere for further analysis. With raise in data generation, large storage area is also required. This may cause any organization to spend lots on infrastructure and storage devices. Cloud computing paradigm assists in planning for storing large pools of data without any extra effort. With success of utility computing and grid computing a new concept emerged known as Cloud Computing. Cloud Computation is defined in various ways; one important definition is given by Gartner. According to Gartner [2], Cloud Computing may be defined as:

"**Cloud computing** is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies." Cloud environment helps organizations to create and deliver solutions of IT related problems by permitting them to access resources and services flexibly and efficiently."

Cloud computing is a next generation technology and is gaining popularity as a conglomerate model. Cloud environment consist of a large pool of computing resources which can be configured according to needs and requirement of consumers. Fig.1 depicts how various resources are connected to cloud and shared among various users.

Fig.1- Resource Sharing in Cloud Environment

Virtualization is the foundation of cloud environment. It is virtualization that creates an illusion of utilizing resources which are not actually present in front of a user. Now organization can outsource their data without investing lot on infrastructure development and deployment. Lots of benefits are achieved while storing data in cloud such as: reduction in cost of IT construction, management and maintenance of infrastructure; resource pooling; rapid elasticity, measured services; broad access network; resource agility etc. But at the same time storing data in cloud exposes data to many security intimidations that can injure data confidentiality, integrity, privacy and availability. Confidentiality refers to protecting data from getting disclosed among illegitimate users. Availability refers to the availability of data whenever user wants to access it or retrieve it. Integrity refers to protecting and securing data from malicious modifications. Since after outsourcing data is no longer in control of owners, even they are unaware of the facts of where the data has been stored and in which location. They only have right to access their data at any time and from many place.

For securing data several techniques have been implemented, for instance authentication process in which only the users with valid username, password or with other identity proofs like retina scan, use of smart card or finger print checking are involved. Another scheme that is implemented is authorization; in authorization process a list of clients can be created who have been granted authority to access the data. This process can be implemented at various levels such as one can achieve access rights of more portions of data and other may get access rights of lesser portions. Last but not the least the mostly used scheme is application of encryption process over data to convert it into unreadable form so that if data is leaked somehow nobody can be able to make use of it without decrypting it. In this paper we are going to use all the above three schemes jointly to augment security level of cloud storage.

Cloud stores users' data in a place which is known only to the organization which is providing cloud services to the consumer. This can result exposure of users data to others and may cause tampering or attackers a chance to hack sensitive data. So the users are required to implement extra mechanism that can protect their sensitive data from being harmed. Encryption process is the oldest and best way by which any sensitive data can be made secure. As the time changes many cryptosystem have been developed but these again have to be made more

efficient as time passes as attackers also become smart enough to break the system. So a more secure mechanism is required to keep data protected. If data remains in encrypted form than if data is lost also or attacked by some malicious attackers there is no need to worry since without keys they can't do anything and in our system since keys are also encrypted which again provide security to users data the threat become negligible. Before describing cryptosystem first of all we need to understand various cloud computing models which are important before implementing the algorithm.

II. CLOUD MODELS

Cloud computing systems can be categorized mainly into two groups, first is based on location and management and second one is based on services offered by cloud vendors. These two models are: Deployment Models and Service Models. Generally Cloud computing systems are categorized mainly into two groups: Deployment Model, and Service Model. This keeps other models in isolation. Different forums have also introduced cloud models which have also become popular and are followed, these are: NIST model and Cloud Cube Model.

A. Deployment Models:

Deployment model of cloud refers to the cloud system which is categorized based on the locations and management. Clouds are classified based on the purpose and nature of the cloud. There are four types of deployment models: ***Public Cloud, Private cloud, Hybrid Cloud and Community Cloud.*** Different deployment cloud models are discussed below and are illustrated in fig.2:

a) **Public Cloud:** Public cloud or External Cloud model refers to a cloud infrastructure in which services are made public to the consumers. These cloud models are owned by big organizations which provide services to the consumers on the rental basis. It is an on premise service.

b) **Private Cloud:** Private clouds or Internal Clouds models refer to a cloud infrastructure which provides services exclusively to a single organization and to the consumers of that organization. This model is like private property which is solely owned by that organization that acquires it. It may be an on premise or off premise service. It may be managed and controlled by the acquired organization or some other third party.

c) **Hybrid Cloud:** Hybrid cloud model is a combination of various other cloud models such as Public, Private or community models. In spite of being a combination of other models each model in Hybrid cloud model retains its identity and uniqueness but act as a unit. This boundness is due to some standardized or proprietary technology and also enables application portability.

d) **Community Cloud:** Community cloud model refers to a cloud system which is mainly built for some specific organization, group of consumers or an individual that have common issues of interest. For instance military, government employees or for some mission. It may be managed and controlled by the organization or some third party or by both. It is an on premise or off premise service.

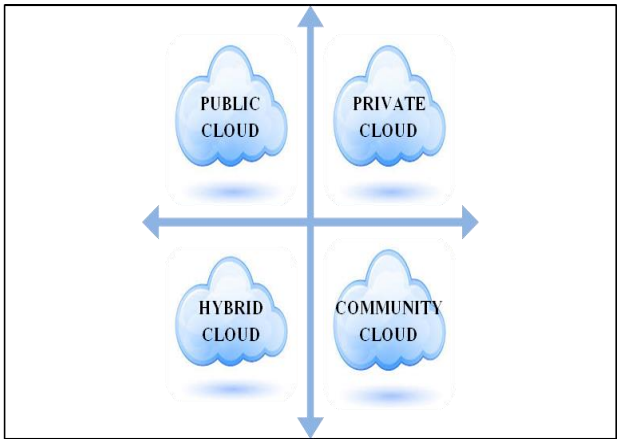

Fig-2 Deployment Models of Cloud Computation

B. Service Models:

Cloud provides a large pool of configurable computing resources as a service to the cloud consumers. Different cloud vendors offer different types of cloud services. This collection of different services offered by cloud

vendors are known as "***Service Models***". Many types of service models have been defined in the literature of cloud computing which have the following structure:

"***XaaS" means X as a Service;***

Where 'X' stands for resources like Infrastructure, Platform, Storage, Software, Compute or Compliance etc. These services take the form like ***IaaS*** (Infrastructure as a service), ***PaaS*** (Platform as a Service), ***StaaS*** (Storage as a Service), ***CaaS*** (Compute as a Service), ***CmaaS*** (Compliance as a Service) and ***IdaaS*** (Identity as a Service). But only the main three services which mainly form a service models are: ***IaaS*** (Infrastructure as a service), ***PaaS*** (Platform as a Service), ***and SaaS*** (Software as a Service). These three service model is commonly known as **SPI (Software Platform Infrastructure)** model of Cloud Computing. Services provided by SPI models are listed in fig. 3.

a) ***IaaS*** (Infrastructure as a service): This service model provides virtual infrastructure like machines, storage, networks, computing and other hardware resources to the consumer to deploy and run any requisite software. Consumer doesn't require maintaining or managing any hardware they have provisioned from service provider. Client only have to look at the other aspects of application development and deployment such as operating system and other user interfaces.

b) ***PaaS*** (Platform as a Service): This service model has the potential to deploy their application on cloud infrastructure. The applications can be created by clients using different programming languages, libraries and tools that are provisioned by service providers. Major services provided by PaaS are; virtual machines, operating systems, development frameworks and transactions control etc. The consumer does not have to manage these resources they just have to use these resources to develop, test and deploy their application onto cloud.

c) ***SaaS*** (Software as a Service): the SaaS model offers operating environment and interface management to cloud consumers. Usually client access the SaaS model through a thin client such as a web browser to for entering and managing their data. All other activities such as infrastructure management, software up-gradation, application maintenance all is done by the cloud vendors, consumer does not have to worry about it.

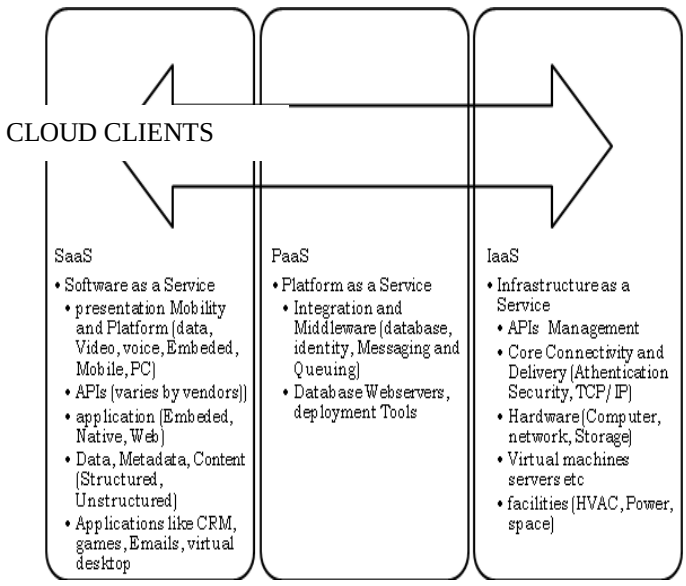

Fig-3 Cloud Service Models

C. NIST Model:

NIST (National Institute of standard and Technology) have given working definition cloud computing differently from common definitions of cloud systems. This working definition distinguishes between deployment model and service model of cloud computing. According to the NIST model, Cloud neither requires virtualization technology for pooling of resources nor requires feature like multi-tenancy to be supported by cloud. Cloud systems are now started supporting Service oriented Architecture (SOA) in which a set of

individual modular components interact with each other using standard protocols. The NIST cloud model doesn't support various services like provisioning of resources, integration of services and services of brokers etc. Fig-4 illustrates NIST Model of Cloud Computing with relationship between various models. The bottom layer consists of Service Attributes such as broad network access, measured services, on demand self service, rapid elasticity etc. Middle layer composes Service Models such as IaaS, PaaS and SaaS etc. and the topmost layer is made up of deployment models such as Private, Public, Community or Hybrid.

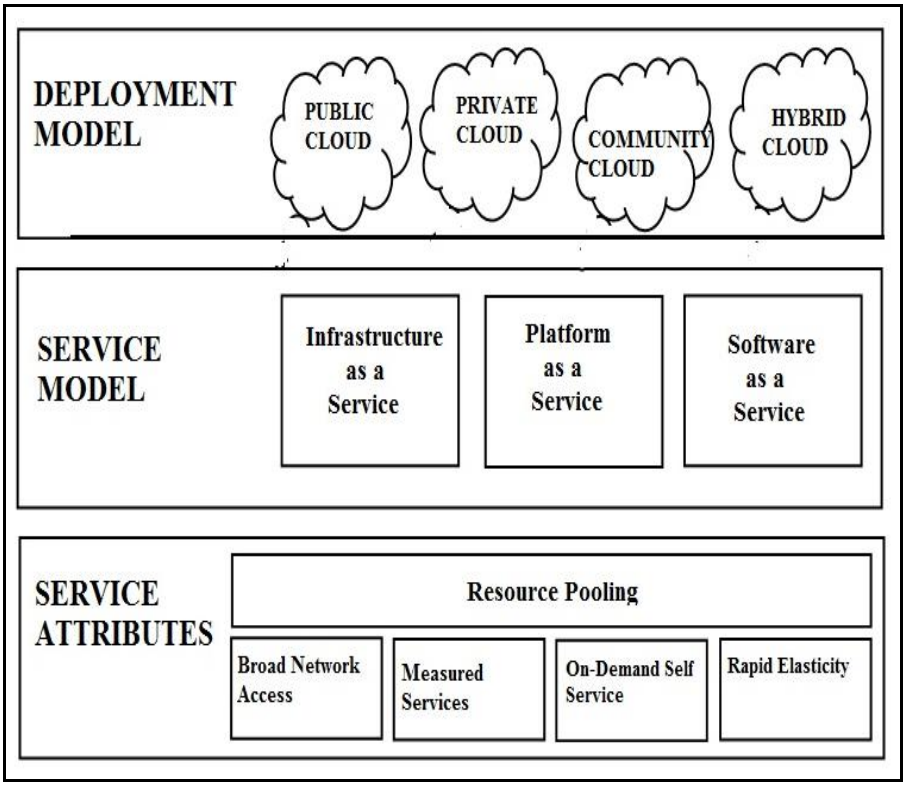

Fig-4 NIST Model of Cloud computation

D. The Cloud CUBE Model:

An association society is maintained by Open Group Known as "Jericho Forum". The main task of this forum is to provide protection to Cloud Networks. This group has defined a model which classifies a cloud network into four dimensional factors based on the concept of where the boundaries of cloud networks start and ends and from where client's network boundary starts. These four dimensions in cube model are depicted in fig.5. These four dimensions are as follows:

- **Physical location of the data**: It determines boundary of an organization as Internal or External.
- **Ownership:** This dimension is described as "**Proprietary (P)" "Open (O)" and** measures the ownership of technology, interoperability, data transfer ease and degree of vendor application lock-ins.
- **Security boundary:** This dimension measures whether the operations performed is inside or outside the security boundary or network firewall. If operation is performed inside security boundary it is known as "**Perimeterised**" (Per) and if operation is performed outside security boundary it is known as "**De-Perimeterised**" (D-P).
- **Sourcing**: This dimension describes whether a service is provided by the customer or service provider. If the service is provided by customer it is known as "**In-sourced"** and if the service is provided by service provider it is known as **"Out-Sourced".**

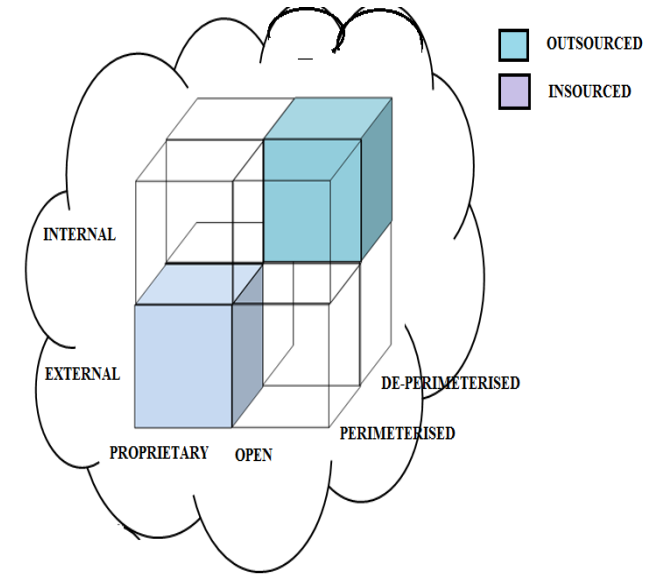

Fig.5 Cloud Cube Model

III. SECURITY CONCERNS IN CLOUD FOR DATA STORING AND SHARING

As we had discussed earlier clouds are open some of the threats when storage is acquired as a service. Some of the most critical security threats are mentioned in Table-1.

Table-1 Security threats and Cloud Environment

S.No	Security Threat	Description
1	Data breach and Data Loss	Losing of sensitive data due to some malicious attacks
2	Account or Service traffic Hijacking	Different ways to hijack an account are phishing, reusing of credential and password fraud
3	APIs and Interface Insecurity	weak set of interfaces can make cloud services exposure to many critical issues causing harm to both organization and cloud customers
4	Denial of Service	stopping or avoiding cloud user from accessing their cloud services and applications by making the cloud services like processing power, memory space and bandwidth low and disordering finite system resources
5	Malicious Insiders	Any one that works inside to a cloud service providing organization and have access to the consumer's sensitive information can cause harm.
6	Nefarious and Abuse of Cloud Services	Malicious attackers can make abusive use of cloud services because of weak registration and relative anonymity of consumers. Users who want to use cloud services gets registered to cloud providers with their credentials which may be used by nefarious user to damage consumers' data
7	Insufficient Due diligence	Problems occur due to Cloud service providers terms and conditions, lock-ins, cloud environment and how much secure is cloud for consumers, mismatch between customers requirement and service provided, insufficient designers that are capable to work in cloud environment
8	Shared Technology Vulnerabilities	Delivery models share their services and this sharing may cause lots of vulnerabilities. Any of the underlying component if is compromised may cause exposure of not only consumers data but may lead to compromise across and expose services of cloud providers.
9	Unknown Risk Profile	Before adopting cloud services consumers should check features and functions of Cloud service providers, who are sharing your infrastructure and where is link getting redirected which almost always remain not a topic of interest when cloud services are opted.

IV. REVIEW OF LITRETURE

In this section, firstly we are going to describe the related work by different authors in examining different security threats in cloud environment and different encryption schemes that had been proposed to face these threats. By analyzing these encryption schemes we may be able to identify the problems in these techniques and able to make some new one to make the data storing and sharing in cloud more efficient and effective.

Yu et al [5] in his work addressed that in cloud computing basic security issues are data confidentiality, data Integrity and data availability (CIA). Due to the intrinsic characteristics of cloud computing data security becomes more vital. Before moving data to cloud environment cloud consumers should use a set security suits to secure their data or applications. They described that Confidentiality, Integrity and Availability should be maintained not necessary that all the three should be maintained but all three should not be compromised also.

Wang et al [7] in their work focused on the critical problem of integrity of data stored in cloud storage. Since in cloud storage users doesn't have direct possession over their data due to which threat of data integrity becomes a fearsome task. So a system was required that can restore and verify data integrity without any worry on the users part and users would be able to access cloud storage efficiently. They proposed a privacy-preserving public auditing system to maintain security for data stored in cloud environment without compromising privacy of data. They used homomorphic linear authenticator and random masking to guarantee that no knowledge would be learnt by the third party auditors (TPA) about the data stored on the cloud server during the auditing process. They also extended their public preserving public auditing protocol into a multiuser setting with which auditing task can be performed in a batch manner by TPAs to make the scheme more efficient.

Wang et al studied this problem of data security and suggested an efficient and publicly verifiable approach in which data integrity is secured without compromising anonymity of a user without extra overhead. Earlier before utilizing data, owners and users were suggested to verify integrity of cloud data with Provable Data Possession (PDP).

But ***Wang et al*** **[8]** also proposed a system consisting of a Security Mediator (SEM). This SEM generates verification signatures or metadata on outsourced data for data owners. This process separate PDP and anonymity protection mechanism from each other so that any organization could implement their own anonymity authentication system. This decoupling will make cloud oblivious from anonymity authentication mechanism implemented by the organization and cloud will only deal with metadata generated due to PDP usage. As a result identity of data owners will not be compromised and no extra expense is required due to anonymity preservation that occurs in PDP. This SEM not only maintains data integrity but also preserve data privacy as SEM doesn't learn anything about data stored in cloud. A multi-SEM is also introduced which increases potential and avoids delays during any SEM failure.

The specialist mainly classified encryption process into three main sections. Literature study has been accomplished under four categories: In our first study we examined security threat for data sharing in cloud computing; in second study we analyzed various encryption approaches and finally had a review on key and short ciphertext generation schemes.

Now we are going to present a brief review on several works which are proposed by different authors. For storing and sharing data in cloud server there are many cryptographic schemes, which had been developed earlier for secure sharing. Some of such techniques are: Symmetric key encryption, Public key encryption, both symmetric (or public key) encryption. Using these encryption techniques different encryption schemes has been discovered. Some of them are-

- Hierarchical key assignment
- Identity based encryption (IBE)
- Attribute based encryption (ABE)
- Proxy Re-encryption (PRE)
- Key aggregate cryptosystem (KAC)

A. *Hierarchical key assignment*:

In a hierarchical key assignment schemes the public data is categorized like a tree structure and then keys are assigned for a given branch. Hierarchical key assignment is a method to assign encryption keys to access classes in a partially ordered hierarchy. The private information in the higher classes can be used to derive keys for lower abstraction in the hierarchy.

Atallah et al has proposed solutions to the problems of key assignment and management for access hierarchies. Also they described solutions for decreasing space complexity of public information and storing of hierarchies and making the updating process local in the hierarchies. There scheme is based on symmetric-key operations [12]. *Akl et al* proposed a scheme that imposes access control in a system where hierarchy is represented by a partially ordered set. This scheme requires storing large numbers of cryptographic keys for the users that are highly placed in the hierarchy [10]. *Santis et al* in his paper described the design of a hierarchical key assignment schemes which are provably-secure and support dynamic updates to the hierarchy with local changes to the public information and without requiring any private information to be re-distributed [11].For both symmetric-key encryption and public-key cryptosystem, these schemes would produce keys but public-key cryptosystem are more expensive than symmetric key cryptosystem.

B. *Identity Based Encryption (IBE)*

Identity Based encryption is a type of cryptosystem in which the public key of a user is some unique information about the identity of the user (e.g. a user's email ID). This can use the text-value of the name or domain name as a key or the physical IP address it translates to. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key referred to as *master key*.

Given the master public key, any party can compute a public key corresponding to the identity *ID* by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ***ID*** contacts the PKG, which uses the master private key to generate the private key for identity ***ID.*** As a result parties may encrypt messages or verify signatures with no prior distribution of keys between individual participants. Based on Diffie-Helman assumption on elliptic curve, a system was made in which chosen cipher-text security in the random oracle model is shown [13].

C. *Attribute-Based encryption (ABE)*

Attribute based encryption is a type of public key encryption in which the secret key of a user and the cipher-text are dependent upon attributes e.g. the country he lives, or the kinds of subscription he has etc. In such a system, the decryption of a cipher-text is possible only if the set of attributes of the user key matches the attributes of the cipher-text. A crucial security issue of ABE is collusion resistance. A system that holds multiple keys should only be able to access data if at least one individual key grants access.

Sahai and Waters [14] used Attribute-based encryption (ABE) in which user's key and cipher-texts are labeled with sets of descriptive attributes and a specific key can decrypt a particular and specific cipher-text only if there is similarity between the users' key and attributes of cipher-text. This system is applicable only if at least ***k*** attributes matched between a cipher-text and a private key. Goyal et al described a private encryption for fine grained sharing of encrypted data known as Key-Policy Attribute based encryption (KP-ABE) [15].

D. *Proxy Re-Encryption*

In Proxy Re-encryption (PRE), special information is allotted to a proxy that permits translation of cipher-text under a key into cipher-text under a different key. The proxy used cannot learn itself anything about the encrypted message under any of the key [16][17]. Numerous re-encryption techniques achieve semantic security and various others require security against chosen cipher-text attacks.

E. *Key aggregate cryptosystem*

Key-Aggregate Cryptosystem (KAC) is a public key encryption scheme. In KAC data owners encrypts a message under a public key and an identifier of cipher-text. Cipher-texts are categorized into different classes. The key owner with a master secret key can extract secret keys for different classes. These keys have aggregate

powers equal to the many secret keys and are compact as single key. Decryption key or the aggregate key are then sent to the delegate to encrypts the data they wanted from data owners [19].

To secure data in cloud storage and while sharing data various standard models have been developed. Using encryption gateway makes sensitive data more secure from both malicious insiders and malicious outsiders. Various combinations of these encryption schemes can be used by different cloud consumers as per their need and requirements.

V. PROBLEM IDENTIFIED

Major problems identified after reviewing work of various authors is that maintaining data confidentiality, privacy, integrity and availability is a major task in cloud. Secondly, the elementary problem in modern cryptography is leveraging of data. If encryption process is applied efficiently than also many problems are faced by data owners. Some of the issues that arise that needs to be considered are: achievement of an efficient cryptosystem, strong key generation for encrypting and decrypting data, effective sharing of encrypted data and keys, secure delegation of decryption keys to the delegate and lastly maintaining and managing access rights of the users so that they can perform their activities seamlessly. Previously built system lacks in resolving some of these problems. So it is required to create a cryptosystem which should be compatible with cloud server and as well as with the users. In the proposed methodology we are designing a cryptosystem to achieve above goals and allow efficient, flexible and secure data sharing over cloud environment.

VI. OBJECTIVE

So objective of our work can be stated as follows:

"To design a secure crypto-mechanism in which data is encrypted server side using both asymmetric and symmetric key encryption bundled with hash function to check data integrity. To make cryptosystem more viable, keys are also be encrypted and password protected. "

VII. METHODOLOGY

The most crucial requirement of file syncing and sharing process is the data security and privacy. So we can solve this issue by designing a cryptosystem which provides data security, privacy, confidentiality and integrity. In the proposed methodology cloud application supports both server side as well as client side encryption. In server side encryption, the process of encryption and decryption happens at the server side. Server side encryption is important for those users who access external storage devices of some third party for storing their surplus data. On the other and Client side encryption can be enforced by those clients who requires more security for their sensitive data.

Here we will mainly focus on Server Side encryption. First of all let us consider a scenario of a private organization where many employees work at various levels. The owner of organization may not want to share each and every detail with everyone but wants access right of each and every data to each and every employee so that no unauthorized user can use the data. This encryption process will help them for securing their data from malicious attacks.

In our work we are going to describe a framework of a cryptosystem which gives authority to administrator to monitor and control access rights of data stored in cloud environment from both internal and external attacks. The entire cryptosystem describes the whole process of how data is stored and can be shared securely wit others in a shared tenancy environment like cloud. Figure-6 illustrates the entire process of data sharing in cloud.

Fig.-3 Steps of Storing and Sharing data in cloud

First we will describe framework of encryption process than we will define algorithm of cryptosystem.

A. *Framework*

The proposed methodology consists of five polynomial time algorithm which occurs as follows:

A public system parameter is generated by the data owner by means of Setup, in other words an account is created in cloud environment and storage as a service is received that can be accessed by data owner for storing and sharing. A public/private key pair and a file key associated with each file are generated by means of KeyGen. Messages are encrypted using Encrypt algorithm in which whenever a file is uploaded an associated file key encrypts large files and then with public/private key pair. Data can be shared using Share algorithm in which a share key is generated for sharing the keys to users. After successful sharing of keys data user can decrypt data via decrypt.

B. *Definition*

The encryption decryption process involves following distinct keys.

- **Private/Public Key pair (SK/PK)**: Every user has a set of "Private/Public Key" pair. The key is an asymmetric key which is 4096-bit strong Key pair consisting of a Public Key and a Private Key. Users' login password is used to again encrypt Private Key using AES-128. In addition to Private Key , there are two key pairs , one is Public Key for sharing and decrypting and other key pair is optional which is a recovery Key pair accessed if users' loses their keys.
- **File key (FK):** Every file is associated with a "File Key" which is unique and randomly generated. It is used to encrypt files stored by users symmetrically with AES-128. For large files this key is used. These keys are 183 byte strong Keys and ASCII in nature. These Files Keys are again encrypted with Public Keys of all users who have access to those files. This File Key increases the efficiency of encryption since if any file user is added or removed than whole file need not be re-encrypted again only a small File Key is required to be re-encrypted.
- **Share Key (SHK):** For sharing a file between multiple users a "Share Key" is used. Whenever a file has to be shared between groups of users OpenSSL which is an encryption library generates a Share Key. The group members can only decrypt the file if they have the combination of Private Key and their respective Share Key.

The process can be stated in five phase which are as follows:

- **Setup ():** A public system parameter is generated that Setup a user account in cloud Storage. Login and get authorized to access the storage service.

- **KeyGen (SK/PK) or KeyGen (FK) or KeyGen (RK)**: KeyGen generates a Private Key "SK" for the user to whom file is to be shared and a Public Key "PK" which is accessed by file owner. If a large file has to be shared a File Key "FK" is generated and if any key is lost in that case a recovery key "RK" is generated.
- **Encrypt (FK, PK, *msg*, CT)**: Whenever a file is uploaded it is encrypted with a "FK" and then with the Public key "PK" of file user i.e. if a "msg" has to be encrypted then it is encrypted by a File Key "FK" and a Public Key "PK". When the file gets encrypted a ciphertext "CT" is generated.

- **Share (SHK, CT):** A Share Key "SHK" is generated if the file is shared by others. And users will receive file in an unencrypted form i.e. they will receive ciphertext "CT"**.**

- **Decrypt (CT, SK, SHK, *msg*)**: When a user gets file in encrypted form from file owner they can decrypt the ciphertext "CT" using Private Key "PK" and a secret key "SK". In turn it generates the original file "msg" in unencrypted form.

The sharing process works in the following manner; the data owner stores his/her data in the cloud storage in an encrypted manner. Whenever data owner encrypts files using asymmetric algorithm a pair of public and private keys are generated and owner secures it with himself. The Private Key is sent to the users who acquire the authority to access the files. Large files are encrypted using associated File key and Public key which results in generation of a cipher-text. Suppose a user who could be a friend or a relative or a colleague of data owner i.e. a known person who wants access to access partial data of data owner stored in cloud storage. Then data owner would send the respected share key to the user. Then the user with respected share key and private key can decrypt the file and use the data required. Figure 4 illustrates encryption process between two cloud users and key sharing between them. Proposed cryptosystem would provide a strong key which is difficult to break and thus provide protection to sensitive data stored in cloud storage.

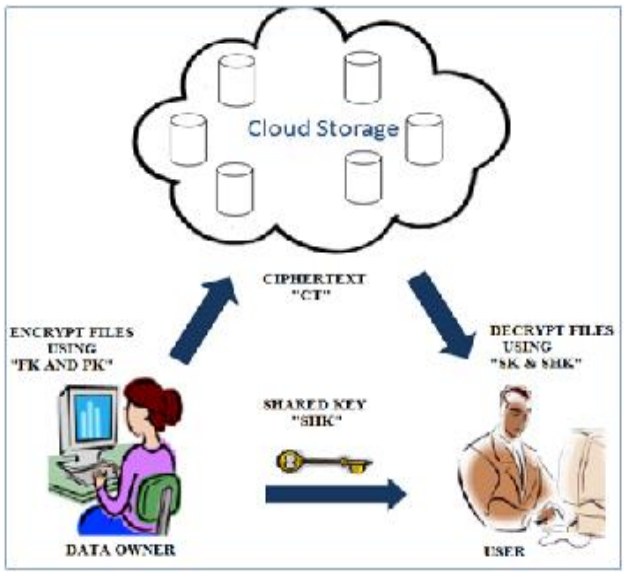

Fig.4- Sharing of encrypted data

VIII. RESULT AND DISCUSSION

The enchantment of accessing a twofold algorithm comes from linear parameter. The algorithm implemented in the proposed methodology is a twofold process which increases the speed up ratio of encryption and decryption process. Our main aim was to provide an encryption scheme that offers security to both the data stored at rest and to the shared data. Another main was to construct a leakage resilient system and reduce secure storage. The

user needs to believe parameter generator for generating random values and erasing any transient values used. The encryption algorithm produces a strong public/private key pair which is difficult to break and if tried so requires high technology infrastructure and long time for processing to retrieve keys. Secondly, if keys are retrieved (in case) than same long process is again has to be implemented by attackers to use the key since again the keys are in encoded form and password protected. So it is suggested to set a strong password while accessing this process.

Again the processing time taken by cloud server to complete the encryption decryption process in local network as well as in cloud network are comparable this means approximately same processing time is required by both type of server whether it is local or cloud. For analyzing the performance of proposed methodology we have compared this scheme with various other schemes developed earlier, which is shown in table-2.

Table-2 Comparison of various Cryptosystems

Crypto-systems	**Encryption type**	**Ciphertext Size**	**Decryption key Size**
Hierarchical based Encryption	Symmetric or Asymmetric key	Constant Size	Non-constant size
Symmetric Key Encryption	Symmetric key/ Private Key	Constant Size	Constant Size
Identity Based Encryption	Asymmetric key/ Public Key	Variable Size	Constant Size
Attribute Based Encryption	Asymmetric key/ Public Key	Constant Size	Variable Size
Key Aggregate Crypto-system	Asymmetric key/Public Key	Constant Size	Constant Size
Proposed Crypto-system	**Both Asymmetric and Symmetric**	**Variable Size**	**Variable key**

CONCLUSION

Organizations have started widely accessing Cloud storage by outsourcing their data and taking gain from various services provided by Cloud. But there is always a question of security and privacy maintenance that arises in the minds of cloud consumers while outsourcing their sensitive data. To answer these questions various security techniques have been proposed which are shows efficiency in different scenarios. Use of cryptosystem is one of the best options that are used widely. Cryptographic schemes can be made more influential and powerful by utilizing powerful mathematical tools. Combination of multiple keys in single application can make application effective to face intruders attack and can take the application to a different level which may offer more security and privacy.

The cryptosystem proposed in this work provides security to data and applications at various level of abstraction and increases the work of hackers as they have to imply more effort to steal the data. In this work we considered how to make encryption process more efficient by increasing its reliability. By using different type of keys and by encrypting Keys data is protected twofold. This scheme is than packaged together with cloud server. This enhances the security of data and application stored in cloud. The delegate gets secure key in encrypted form and can decrypt it using the keys and valid passwords. Our approach is a leakage re-silent system that has greater impact for the selective sharing of data at coarse grained level. The application can be securely accessed through mobile devices proficiently. It decreases data leaking to a higher an extent.

REFERENCES

[1] P.Mell and T.Grance, "The NIST definition of Cloud Computing,"http://csrc.nist.gov/publications/nistpubs/800-145, September 2011.
[2] T.Erl , Z. Mahmood, R. Puttini, 2013, "Cloud Computing Concept, Technology and Architecture", pp: 26-44.
[3] Cloud security alliance, "The Notorious Nine: Cloud Computing Top Threats in 2013",http://www.cldsecurityAlliance.org/topthreats. L.Hardesty, secure Computers Aren't so Secure, MIT Press, http://www.physorg.com/news176107396.html, 2009.
[4] L.Arockiam, S.Manikandam, "Efficient Cloud storage Confidentiality to ensure data security". Computer communication and informatics, 2014 International conference.
[5] S.Yu, W Lou, K.Ren, "Data Security in Cloud computing", Ch-5.3, pp: 1-29
[6] S.S.M.Chow, Y.J.He, L.C.K.Hui, and S.M.Yiu, "SPICE- Simple Privacy-Preserving Identity- management for Cloud Enviroment,"Proc.10th Int'1Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp.526-543, 2012.
[7] C.Wang, S.S.M.Chow, Q.Wang, K.Ren, and W.Lou, "Privacy-Priserving public Auditing for secure Cloud Storage," IEEE Trans. Computers, vol.62, no.2,pp. 362-375, Feb. 2013.
[8] B.Wang,S.S.M.Chow, M.Liu, and H.Li,"Storing Shared data on the Cloud via security-mediator," proc.IEEE 33rd Int'1 Conf. Distributed Computing systems (ICDcs), 2013.
[9] A.Hudic, S.islam, p.Kieseberg,"Data Confidentiality using fragmentation in Cloud computing", Int.J.Communication Networks and Distributed Systems, Vol.1, No.3/4,2012.
[10] S.G.Akl and P.D.Taylor,"Cryptographic Solution to a Problem of access Control In a hierarchy," ACM Transactions on Computer Systems (TOCS), vol.1, no.3,pp.239-248,1983.
[11] G.Ateniese, A.D.Santis, A.L.Ferrara, and B.Masucci, "Provably Secure Time Bound Hierarchical Key assignment Schemes," J.Cryptology, vol.25, no. 2, pp.243-270, 2012.
[12] M.J.Atallah, M.Blanton, N.Fazio, and K.B.Frikken, "Dynamic and Efficient Key management for Access Hierarchies," ACM Transactions on Information and system security(TISSEC), vol.12, no.3. 2009.
[13] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139, pp. 213–229. Springer, 2001.
[14] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT '05, ser. LNCS, vol. 3494, pp. 457–473, Springer, 2005.
[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, ACM, 2006.
[16] R. Canetti and S. Hohenberger, "Chosen-Cipher-text Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 185–194, ACM, 2007.
[17] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient Unidirectional Proxy Re-Encryption," in Progress in Cryptology - AFRICACRYPT 2010, ser. LNCS, vol. 6055, pp. 316–332 Springer, 2010.
[18] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1–30, 2006.
[19] C.K.Chang, S.S.M Chow, W.G. Tzeng, J Zhou and R.H.Deng, "Key Aggregate Cryptosystem for scalable data sharing in cloud storage", in IEEE Transactions on Parallel and Distributed systems, Vol.25, issue: 2. Year: 2014.
[20] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.
[21] C.K. Chu, S.S.M.Chow, W.G.tzeng,J.Zhou and R.H.Deng, "Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," in IEEE Trans. On para. And distributed systems, vol.25, issue. 2, 2014.
[22] V. Spoorthy, M. Mamatha, B. Santhosh Kumar, "A Survey on Data Storage and Security in Cloud Computing",IJCSMC, Vol. 3, Issue. 6, pp.306 – 313, June 2014.
[23] S V.Nandgaonkar, A. B. Raut, "A Comprehensive Study on Cloud Computing", IJCSMC, Vol. 3, Issue. 4,pp.733 – 738, April 2014.
[24] K.Lee, " Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications,Vol. 6, No. 4, October, 2012.
[25] R. B.Chandar, M. S. Kavitha and K. Seenivasan, "A proficient model for high end security in cloud computing", ICTACT Journal on soft computing, vol. 04, issue: 02 697, January 2014.
[26] D.Chen, H.Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, Vol. , pp. 647-651, 2012.
[27] S.Sharma, A. Chugh, "Survey paper on cloud storage Security", IJIRCCE, Vol. 1, Issue 2, April 2013.
[28] R. P. Padhy, M. R. Patra, S.C. Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST-(IJCSITS), Vol. 1, No. 2, December 2011.
[29] Sh. Ajoudanian and M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing", IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, pp 326-329, June 2012.
[30] A.Ukil, D. Jana, A. D. Sarkar , "A security framework in cloud computing infrastructure", IJNSA, Vol.5, No.5 pp 11-24, September 2013.
[31] M. Ahmed and Md. A. Hossain, "Cloud computing and security issues in the cloud", IJNSA, Vol.6, No.1, January 2014.