The Comprehensive Approach for Data Security in Cloud Computing: A Survey

Nilesh N. Kumbhar Virendrasingh V. Chaudhari Mohit A.Badhe

ABSTRACT
Cloud Computing is becoming next stage platform in the evolution of the internet. It provides the customer an enhanced and efficient way to store data in the cloud with different range of capabilities and applications. The data in the cloud is stored by the service provider. Service provider capable and having a technique to protect their client data to ensure security and to prevent the data from discloser by unauthorized users. This paper, will gives a descriptive knowledge regarding cloud computing privacy and security issue provided by encryption and decryption services. If a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization. This increases the risk factor in terms of security and privacy. This paper helps us on proposes a business model for cloud computing which focused on separating the encryption and decryption service, from the storage service provided by service provider. I means that both encryption and decryption of the data can performed at two distinct places. For studying this proposal are using a business model named as CRM (customer relationship model) for an example. For the evaluation of effective an efficient technique of data storage and retrieval we are providing three clouds separately such as including encryption and decryption services, secondly storage and a CRM application system. In this Research paper, we have tried to access separate encryption and decryption service using RSA algorithm and computing is a paradigm in which information is stored in servers on the internet. That information retrieved by the client as per usage. For this manner, we provide us a solution for data security, confidentiality and privacy based on a concept of separate encryption and decryption service.

Keywords
Cloud computing; encryption and decryption cloud service; service level agreement; availability; reliability; integrity; data privacy protection

1. INTRODUCTION
In recent years, cloud computing one of the new big shining stars in the global technology industry. Previously, before the development of the concept of cloud computing, critical industrial data was stored on the storage media. This data was protected by firewalls to prevent getting disclosure of the confidential data externally and with the help of the organizational regulations its possible to prevent the internal unauthorized access. Whereas, in the cloud computing, storage service provider must provides data security from getting prevented by unauthorized access. Now-a-days, as distributed system and network computing are used on large scale, security is becoming one of the risk factor an important issue in the future. User confidential data is not secured and safe in this fast developing of distributed computing technologies. As there are much more changes of getting data hacked by any unauthorized user. This results in lack of efficiency and privacy. We can overcome such problems by one the technique named as cloud computing. Cloud computing is simply internet based computing. While 'cloud's the combination of work of server and connections. It is easy to access information stored in the cloud. The user doesn't have to give efforts on the sources which are required to their business processes. In short, they don't have to spend their time in the database process instead they can pay attention and concentrate over the business process. Cloud computing collects all the computing resources and software required to work on them. Cloud computing provides an efficient technique to provide an accurate information and proper service to users and enterprises. In this process, user does not have to take care of how to buy servers, resources and software. Depending upon the user need, the user can buy the computing resource through Internet. Cloud Computing is also described as "on-demand computing" because the user can access as per their requirement and demand. Cloud computing can also be defined as it is a new service, which are the collection of technologies and a means of supporting the use of large scale Internet services for the remote applications with good quality of service (QoS) levels [3]. Cloud Computing services are delivered through software as service (SaaS), platform as Service (PaaS), and Infrastructure as Service (IaaS).

1.1 Software as a Service (SaaS)
Software as a Service is nothing but a software distribution model which are made available to customers over a network such as server or Internet . The application of SaaS are hosted by Service Providers. Saas is an interface between cloud applications and customers to offer them on demand network. Even Saas can be provided many times fee based access to the software through web browsers. IT managers and its license holder users required Software as a Service in which they pay as per their uses.

Cloud Service Providers can update their software or cloud applications without user. Because all cloud software resides on servers. Cloud Service Provider has a high administrative authority to control on application and is responsible for update, maintenance and security. The example of SaaS are Google Apps, Cisco's WebEx, Salesforce CRM.

As SaaS is available to the user as and when required. Hence it is also known as "Software on demand". Through SaaS its become possible to access from any location, rapid scalability, high security. SaaS is one of the oldest and mature domain of cloud computing.[11]

Characteristics of SaaS:

- Its easy to work under administration
- It can be globally access
- The software can be updated automatically
- All license holder user will have same version of software

1.2 Platform as a service (PaaS)

Platform as a Service provides a high level environment to design, build, test deploy and update online cloud applications. Paas is a paradigm which mainly deals for delivering operating systems and other services over the internet. In Paas there is no need of downloading or installation of hardware, operating systems over the internet. This saves customers money on purchasing of hardware. PaaS provides solutions for developing as well as deploying applications over the internet such as operating systems and virtualised servers.

Application design, web application Management, storage, security etc are all comes under this category. Today the biggest PaaS providers are Google App Engine, Salesforce's Force.com, the Salesforce owned Heroko and Engine Yard.

PaaS provides infrastructure to customer on which software developers can build new applications, software without investing money for managing hardware and software. This would help user for developing his own solutions. [11]

Characteristics of PaaS:

- No need of downloading and installing operating System
- It saves Customers money
- It mainly deals for delivering operating systems over Internet
- Software can be developed, tested and deployed

1.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service is an equipment which is used to support hardware, software, storage, servers and mainly used for delivering software application environments. It is totally depend on pricing model i.e. pays on as per use basis.

IaaS companies provide off line server, storage and networking hardware as per rent basis and can be access over the Internet. So it becomes easier to get access to run their applications on this hardware anytime without wasting office space. Some of the example of IaaS are Amazon, Microsoft, VMWare and Red Hat.

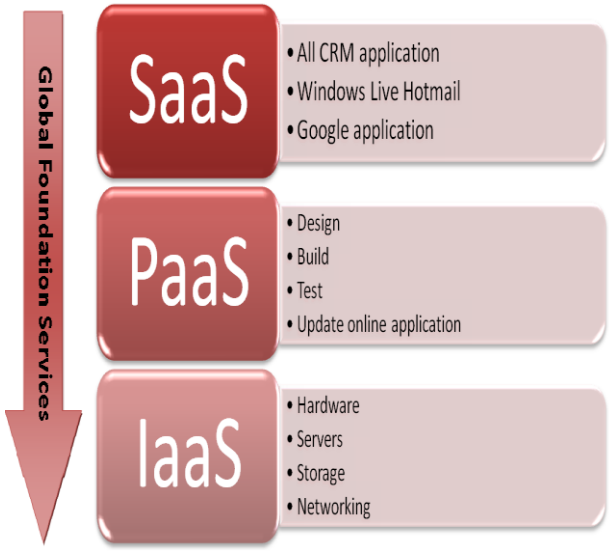

Fig 1: Cloud Environment

Characteristics of IaaS:

- Policy based Services
- Utility computing Services
- Dynamic Scaling
- Internet Connectivity

In the cloud computing data is stored in the storage provided by the service providers. In the cloud computing, the service providers adjust the service content as per the user demand service providers follow distinct policies and methodology for protect user's data and this data is stored in the service contract. For example, a yahoo. Before creating any account, user must read service contract and have to go through all the rule and regulation. The service contract specifies the service scope of privacy protection, regulations on user data collection, sharing and released and suggestions over user responsibilities.

In cloud computing the user demand for the service provided. Consider an example, the user demands for transmission speeds, the different amount of storage, data encryption and other services. The agreement contains information about all these kind of service items, time, and type of quality and performance requirements. These type agreements are usually named as Service Level Agreement (SLA) [6]. By reading all the terms, rules and regulation, after signing the agreement (SLA), the user has understood the contents of the services and accepts me primary and protection policies.

Previously, the data to be stored and the encrypted data is stored on the same storage system. This increases the risk factor of getting disclosure of data by unauthorized user. Because the data is stored at the storage system. Even the key required for decryption is also stored at the same place. So, it become easier for any of the service provider's internal staff (e.g. system administrators and authorized staff) to get that decryption key and easily gets an accesses to catch the internal data so here we are proposing a separate encryption and decryption service in which the data to be stored is placed at different cloud and the encryption and decryption data is placed at another cloud by the service provider. This reduces the chances of getting discloser internally. In this manner, the client working with the purples of storage data will have no access for decrypting the user data. While those working under encryption and decryption service will automatically delete all encrypted or decrypted the user data after transferring the encrypted data to system of data storage service provider. In this manner, a relationship is established to cooperation model between operator and service provided to the user.[11]

2. LITERATURE REVIEW

2.1 Security Concerns in the Cloud

2.1.1 Data Leakage:

Security and privacy is the major factor related to the cloud computing. The cloud computing environment are multi domain environment in which various resources are shared. While sharing hardware and placing data it seems to be risky. As any unauthorized person can easily hacked either accidently or due to malicious attack. Due to this data storage would be a major security violation.

To overcome this, a sensible strategy to ensure data security the encryption technique is used. Data should be encrypted from the start so there is no possibility of data leakage. The user should have control not over the secured data but also over the keys used for decrypting it. From the security point

of view, this one is the best equivalent approach for securing data at your premises. The encryption should be done at proper cloud and not anywhere at an intermediary place before transmission to the cloud

2.1.2 Customer Identification

Customer identification is another factor for ensuring security in cloud computing. The encrypted data can be vulnerable by any customer in your organization if incase your files are pooled. Any one among your organization can easily get access to your personal data as there are no restrictions made between the organization. So due to that any one can delete it or can easily made changes to it. So customer identification is an important aspect in cloud computing. Due to this only authorized user have rights and authority to access data and to modify the contents in it. Without user id verification the system will not allow to undergo any of the request made to allow some transactions. This will ultimately help in data privacy and security.

2.2 Definition of Cloud computing and System model :-

Cloud computing is an internet base computing. Cloud computing is an utility where users are remotely stored the data in the cloud. The US National Institute of Standards and Technology (NIST) define cloud computing as "a model for user convenience, on-demand network access contribute the computing resources (e.g. networks, storage, applications, servers, and services) that can be rapidly implemented with minimal management effort or service provider interference" [2]. The user can easily gather and shared the recourses, software and information is provide as per user need. With the help of cloud computing, as it works on server, it dynamically delivers everything as service over the server or internet. Through this, the user can access the data or share it from any place over the internet. The user will not have to require store the whole information at one work situation.

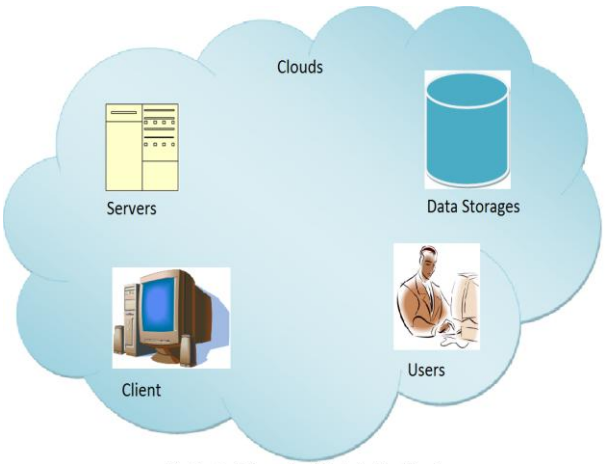

Fig 2: Typical Example of Data in the Cloud

This will help to increase the efficiency, performance, reliability. The user don't have to spend time for gathering knowledge about the software, resource and no need to care about the data where to be stored or services where to be provided. Cloud computing it's self provides the easiest way to provider to developed run application which can fanally increased the flexibility, reliability and can easily grow capacity without depending on the locations of the underlying infrastructure.

Cloud computing is an advanced way of providing service software, infrastructure, platform service to the end-to-end user system and to customers on a demand basis as per their requirement to achieved adequate security the five goals should be achieved namely availability, confidentiality, data integrity, control and audit. Few cloud computing can achieve the five goal together now a days.

In order to achieve security, confidentiality, prevent disclosure of data, here we are representing one cloud for storage service, secondly encryption/decryption cloud for storage service and third one is a CRM cloud service.

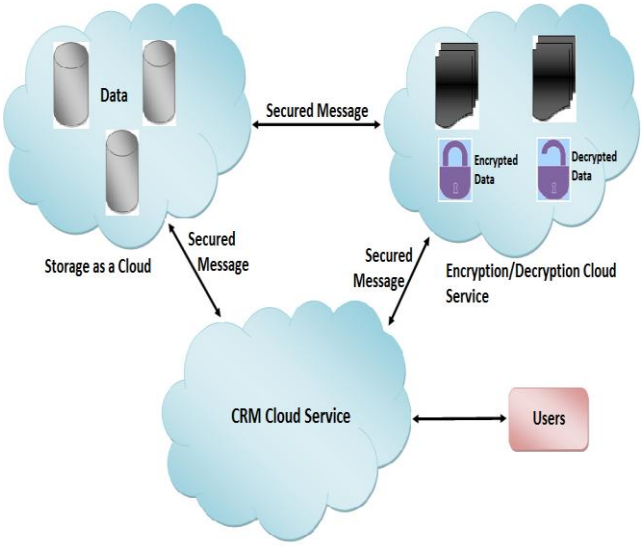

Fig 3: Cloud Data Storage Retrieval

2.3 Deployment model

There are three deployment model cloud computing namely public, private and hybrid[1].

2.3.1 Public cloud

The public cloud is cloud computing in which resources are provisioned dynamically over the interface on self service basis. The physical infrastructure is managed by the service provider.

2.3.2 Private cloud

The private cloud is a cloud computing in which various application or offering on private networks .It consist of application in company host. All the management and security is controlled by their own organization.

2.3.3 Hybrid cloud

Hybrid cloud means as the name suggest that is the combination of two separate cloud combining together or even we can say that it is composition of two or more cloud (public or private) which are bound by proprietary technology which helps us protecting security and maintaining application portability.

3. RSA ALGORITHM

The RSA algorithm was described in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman. The letter RSA is abbreviating form by initials of their surname.

RSA algorithm involves three steps algorithm key generation, encryption and decryption.

In this RSA algorithm, m is known as the modulus, 'E' is known as the encryption exponent or public key exponent and 'D' is known as the decryption exponent or private key exponent.

3.1 Key Generation Algorithm

1. Choose a and b: two distinct prime numbers.

2. Compute m = a b, Where m is used as the modulus for public and private keys.

3. Compute Φ (m) = (a-1)(b-1), Where Φ is totient function.

4. Choose an integer E such that, 1 < E < Φ (m) and common divisor of (E, Φ (m)) = 1.

5. Determine D = 1/E mod Φ (m).

6. All the above values of public key and private key must be kept secret.

3.2 Encryption Algorithm

1. Sender A transmits her public key (m, E) to recipient B for the process of encryption data.

2. Represent the plaintext message as a positive integer n.

3. Computes the cipher $c = n^E \pmod m$.

4. Sends the cipher text c to recipient B.

3.3 Decryption Algorithm

1. Recipient B uses private key (m, D) to compute

$n = c^D \pmod m$.

2. Decrypt the plaintext from the message representative n.

4. CHARACTERISTIC OF CLOUD COMPUTING

The cloud computing is having a ultra large scale give 'cloud' is analogical to the server or Internet. There are more than one million of servers in the Google cloud.

There are example of cloud data storage as AMAZON'S Elastic compute (EC2) and Amazon simple storage service(s3)[4] an Google app engine[5]. Even AMAZON'S, IBM, Microsoft, Yahoo, also have more than thousand of servers. The scale of cloud can extend dynamically to meet increasing requirement.

4.1 Virtualization

It becomes easier for the user to gather information related serviced anywhere. With the help of any kind of terminal, user can get service through cloud computing. It very convenient for user to store and retriever or share data safely through converting and easier way, anytime, anywhere. User can easily create a task that can't be completed in a single workstation. The user completes all kind of work through net service using a mobile phone of another source.

4.2 High Reliability

Cloud computing is the reliable as compared to local computer. Cloud uses multitranscript fault tolerant in order to ensure high reliability of the service.

4.3 On Demand Service

The cloud can be buy according to the user requirement and request for demand. In this service, customer can configured memory, storage, amount of CPU, operating system. The forever can even choose whether to pay for cloud on demand monthly basis. The charges will be the amount you used accordingly.

4.4 User Data privacy in cloud computing

In a cloud computing, the business operation can be leased a single service provider. While the data related to the business operation can be stored on the equipment by the same service provider. But storing the company's data on the equipment the increases risk factor of leaking the information [7]. This raises the disclosure of the data internally. While doing research, of the researches have suggested that the data should be encrypted before storing on service provider equipment [10]. When the data is encrypted and stored in the equipment which help in protection and firewalls are used in order to make surety that decryption keys associated with encrypted user are disclosed to outsiders.

5. CORE CONCEPT OF SECURED IMPLEMENTATION OF CLOUD COMPUTING

This paper proposed a Business model for cloud computing. In this paper we are focusing mainly two provider security, reliability, flexibility to the user while working. So we are studying and separating the storage cloud service and encryption or decryption cloud service. It's means that in this,

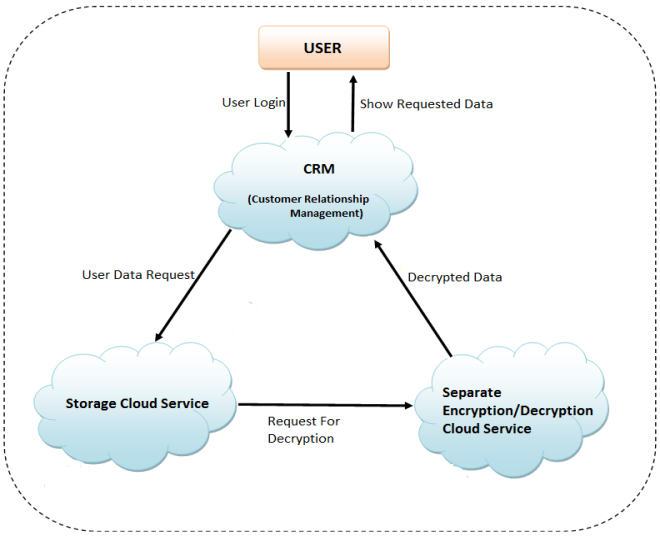

Fig 4: User Data Retrieval Diagram

CRM business model encryption or decryption as service and storage as service are not provided by a single client. The interesting point is that the SaaS provider the dose not stored the unencrypted user data. This ensure security and privacy to the user and reduces discloses of the data. Because when the user requests for encrypt or decrypt of the data to the encryption or decryption as service, and when all this process conversion completes and then handled it CRM application. After this overall process completes at that time, the encryption or decryption service must delete all encrypted and decrypted user data. In addition to this, data storage and decryption of user data works independently. This means that

those working with data storage cloud system will have no access to decrypted user data. In short here we are just dividing and separating the encryption or decryption cloud service from the storage as service.

For enhancing the security and privacy in an organization, the concept of dividing authority is applied in business management. If the user had decided to provided access to some of the operator of an organization to decrypt the data while some of them will work on storage service only. So, it's up to user for deciding the concept of dividing the authority. Consider and example of motor garage system organization. The user will supposed to divide the authority in the billing department as one of the factor named as, accountant operator and another factor is cashier. Due to this, the accountant is responsible for keeping records and making billing of various Motors. While cashier is responsible for making payment to the customer. So, by keeping the two section separately the company prevents from fraud if an accountant make any. Because as accountant has authority of making billing section only and not to provide payments to the customer and the employee. This example of division of authority are design to avoid the operational risk factor.

In cloud computing environment the user ties to uses effective and efficient services provided by the cloud with some of specific function. Consider for an example, salesforce.com's CRM service [8], SAP's ERP services[9], etc. Data generated while using these services is then stored on the storage cloud service. This study related to the business model provides division as per the responsibility for data storages and data encryption or decryption.

To illustrate the concept of separate encryption and decryption consider the example of CRM cloud service, storage and encryption or decryption. In cloud computing, CRM application can be replace with some other services ex.ERP cloud service, account software cloud services etc. In this manner these three cloud can put separately for insuring security.

5.1 Appropriate access to data for data retrieval system

The following figure show the data flow required for preserving privacy and usability when data is encrypted and decrypted in to the cloud. This block diagram helps us to understand and provides us a technique for obtaining security and preventing discloser of confidential data without lost of functionality.

As shown in the figure, these architecture required collaboration of tree cloud namely separate encryption or decryption, storage service and CRM service. Here we have mentioned CRM an example of the new business model. Before working process implement, the user authentication is verified. Unless and until user verification completed this architecture mandate that the user must do valid login registration and contact with the CRM cloud service. For this user's access authorization process, we can use e-commerce or other services which have capabilities of securely verified the user registration, such as reply login verification, one time password etc. Upon authentication of the user and satisfaction of any criteria set out in the access delegation, then only C RM service system accepts any kind of request from the user. After the user logs into the CRM system, is the CRM receive request for client information, it will execute a data Retrieval program.

In the data retrieval system, one the user logging has been successfully verified, the CRM will access the user request for the data retrieval. Every user associated to an organization has its own user ID. This entity helps to know about the user data in the storage cloud system. The CRM will proceed the user request to the storage service system, where user data are stored in to the encrypted form. So these data is not readable by the user. This request is send further to the encryption or decryption service system where data is converted into

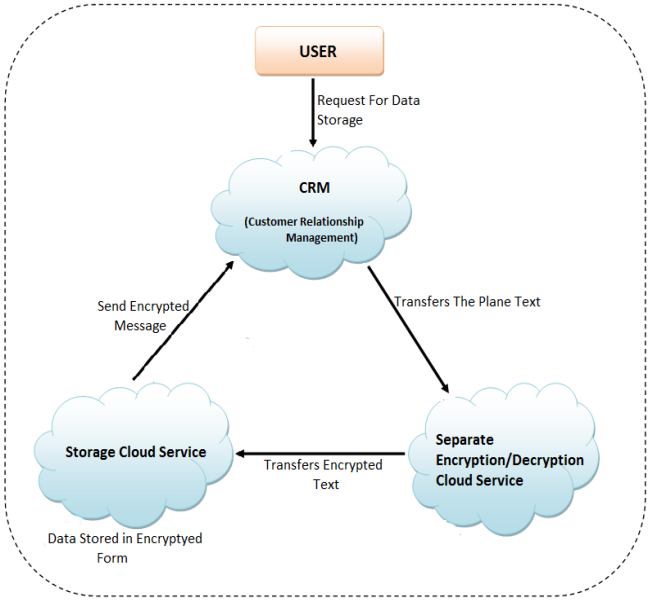

Fig 5: Use Data Storage Diagram

decrypted data but for this conversion, the encryption or decryption cloud service required the user ID to index the user

data decryption key. Storage cloud send request along with the user ID to the encryption or decryption service system.

As the encryption or decryption cloud system can serve multiple user and the encryption or decryption for each user's data requires for different key hence each user unique ID and keys are stored together so the encryption or decryption cloud system required the user ID to index the users data decryption key, which is then used to decrypt the user data. But here, it is against critical to restoring the data to original state. So, any other unauthorized user can tries to hack the data. For that purpose, the CRM can established a secured data transmission channel (e.g. A secured socket layer connection) for the secured transmits the data from encryption or decryption cloud system to the CRM cloud service. This service later on displaced the data to the user in this way, the user received the required information and complete the data retrieval process.

After sending the data to the user, the encryption or decryption cloud system is not having authority to stored the decrypted data and any unencrypted data. It should be deleted after the data send had be send to the user the reason behind this is as decryption key is being stored in the same cloud. In order tp reduced the risk factor a decrypted data should be deleted be deleted to insured security can privacy.

5.2 Appropriate access to data for data storage system

Following fig.illustrates the data storage of the system. The data storage system methodology is exactly opposite to the data retrieval. Here this process is also conducted in three main steps. The user will first of all do login. Unless and until user verification is confirmed the CRM cloud service will not proceeed further. After successfully login the user will firstly send the request for storing data to be stored to the CRM system. Later CRM will forward the user request with user Id to the Separate Encryption and Decryption cloud service provider. Now the data is in decrypted form. So in separate encryption and decryption cloud service provider the decrypted data gets converted into encrypted form. The user Id is very important while encrypting or decrypting the data as this cloud service provider mainly serve multiple user. So that unique user Id is stored with the keys on the same place. So this user Id is later used as an identifier to get the decrypted data key. This key is also stored on the same cloud which will later help while decrypting data whenever user required. After this the Encryption or decryption cloud service provider will sent the encrypted data to the Storage cloud service.

The encryption and decryption cloud service had no authority to store the data either in the encrypted form or decrypted form on the same cloud service. So this cloud automatically deletes the data after sending it to its proper designation. This will increase the data security. After data send to the Storage Cloud Service, here the data is stored in the encrypted form alongwith the user Id. This will help in future to identify and differentiate among the data of multiple users. Finally this Storage Cloud Service Provider will send request to user that the data is stored in the encrypted form.

After sending confirmed request of data stored in the encrypted form to user then only the Separate Encryption and Decryption Cloud Service Provider will delete the data which is stored there as on temporary process for encrypting or decrypting data for completing the data storage process will delete the data. This would help in reduce the risk factor of getting data hacked due to some unauthorized persons. Thus the data storage process is completed successfully.

6. PROPOSED METHODOLOGY OF PGP FRAMEWORK OF ENSURING SECURITY

Cloud computing environment are multidomain environment. Among which different domain can use security, privacy and trust requirements in a different manner. So as far as cloud computing is newly idea developing, security has made commercial Internet possible. Secure Socket Layer (SSL) like this cryptographic protocols are used for securing data and encryption purpose.

In 1991, Philip Zimmermann develop a Pretty Good Privacy(PGP) computer program for ensuring cryptographic privacy and authentication. While in 1998, the Internet Engineering Task Force (IETF) created the open PGP Standard in which the Standards develop helps to run Internet.

Open PGP is a computer program which developers a framework for combining different widely algorithms for ensuring security and privacy into a secure system. This open PGP Standard published by IETF is in form of Request of Comment (RFC). Open PGP combines symmetric and asymmetric algorithms togetherly to formulate a security model. This helps in protecting the data and doesn't affect the performance of the system. In symmetric algorithms, while encrypt and decrypt the data the same key is used. So symmetric algorithm founds to be fast while encryption algorithm used by the U.S. Government where 256 is the size of the key in bits.

Open PGP uses both symmetric encryption like AES for encrypting data and asymmetric encryption like RSA (Rivest-Shamir_Adleman) to encrypting the keys for encrypted data used by AES-256. Asymmetric Encryption is better than symmetric encryption for performing encrypt the data and simplifies key management. But comparatively it is slower than symmetric encryption.

So this combination of Symmetric and asymmetric hybrid approach i.e. fast process of encrypt data symmetric algorithm and comparatively slow process of asymmetric encryption algorithm only for encrypt keys helps to attain high level of granularity and to encrypt data efficiently. Data in the cloud can be protected separately with symmetric key and those keys will be managed through asymmetric key. The user keeps the asymmetric keys in a key ring which one is the single point of access control to the whole system. Open PGP also specifies cipher modes, proper salting.[12]

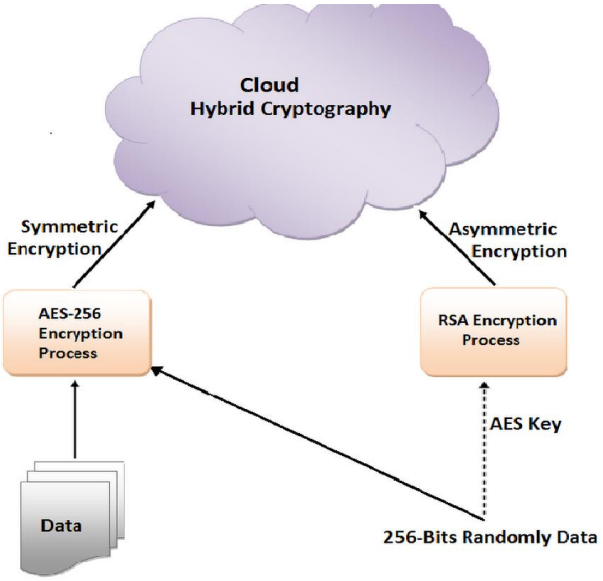

Fig 6: Open PGP artificial encryption to the Cloud

7. CONCLUSION

In this, paper we proposed a comprehensive and effective methodology to data storage and retrieval security issue in cloud computing. Our method achieved the availability, reliability and integrating though out the process. Even any unauthorized user trying to access the confidential data, out method should not allow to access within the cloud. Cloud computing environment includes three type of services mainly Infrastructures, platform and software. Even to access services provided by cloud computing, the user required only a means of accessing the internet For example Smart cart, PDA, etc which help in reducing the cost for the development of cloud computing there must have a high level of trust in the method by which service provider's protect there data.

We study proposes a business model for cloud computing where we are dealing with separation of encryption or decryption cloud system and storage cloud system. The conversion of encryption or decryption of data and storing of data is done at two distinct places provided by two different service provider. After the decrypted data is send to the

client, the encryption or decryption cloud system is not allowed to retain the decrypted data and any unencrypted data must be deleted to prevent the encrypted data and decryption key from being stored in the same system. The service level agreement includes all the rules and regulation for cloud computing rental user, encryption or decryption service provider, storage service provider etc. Even it contains the rights and obligation between the client to achieved high level security. This study will help to reduce the operational risk and avoid the risk of wrongfully disclosure of user data.

8. REFERENCES

[1] Cloud Computing FOR DUMMIES by Judith Hurwitz, RobinBloor, Marcia Kaufman, and Fern Halper. WILEY INDIA EDITION.

[2] Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009, from http://csrc.nist.gov/groups/SNS/cloud-computing

[3] Sales force Customer Relationships Management (CRM) system, http://www.salesforce.com/

[4] Amazon EC2 and S3, Online at http://aws.amazon.com/

[5] Google App Engine, Online at http://code.google.com/appengine/

[6] B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues,"in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[7] N. Hawthorn, "Finding security in the cloud," Computer Fraud & Security, vol. 2009, issue 10, pp. 19-20, October 2009.

[8] Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from http://www.salesforce.com/tw

[9] SAP AG., "SAP services: maximize your success," Retrieved Jan. 2010, From http://www.sap.com/services/index.epx

[10] A. Parakh and S. Kak, "Online data storage using implicit security", Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September 2009

[11] Delivering and implementing a secure infrastructure. Pete boden and mark estberg online services security and compliance Microsoft Corporation.

[12] Nasuni, data storage: www.nasuni.com