

**SECURITY TO CLOUD DATA THROUGH KEY SECURITY MECHANISMS**

A Dissertation Proposal

Submitted

By

**Sapna Devi**

**11309917**

To

**Department of Computer Science and Engineering**

In partial fulfillment of the Requirement for the

Award of the Degree of

**Masters of Technology in Computer Science and Engineering**

Under the guidance of

**Mr. Ravinder Singh**

**(Asst. Professor, LPU)**

**(May 2015)**

# PAC APPROVAL FORM



School of: Computer Science and engineering

## DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Sapna Registration No. 11309917  
Batch: 2013-2015 Roll No. B-51  
Session: 14-15 Parent Section: K2307  
Details of Supervisor: Designation: Asst. Professor  
Name: Ravinder Singh Qualification: M.Tech  
ID: 17750 Research Experience: 1 yr

SPECIALIZATION AREA: Database (pick from list of provided specialization areas by DAA)

- PROPOSED TOPIC: Security to cloud data through Key Security method  
Cloud Computing Issue, research and implementation (Security)
- Big data
  - Data mining algorithms

Ravinder Singh  
Signature of Supervisor

PAC Remarks:  
first topic approved  
Wk 11/29

Signature: [Signature]  
Date: 30/9/17

APPROVAL OF PAC CHAIRPERSON: \_\_\_\_\_ Date: \_\_\_\_\_  
\*Supervisor should finally encircle one topic out of three proposed topics and put up for a approval before Project Approval Committee (PAC)  
\*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.  
\*One copy to be submitted to Supervisor.

## **ABSTRACT**

The purpose of this thesis work is to secure the important data that we share on the public cloud. Cloud provides the services to the organizations like storage, applications and servers. Cloud computing is on demand and pay per use service. The risk and easiness is the key for deciding or declaring on the cloud selection strategy. Selecting right deployment model is a difficult task. This work helps to remove the problem of key escrow and certificate revocation problem of cryptography. In this work the Elgamal method used to solve this problem and for key encryption hashing is used. Before sharing the important data on cloud the data will be encrypted. Then decrypt the encrypted data. First of all create a virtual environment through CloudSim simulator. Then implement Elgamal method for encryption. For decryption user authenticates itself on cloud and key matched with hash code, if keys matched then full decryption is made possible.

## CERTIFICATE

This is to certify that **Sapna Devi** has completed M.Tech dissertation proposal titled “**Security to cloud data through key security mechanism**” under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech in Computer Science and Engineering.

Date\_\_\_\_\_

Signature of Advisor

Name:

UID:

## **ACKNOWLEDGEMENT**

I would like to present my deepest gratitude to **Mr. Ravinder Singh** for his guidance, advice, understanding and supervision throughout the development of this dissertation study. I would like to thank to the **Project Approval Committee Members** for their valuable comments and discussions. I would also like to thank to **Lovely Professional University** for the support on academic studies and letting me involve in this study.

Sapna Devi

Registration No. 11309917

## DECLARATION

I hereby declare that the dissertation proposal entitled, “**Security to cloud data through key security mechanism**” submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: \_\_\_\_\_

Sapna Devi

**Registration No. 11309917**

# TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1.2 Layers of clouds	2
1.3 Deployment models	4
1.3.1 Public model	5
1.3.2 Private model:	5
1.3.3 Community cloud	6
1.3.4 Hybrid model	6
1.4 Security issues in cloud	6
1.5 Cryptographic security mechanisms for cloud computing	7
1.5.1 Symmetric key algorithm:	7
1.5.2 Asymmetric key algorithm	7
1.6 Data mining:	12
CHAPTER 2 REVIEW OF LITERATURE	13
CHAPTER 3 PRESENT WORK	27
3.1 Problem Formulation	27
3.2 Objectives	28
3.3 Methodology	29
3.3.1 Elgamal scheme:	31
3.3.2 Private Key encryption using SHA:	33
3.3.3 Authentication:	33
3.3.4 Performance evaluation:	33
CHAPTER 4 RESULTS AND DISCUSSIONS	34
CHAPTER 5 CONCLUSION AND FUTURE SCOPE	41
CHAPTER 6 REFERENCES	42

## LIST OF FIGURES

Figure 1 : IaaS, PaaS, SaaS models (Gnanasundram & Shrivastva, 2009)	2
Figure 2: characteristics, service models and deployment models of cloud (Gnanasundram & Shrivastva, 2009)	3
Figure 3 : Public model (Gnanasundram & Shrivastva, 2009)	4
Figure 4 : Private model (Gnanasundram & Shrivastva, 2009)	5
Figure 5 : Community cloud (Gnanasundram & Shrivastva, 2009)	5
Figure 6 : The Elgamal cryptosystem (stallings, 2006)	7
Figure 7 : RSA Algorithm (stallings, 2006)	8
Figure 8 : Diffie-Hellman key exchange algorithm (stallings, 2006)	9
Figure 9 : Cryptographic hash function, $h= H (M)$ (stallings, 2006)	10
Figure 10 : comparison of SHA parameters (stallings, 2006)	10
Figure 11 : Architecture of FH-PRE based cloud storage (Xu, Chen, Zou, & Jin, 16 July 2014)	14
Figure 12 : Security mechanism in cloud computing model (Du, Zhang, & Li, 12 July 2013 )	17
Figure 13 : A secure cloud storage system (Chen, Xiang, Yang, & Chow, 2014)	22
Figure 14 : System model (Dongt, Luot, Chen, G., & Lit, Dec 2013)	25
Figure 15 : Flow chart of Existing methodology	28
Figure 16 : Flow chart of proposed methodology	29
Figure 17 : Registration of user on cloud	33
Figure 18 : Login before uploading data	34
Figure 19 : Upload encrypted file on cloud	35
Figure 20 : Match hash code	36
Figure 21 : Encrypted data	36
Figure 22 : Decrypted data	37
Figure 23 : Encryption time graph	38
Figure 24 : Decryption time graph	39



#### **1.1 Cloud computing**

Cloud computing is an Internet based computing. It provides the services to the organizations like storage, applications and servers. Cloud computing is on demand and pay per use service. That means customers pay providers based on usage. The providers who provide services of cloud are Amazon, Google and Microsoft. Cloud is a pool of resources such as hardware, development platforms and services. In hardware that are virtualization and multi core chips. Internet technologies like web services, service oriented architecture etc. System management, like automatic computing and data center automation. These are roots of the cloud computing. These features make cloud computing effective and flexible because the services of cloud computing are accessible at anywhere and anytime. Cloud services need to understand the cloud adoption considerations. The risk and easiness is the key for deciding or declaring on the cloud selection strategy. Selecting right deployment model is a difficult task. Like there are four model, public, private, hybrid and community. If we select public model, then the benefit of choosing this model is that it reduce the cost but the issue of this model is that it is less secure as compare to private cloud. And if we select the private model which is very secure but the cost of this model is very high. Section of cloud service provider is also a consideration of cloud adoption and it is important for cloud. Clients want to know how long and how well the provider has been available to provide services. The clients should also know when they want to transfer from one to another provider is that easy or not. There are so many considerations like financial advantage, application suitability and etc.

#### **1.2 Layers of clouds**

There are three layers of clouds as following:

- i. Infrastructure as a service
- ii. Platform as a service
- iii. Software as a service

- i. **Infrastructure as a service:** As all know that, cloud provides so many services to the users like storage, applications, servers, networks etc and users pay as they use. Infrastructure as a service is that in which users able to run their applications as well as operating system. Users do not manage the infrastructure or control but they can manage operating system. Amazon is the example of the infrastructure as a service.
- ii. **Platform as a service:** As we know that infrastructure provides a infrastructure where the applications runs and that applications created using languages, libraries and tools provided by the cloud owners or cloud service providers. In this service also users does not control over the infrastructure, networks and storage but control the applications. For coding, users use their applications and locate their applications on cloud. Microsoft windows Azure and Google App engine are the example of platform as a service.

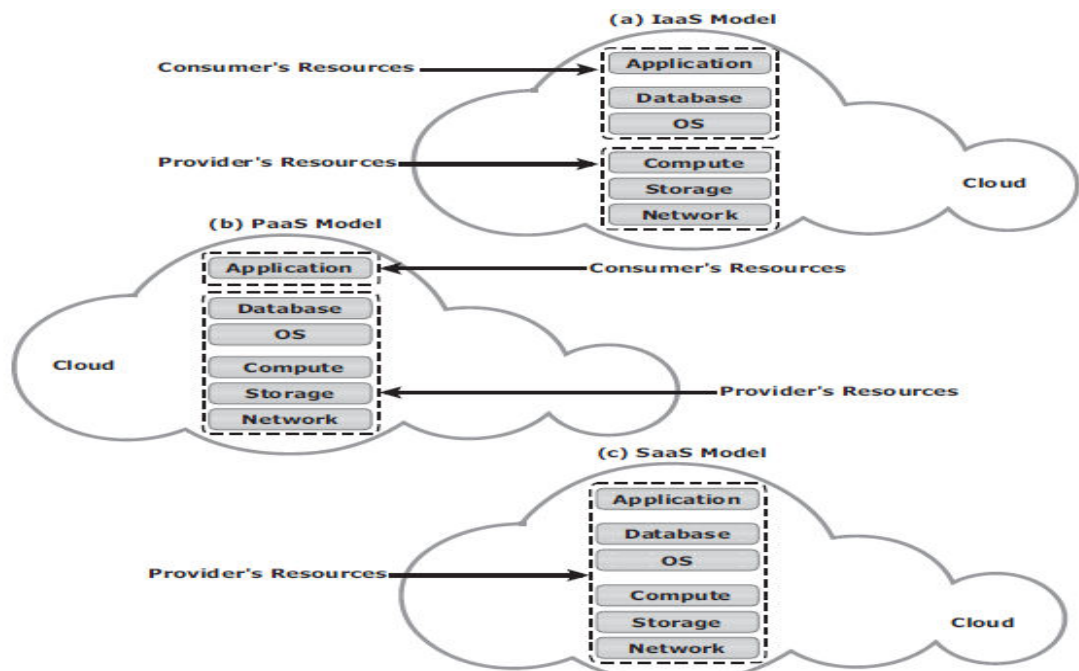
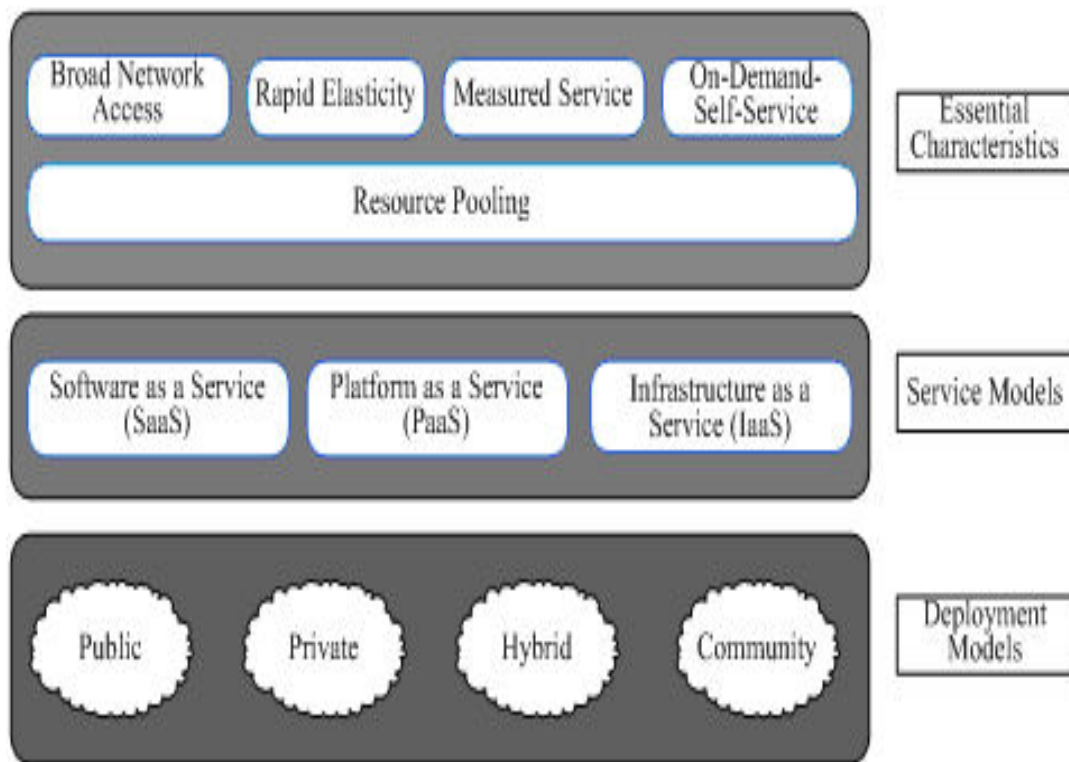


Figure 1 : IaaS, PaaS, SaaS models (Gnanasundram & Shrivastva, 2009)

- iii. **Software as a service:** In software as a service cloud service providers provides the service like e-mail and massaging. The applications can be accessed through various client interfaces like web browser. In this service user have no control over applications, infrastructures, storage, networks and services. The example of software as a service is salesforce.com.

These layers are very important part of the cloud computing. Those provide infrastructure, platform and software services to the clients. Cloud computing provide the place to the clients to run their applications and operating system. The client do not control or manage the infrastructure but it can control the operating system and applications. The capability of the Paas is that on cloud infrastructure the client creates their applications using programming languages, services and tools through cloud providers. Saas provide the capability to the client to use of the applications supported by the providers. In this model the applications like e-mails and instant messaging etc.



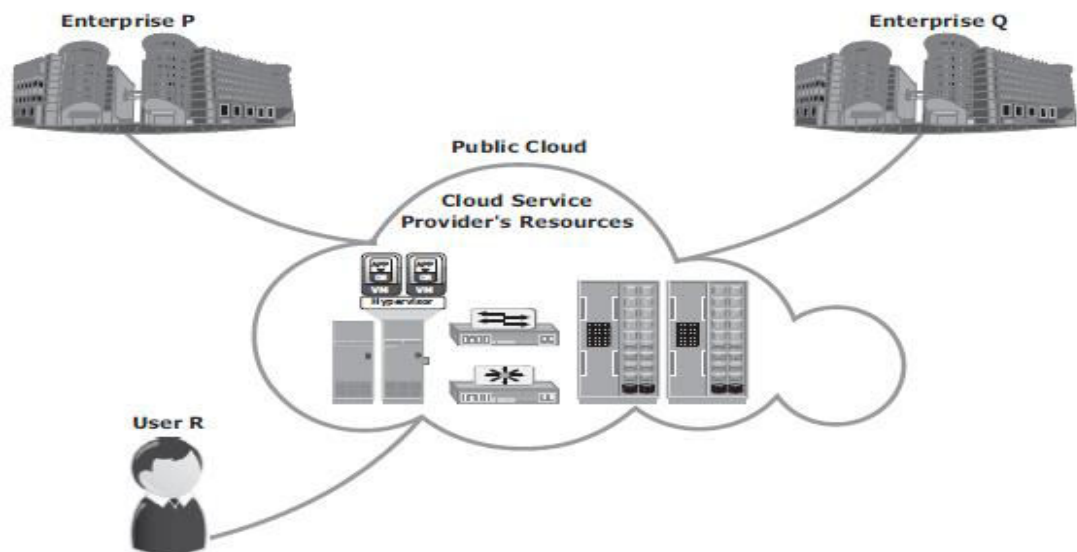
**Figure 2: characteristics, service models and deployment models of cloud (Gnanasundram & Shrivastva, 2009)**

The cloud computing can be classified into public, private and hybrid model. The cloud has many features like virtualization support, elasticity, on-demand self-service etc. Clouds provide software and hardware services to the clients. But with so many benefits there are various security issues in cloud computing.

### 1.3 Deployment models

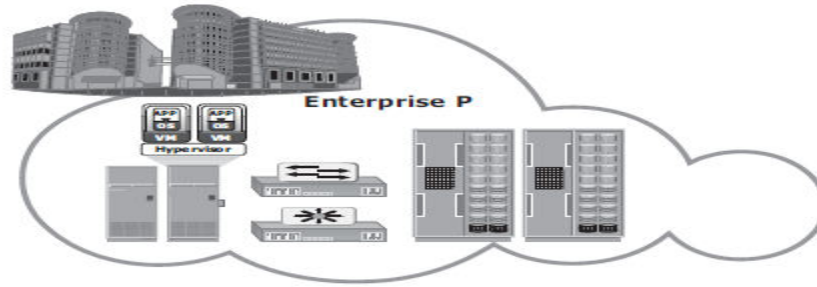
There are four types of deployment models as follows:

**1.3.1 Public model:** In this infrastructure, there is open use of the cloud services by anyone or public. It can be managed, controlled or operated by any business organization, government organizations and colleges. Users use the services that are provided by service providers and users pay as they use. The benefit of the public cloud is that the cost is very low.



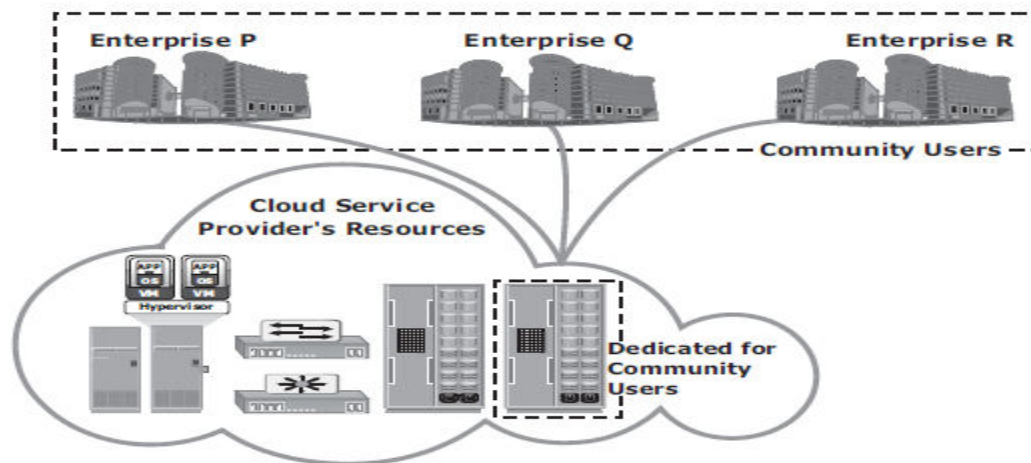
**Figure 3 : Public model (Gnanasundram & Shrivastva, 2009)**

**1.3.2 Private model:** In this model the infrastructure supplies the services to a single organization, which is controlled or managed by the organization or another third party which is connected to the organization. The cost is very high in this cloud as compared to the public model, but this model is more secure.



**Figure 4 : Private model (Gnanasundram & Shrivastva, 2009)**

1.3.3 Community cloud: In this model infrastructure provides the services to a particular community that shared deals like security requirement, compliance etc. this model is managed or controlled by one organization or more organizations that are involved in one community or third party which is connected to the community. In this model the cost is high as compare to public model, but in this model have higher security and privacy.



**Figure 5 : Community cloud (Gnanasundram & Shrivastva, 2009)**

1.3.4 Hybrid model: In this model the infrastructure connected to two or more district cloud infrastructure like public, private or community model. The hybrid model gives the permission to the organization to deal with low critical applications and data to the cloud.

**1.4 Security issues in cloud:** Privacy and security related issues of cloud computing are:

- i. Governance and compliance are the issues in cloud computing.

- ii. Malicious insider is a big threat in the cloud that affects the organization. These are inside the organization or we can say the member of the organization and that has access to the data.
- iii. Accounts hijacking is also a big threat in cloud computing, that occurs because of fraud etc. In which attacker steal important information.
- iv. Hypervisor vulnerabilities and insecure APIs are also an issues in cloud computing. In this unauthorized access, reusable passwords, limited monitoring etc are security threats.

**1.5 Cryptographic security mechanisms for cloud computing:** Cryptographic security mechanism used to protect the data or we can say secure data from unauthorized person. Cryptography used to solve the problem related to the cloud computing such as data security, file system, network traffic, recovery etc. We know that cloud provides many benefits to organizations but there are still many companies which are not ready to accept cloud computing services because of lack of security. There are three kinds of algorithms used as following:

- i. Symmetric key algorithm
- ii. Asymmetric key algorithm
- iii. Hashing

Using these methods we can secure our data on cloud. Many users are not still willing to use cloud services because of the lack of the security. So we can improve the security of the cloud computing through these cryptographic algorithms.

#### **1.5.1 Symmetric key algorithm:**

This method used for encryption and in this method same key use to encrypt and decrypt. The good point of this method is that the speed of this method is high and computing power is less. There are some symmetric key algorithms like:

- i. Data encryption standard (DES)
- ii. Triple DES
- iii. Advanced encryption standard (AES)

### 1.5.2 Asymmetric key algorithm:

This method is used to encrypt and decrypt the data with different keys that are public and private. Public key used to encrypt and private key used to decrypt the data. In cloud computing these methods are used to bring forth the encryption key. The common methods for cloud are as following:

- i. **Elgamal encryption algorithm:** The Elgamal encryption algorithm is an asymmetric key encryption based on the Diffie-Hellman key exchange method used in cryptography. Also this algorithm is public key algorithm based on discrete logarithms. For public key encryption, this algorithm provides an alternative to RSA. The advantage of Elgamal encryption algorithm is that, if there is same plaintext then it gives different cipher text each time it is encrypted. The limitation of this algorithm is that the cipher text is double or twice than the plaintext or original data. The Elgamal algorithm has of three parts that are, key generation, the encryption algorithm and decryption algorithm.

Global Public Elements	
$q$	prime number
$\alpha$	$\alpha < q$ and $\alpha$ a primitive root of $q$

Key Generation by Alice	
Select private $X_A$	$X_A < q - 1$
Calculate $Y_A$	$Y_A = \alpha^{X_A} \text{ mod } q$
Public key	$PU = [q, \alpha, Y_A]$
Private key	$X_A$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer $k$	$k < q$
Calculate $K$	$K = (Y_A)^k \text{ mod } q$
Calculate $C_1$	$C_1 = \alpha^k \text{ mod } q$
Calculate $C_2$	$C_2 = KM \text{ mod } q$
Ciphertext:	$(C_1, C_2)$

Decryption by Alice with Alice's Private Key	
Ciphertext:	$(C_1, C_2)$
Calculate $K$	$K = (C_1)^{X_A} \text{ mod } q$
Plaintext:	$M = (C_2 K^{-1}) \text{ mod } q$

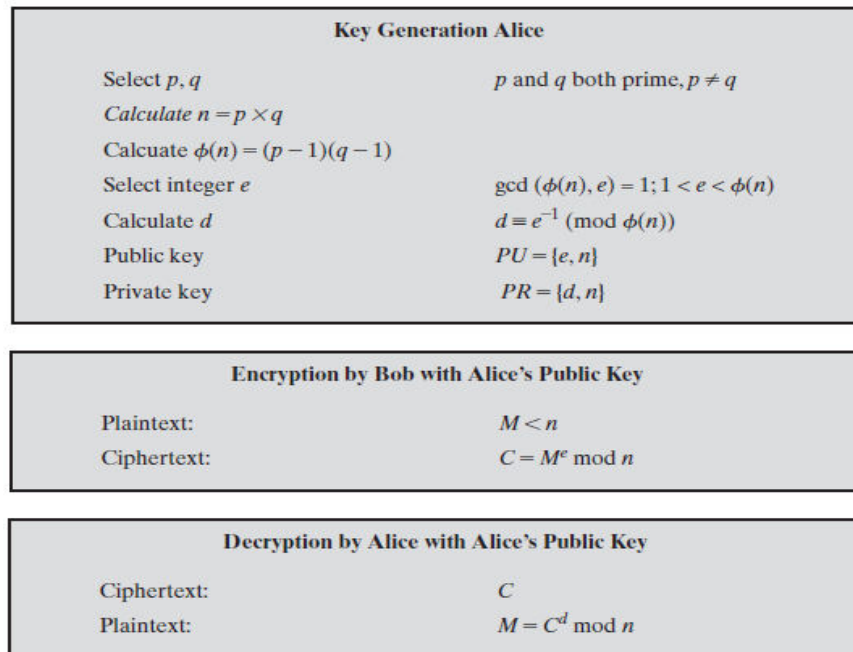
Figure 6 : The Elgamal cryptosystem (stallings, 2006)

Elgamal cryptosystem is used in hybrid cryptosystem that is the message itself is encrypted using a symmetric algorithm and then Elgamal encrypt the key. The security of Elgamal algorithm depends upon group and also any padding scheme used on the messages.

- ii. **RSA algorithm:** It is general purpose scheme to public key encryption used to encrypt and decrypt the data. It is also used for secure data transmission. RSA is a block cipher in which plaintext and cipher texts are integers. In this algorithm users use two different keys that are public key and private key. Public key is known to all users which encrypts the data that we want to share on cloud. Private Key should be kept secret, which is use to decrypt the data. This algorithm provides the assurance of confidentiality, integrity and authenticity of data storage. The encryption and decryption in RSA is

$$C = M^e \text{ mod } n$$

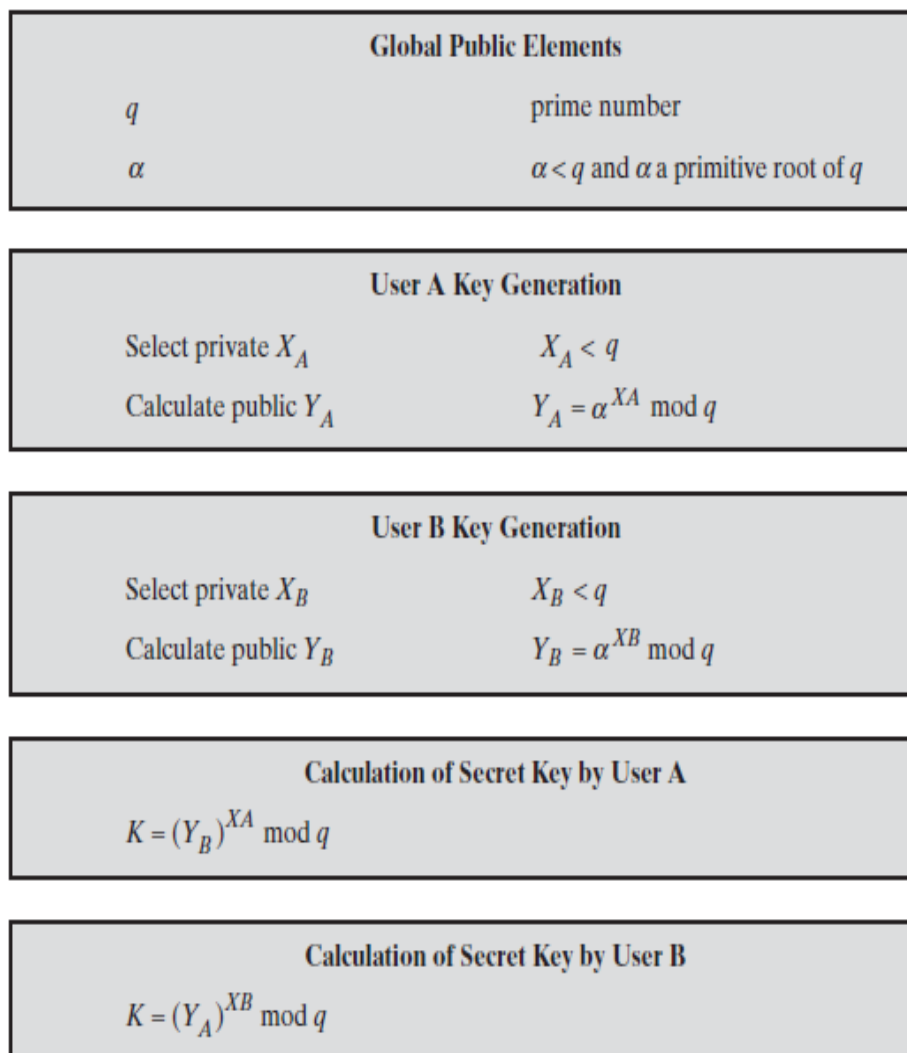
$$M = C^d \text{ mod } n = (M^e)^d \text{ mod } n = M^{ed} \text{ mod } n$$



**Figure 7 : RSA Algorithm (stallings, 2006)**

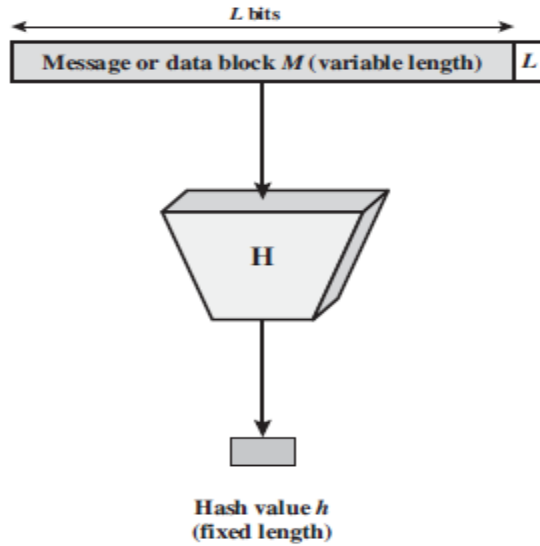


iii. **Diffie Hellman algorithm:** The main aim of this algorithm is that two users can exchange key securely that used for encryption of message. Diffie Hellman depends upon the computing discrete algorithm.



**Figure 8 : Diffie-Hellman key exchange algorithm (stallings, 2006)**

**1.5.3 Hashing:** Hash function calculates the variable length message into a fixed length hash value. Hash methods have checksums, check digits, fingerprints, randomization function, ciphers etc. the main purpose of hash function is data integrity.



**Figure 9 : Cryptographic hash function,  $h= H (M)$  (stallings, 2006)**

The applications of cryptographic hash function are message authentication, digital signatures etc.

Secure hash algorithm (SHA): SHA is most widely used hash function, which is developed by national institute of standard and technology (NIST) and published as a federal information processing standard (FIPS).

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
<b>Message Digest Size</b>	160	224	256	384	512
<b>Message Size</b>	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
<b>Block Size</b>	512	512	512	1024	1024
<b>Word Size</b>	32	32	32	64	64
<b>Number of Steps</b>	80	64	64	80	80

**Figure 10 : comparison of SHA parameters (stallings, 2006)**

**1.6 Data mining:** data mining is a process in which meaningful or useful information fetched from the large data. Tasks of the data mining are

- i. Extracts data from the group of protocols
- ii. Unusual records
- iii. And dependencies

Cloud computing is used in the data mining for security purpose. Because attackers or hackers hacks the important data from any organization's large scale data using data mining algorithm. So using cloud computing user can encrypt that large data and share on cloud so that attacker cannot hack the important data easily.

### REVIEW OF LITERATURE

---

#### **A An Na Kang, Lard Brollie, Jong Hyug Park, Young-Sik Jeong(2013)**

Cloud computing is most widely used service that provides a variety of computing resources, from servers and storage to enterprise applications like email, security and backup all delivered over the internet. Cloud computing also manages the user's IT resources as well as enterprises the IT resources in an effective manner. With the development of internet cloud computing effectively manage and use the number of data. While using cloud computing so many threats have occurred, since they will raise to security threats to enterprise information. Because of the strength enterprise widely use the cloud computing. Authentication and access authority management is the basic idea to be considered to protect information leakage, service abstraction etc. Core factors that cloud computing use to protect data are management of keys and powerful encoding (Kang, Barolli, Park, & Jeong, September 2014).

#### **Raghul Mukundan, Sanjay Madria, Mark Linderman(2014)**

In this paper cloud service provider (CSP) is boon for data owners, to outsourcing their data and reduce their burden of local data storage and maintenance. Cloud service provider replicates the data to increase the data availability, reliability and durability. And clients or data owners have to pay to store data to CSPs storage place. The client needs to be persuade that CSP is storing data copies upon. Since the data are copies it is difficult to know that the cloud really stores the multiple copies of data because the CPS can cheat the client by storing only one copy of replicated data. So the data owner is not to only check the data is complete or perfect but also to recover the data if there is any damage of data is occur. To maintain the data confidentiality stops the cloud service provider from cheating by maintaining fewer copies than paid for data, in this paper they propose the Dynamic Multi Replica Provable Data Possession scheme (DMR-PDP). This scheme also provides service of dynamic operations such that insertion, deletion and modification on replicated data over the cloud server. As the replicated data is stored at different locations, so the data loss will not occur at

the same time on all the replicas. If there is any loss of data, using DMR-PDP scheme the data owner can detect that loss and can recover the data from other perfect stored replicas. To validate the integrity of data stored on remote server the Provable Data Possession technique is used. To ensure data integrity, in this paper they use data encryption is the best technique. This idea also supports the basic file versioning system. In this system the data owner can review the changes done to the file and also retrieve the older version of the file. (Mukundan, Madria, & Linderman, June 2014)

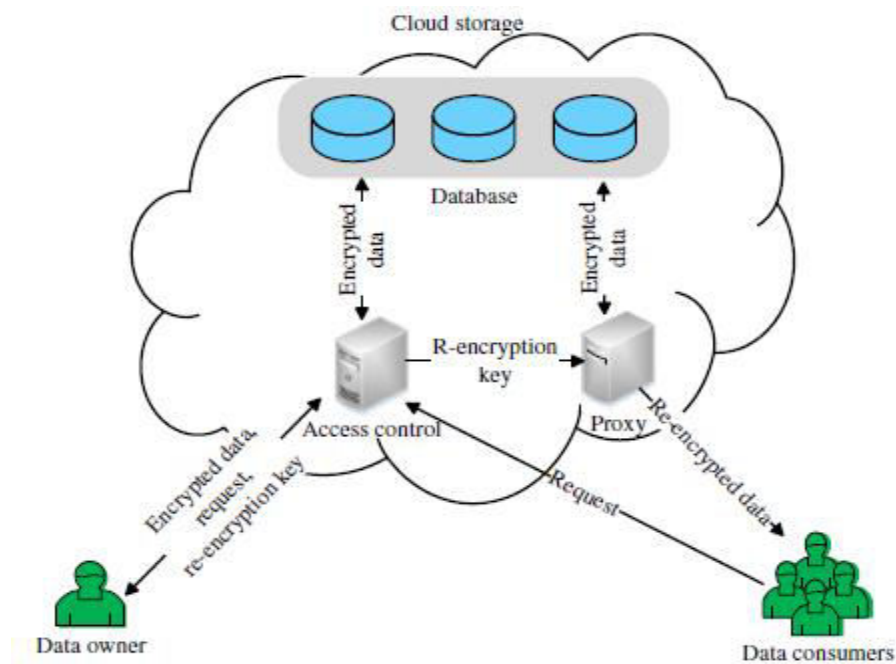
**Kuen-Min Lee, Wei-Guang Teng, Jin-Neng Wu, Kuo-Ming Huang, Yao-Hsing Ko, Ting-Wei Hou(2013)**

The recent underlying assumptions of cloud computing has brought deployment of operating systems onto a large scale computer network. It should be noted that, as in cloud computing, there are number of nodes with different functions, so operating system's deployment is necessary onto its different parts. For the above, time-consuming and bandwidth-intensive are the conventional techniques of using unicast deployment, when a massive cloud of OS is being distributed onto thousands nodes. Since previous techniques for OS deployment doesn't worked efficiently and flexibly, so new multicast deployment approach is nominated to improve the efficiency and influence of existing settings of the unicast deployment. This new approach provides the support of reliable multicast protocol, a heterogeneous infrastructure and hypervisor surroundings. When implementing, using Cent OS and Ubuntu, their new deployment approach on several tens of nodes, is only a practical application for calculating the feasibility of new approach. The preboot execution environment (EXE) is adapted to OS installation and configuration. Experimental studies have calculated that the required time for whole distribution process and the network bandwidth consumption are less in comparable to previous unicast deployment approach. Finally, new nominated approach has been considered more useful for cloud surroundings over that previous one. (Lee, Teng, Wu, Huang, Ko, & Hou, December 2013)

**Peng Xu, Hongwu Chen, Deqing Zou, Hai Jin,(2014)**

Cloud is a widely used computing model that provides proxy and outsourced storage services. A data owner stores their data in cloud, that data is accessible without any authorization and by un-trusted cloud. So the confidentiality of data owner's data that store

on cloud is big issue. The idea to solve this problem is fine grained and heterogeneous proxy (FH-PRE) re-encryption methods are used. The fine grained sharing of data owner's cipher text proposed a type based PRE system that is ITHJ08 system. It is also identity based encryption system (IBE). Ithj08 system to build a secure cloud storage system may be not acceptable. In FH-PRE system both data owners and consumers belong to different cryptographic primitives that are IBE and Elgamal. A data owner and consumer own a pair of IBE and Elgamal public and private keys respectively. To generate a new cipher text an IBE cipher text of data owner can be re-encrypted by a proxy and this new cipher text can be decrypted by the Elgamal private keys of consumers. So without more registrations data consumers can share cloud data. A novel function allows data owners to update the old type of his cloud data. The Pre has more efficient re-encryption and decryption processes. (Xu, Chen, Zou, & Jin, 16 July 2014)



**Figure 11 : Architecture of FH-PRE based cloud storage (Xu, Chen, Zou, & Jin, 16 July 2014)**

**Yuxiang Wang, Junzhou Luo, Aibo Song, Fang Dong(2014)**

To save time and cost of computation cloud support online aggregation by taking nearly result. There are two disadvantages that control the performance of online aggregation

(OLA) that are large amount of unwanted cost and replicative computation cost. To remove this disadvantage, in this paper they use this sharing strategy in cloud that is based on MapReduce method. MapReduce method works on two functions that are Map and Reduce. Map function maps or measure the large amount of data and Reduce function divided that data in separate levels and then make a summary of useful data. The online aggregation is based on sampling to make aggregation query by an approx guess to the result. So the method that we discussed above based on cloud is construct for large amount of data analysis, from this user measures the query performance and save money. (Wang, Luo, Song, & Dong, January 2014)

**Yating Wang, Ing-Ray Chen, Ding-Chua Wang (2014)**

In this paper the name mobile cloud computing comes from the combination of mobile devices and cloud computing. In this paper, they provide the perception or awareness applications and challenges to move from mobile computing to mobile cloud computing and also define their solutions. In this wireless world mobiles can connect to cloud at any place and time. Virtual machines and various operating system runs on mobile. In this paper they talk about and make an appearance of mobile cloud computing applications. (Wang, Chen, & Wang, A survey of mobile cloud computing applications: Perspectives and Challenges, 14 october 2014)

**Xing Ge, Bin Yao, Minyi Guo, Changliang Xu, Jingyu Zhou, Chentao Wu, Goungtau Xue (2014)**

In this research work LSShare used to solve the problem of multiple query optimizations, that is a big problem in database. This research is done in cloud computing environment, that runs large amount of data analysis jobs in schedule and these queries are very difficult and wasting time but still sense, share common components, which is very difficult task. In this work, they make a share system through Lineage signature method. In this work, they also use map reduce structure or bodywork to investigate the queries. The Map reduce structure implement on hadoop. (Ge, et al., 01 June 2014)

**Madarapu Naresh Kumar, P Sujatha, Vamshi Kalva, Rohit Nagori, Anil Kumar Katukojwala, Mukesh Kumar (2012)**

There are number of attacks every day on cloud service provider which specifically attacks the network which is called as DDoS attack. This attack in cloud is due to the DDoS attack, the service provider who is utilizing cloud will acquire a disabling bill by utilizing intensely flexible ability to unknowingly serve a lot of unpleasant movement to keep up quality of service. So to stop that, they reduce DDoS. Cloud computing is turning into one of the quickest developing field in the data innovation. Cloud computing allow to scale servers in size and accessibility to give direction to more number of clients. In addition cloud managment model are charged focused around a pay for every use of the cloud's server and system asset. In cloud computing where base is imparted by possibly a large number of clients, DDoS thrash can possibly have much more well known effect than against single resident architecture. With this model, a traditional DDoS assault on server and system asset is changed in a specific Economic Denial of Service (eDDoS) assaults. In this work, they propose a more arrangement. Where requesting client's validity will be checked through his previous reputation, as well as he has to go through a puzzle solving procedure to prove validity. (Naresh Kumar, Sujatha, Kalva, Nagori, Katukojwala, & Kumar, 2012)

**Yung Joon Jung, Donghyouk Lim, Yong Bon Koo, Eun-Ser Lee, Hoon Choi (2013)**

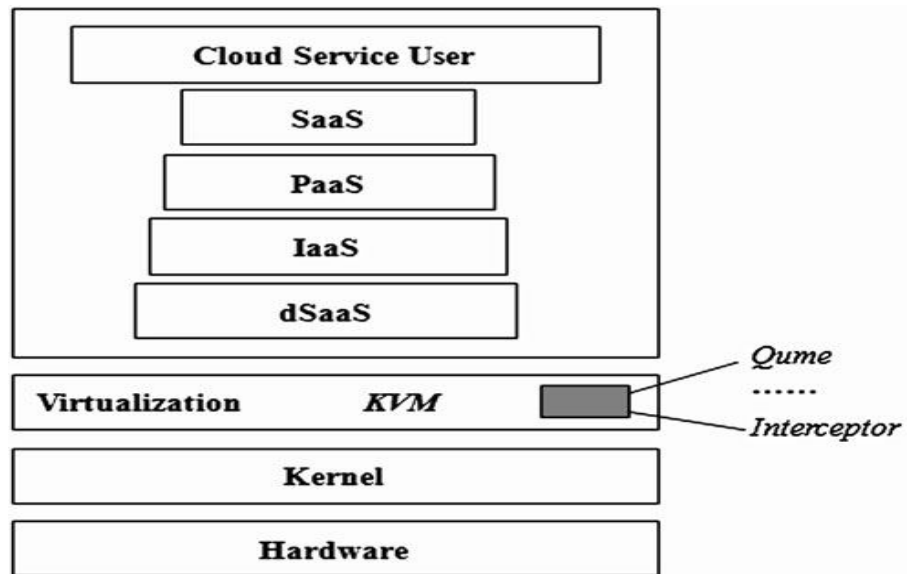
There are many types of Linux-based mobile computing systems. There is need of real time characteristics to improve the performance of mobile computing, so they measure the real time responsiveness. So for this time interval measured through many tools. But these tools do not the perfect measurement that they want. One tool measure only delay, one measures periodic interrupt and these tools works only on X86 operating system. So to overcome this incomplete measurement of real time, they use embedded Linux real time responsiveness measurement method (ELRM). This method shows instinctive and exact or we can say correct measurement results. (Jung, Lim, Koo, Lee, & Choi, 6 July 2013)

**Ye Du, Ruhui Zhang, Meihong Li (2013)**

Now a days security of cloud computing is main concern. In this work virtualization is used for security purpose of cloud computing that make safe the cloud. In which virtual machine monitor (VMM) scans the infected data. So firstly it collects behavior of the process and



calculates the distance to check whether malevolent behavior occurs, this is calculated through intrusion detection method. (Du, Zhang, & Li, 12 July 2013 )



**Figure 12 : Security mechanism in cloud computing model (Du, Zhang, & Li, 12 July 2013 )**

**Seung-Hyun Seo, Mohamed nabeel, Xiaoyu Ding, Elisa Bertino (2013)**

In this paper to share the important data in public cloud securely mediated certificateless encryption scheme is used. This method is used to solve the problem of escrow in identity based and revocation in public key. In this paper they create public cloud environment and then implement above scheme for data in cloud. The key that are created saved to the cloud. For decryption user authenticate itself on cloud. Then cloud decrypts the some part of encrypted data. After that it decrypts the all data through private key. (Seo, Nabeel, Ding, & Bertino, 5 August 2013)

**Jaekyung Lee, Junggab Son, Rasheed Hussain, Heekuck Oh (2014)**

In this paper with the development of cloud computing has caused effects of various services combining with it. There are many important functions of cloud computing like, cloud service provider, service quality assurance and cloud media and content protection is one of the important combining service of cloud. So in this proposed work virtualization is used to provide the secure and efficient media services through the cloud and the advantage of this is

that is to prevent internal attacks and use cloud resources securely. Media cloud is cloud based service which suits the media environment that is storage, sharing and management of high capacity video and it reduce the implementation and maintenance costs. In this paper contents protect without using encryption. The framework has virtualized media service (VMS) module placed inside cloud. For the protection and authentication of transmission, Kerberos and DCAS methods can be used. (Lee, Son, Hussain, & Oh, Jan 2014)

**Daniel Kouril, Tomas Rebok, Tomas Jirsik, Jakub Cegan, Martin Drasar, Martin Vizvary, Jan Vykopal(2014)**

In this proposed work, shows how to inspect the nature of the attacks, so that one can find the way of detection and understands the effect of attacks. In this paper testbed used to mimic the attacks that allows to study a wide range of security scheme. In this there are real world arrangements in which full control over activities performed by the mimic infrastructure. The design of the scheme is based on the IaaS cloud in which various attacks and evaluates the effects on real infrastructure. The study of the attacks in is their simulation. Simulating an attack makes it possible to understand the behavior of the attack on services in the infrastructure, that how the attack is flowing, what kind of attack is this and what are the effects of attack. To estimate the size of the attack, verified the simulation of the DDoS attacks of different types. Before simulating the attacks, it is important to know whether it is possible to build an artificial environment which is like real world environment, then it provide control and isolation over activities performed in it. The scheme design for, and built upon an existing cloud infrastructure, where different virtual appliances can be easily deployed, which provides additional layer for configuration. It allows testbed to transparently observe network communication among individual network nodes and their performance (Kouril, Rebok, Cegan, Drasar, Vizvary, & Vykopal, 2014).

**Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang and Shuo Chen (2014)**

Internet plays an important role in our information infrastructure, e-business and e-pay side. Internet security problems still a challenge with security concerns like spam, worms and phishing attacks. The underground economics based on internet scam and frauds are also flourishing. Intrusion detection firewalls and anti viruses are now widely used to protect systems from attacks. Botnets is a distributed attack that generates a distributed denial of services (DDoS) attack on target hosts. To solve this kind of problems, a collaborative

network security management is used with Unified Threat Management (UTM) and traffic probers. A distributed security network with centralized center leverages communication protocol used in UTMs collaborative modules and connects them to exchange network events and security rules. Security functions for the UTM are retrofitted to share security rules. In this proposed work they design and implementation of a cloud based security centre for network security forensic analysis. To keep collected traffic data they use cloud storage and to find malicious attack, they process it with cloud computing policy. As a practical example, phishing attack forensic analysis is presented and the required computing and storage resources are evaluated based on real trace data. The cloud based security center can command each collaborative UTM and prober to collect events and raw traffic and to generate new security rules, send them back for analysis. These new security rules are enforced by collaborative UTM and the feedback events of such rules are returned to the security center. The collaborative network security management system can identify and address new distributed attacks more quickly through this type of close loop. (Chen, Han, Cao, Jiang, & Chen, Feb 2013)

**Marc Sanchez-Artigas, Universitat Rovira I Virgili(2013)**

As cloud computing become famous day by day, because of pay per use service model, falling store costs etc. When data is stored on cloud there is indication for security and security. So solution of this problem is to encrypt the data before sharing on cloud, but only encryption is not enough to secure the data. The data access patterns can disclose important information using a little bit of knowledge. Brute force attack is also the example of hacking the information or broking the pattern without any knowledge. Attackers keep their eye, when data accesses on cloud and try to conclude the data of encrypted data. To solve this problem Oblivious RAM (ORAM) is proposed in this work. For clients there are still problems like limited storage and bandwidth. To hide the access pattern another scheme is private information retrieval (PIR). In PIR scheme there are some limitations to hide the access pattern. ORAM is different from PIR scheme to hides the pattern. ORAM is used to authorize the access privacy in mobile cloud computing. In mobile phones there is limited store capacity. To solve this problem, mobile systems transfers there data to cloud into the cloud. When we want to download some data from the internet or any site of the internet and

the size of the data is large, means if downloading 50gb data and 10 gb data taking half day to download, cost is also running on the basis of time, then 50gb will take very much time and cost to download. So to solve this problem optimization is proposed in this work, that will minimize the size of the data or compress the size or volume of the data, then easily can download or share on cloud with less time and costs. (Artigas & Virgili, Nov 2013)

**CHEN Danwei, CHEN Linling, FAN Xiaowei, HE Liwen, PAN Su, Hu Ruoxiang (2014)**

A personal health record (PHR) authorizes a patient to create, control and manage their personal health data through web in one place. Every patient can be enable their personal health records and can share with many users like doctors, healthcare providers, family members and friends. Mainly this paper ensures flexible and scalable access control to PHR data in cloud computing in various occupancies. Attribute based encryption (ABE) used in patient health record (PHR) system, when file encryption is applied in one- to- many manner. To achieve a form of attribute based encryption (ABE) that authorizes the delegation of access rights for encrypted electronic health records, there are so many works have been conducted using attribute based encryption (ABE) to achieve fine grained access control to cloud based data. In this proposed work the scheme is divided into public and private two different security domains or parts. In public domain we use multiple and hierarchical authority attribute based encryption, each authority have different attribute sets and user private key distribution, so it minimize the workload of single authority and achieves flexible access control. (Chen, Chen, Fan, He, Pan, & Hu, 2014)

**YANG Pan, GUI Xiaolin, AN Jian, YAO Jing, LIN Jiancai, TIAN Feng (2014)**

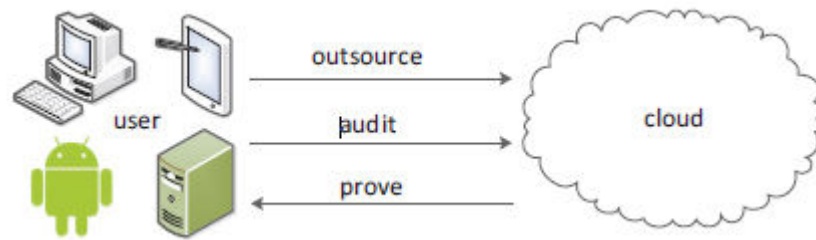
Cloud computing is most famous network that provides pay per use or on demand services that provides resources like servers, storage and networks. The authorized users borrow data from the data owners from their clouds and access or use the data, and pay as per use of data. There is storage cloud in which the data is maintained, and cloud data owners get some relief from the maintenance of the data. On the other hand, there are the challenging privacy disclosure threats. The data that we store on cloud is the property of the cloud service providers (CPS), the latter can easily stole the user's data. Encryption can protect the data

privacy. Before sharing data on cloud, the data encrypted from original form to cipher form. So the privacy is safe from the disclosure and authorized user can access the data to cipher text and decrypt it to get the original data, which have the key. There are many services that can't be executed successfully, since the CPS is not able to operate the encrypted data. To solve this problem they used some improved schemes of encryption. Cloud is the good place to store or share the data. An data owner can share the data which stored in cloud, where others can analyze the data. In this process the problem of privacy disclosure comes as well. K anonymity protects the privacy from identity disclosure. But it is true for some information; the privacy is not confirmed as the intruder confirms the subject of record based on background knowledge. Many researchers focus on transferring the original data into other format to remain the important data of the cloud while hiding the privacy, like data masking and data obfuscation. The perturbation is the method of the data masking. In this method, they add some noise to disguise the true data. Users get true result without disclosing the DO's privacy, when they doing statistics on perturbed data. (Pan, Xiaolin, Jian, Jing, Jiancai, & T., Aug. 2014)

**Fei Chen, Tao Xiang, Yuanyuan Yang, Sharman S.M. Chow (2013)**

In this work, they configure the relation between secure cloud storage and secure network coding, which look not related to each other firstly. One is deal with the problem of checking that when the data is stored on cloud remain the same that share on the cloud and other focuses on protecting network code from being stolen while the transferring or routing. The solutions of the problem are proof of irretrievability and provable data possession (PDP). On the other side the latter area has been studied for so many years. If we connect them together, it will be helpful for both the areas. In this paper they made a relation or connection in these two areas. The previous protocol for the secure network coding can be transformed for securing cloud storage. These days secure cloud storage designed in a ad hoc and from that some protocols successful. There are two operations present in these protocols, user and cloud service provider (CSP). User shares the data to the cloud that promises to store all the data on the cloud. The user confirms the probity by connecting with cloud using secure cloud storage protocols. The reason of checking the probity is that the user's data could be improved without any acknowledgement of the user, because of some reasons, like loss of

data because of poor management of CSP, hardware or software failure, intentional discard and etc. These occurrences may be hidden by cloud without secure cloud storage protocol.



**Figure 13 : A secure cloud storage system (Chen, Xiang, Yang, & Chow, 2014)**

Secure network coding is also a problem that is proposed in this paper, network coding is a routing or transferring operation which is not like old store and forward method. A router is a network sends encoded data packets, here encoding is a function of received data packets. In this work, other work is that they extend the protocol to support a more advanced functionality of third party public auditing. Then protocols used to evaluate the performance. (Chen, Xiang, Yang, & Chow, 2014)

**Bao Rong Chang, Hsiu-Fen Tsai, Yun-Che Tsai and Yi-Sheng Chang(2013)**

These days the service oriented hosts like ERPs system, databases, websites, AP servers, file servers etc in enterprises have faced the critical problem of unexpected down or system failure that will cause data error, loss of very important data and etc. once upon a time a real host is difficult to transfer everything to another host timely and then start its task as usual, so data cannot be updated. In this work, they propose the cloud services to solve these problems like data loss and system termination. There is a virtual machine (VM) used to solve the problem of failover. To stop the service oriented hosts from the problem like fraud, intrusion and malicious attacks. The benefits of the cloud services are, decreases the cost of hardware, centralized monitoring, quick management, dynamic optimization, well organized backup and faster speed. This paper proposed in cloud enterprise resource planning in virtual environment and mobile users that can easily get access the in cloud services through wired and wireless network. To achieve identity verification, safe sign in and attendance audit, access control authentication has kept into virtual machine. Also virtual machine is used to

form the firewall to separate the virtual internal network from internet where this framework secured the open ERP and related database. (Chang, Tsai, Tsai, & Chang, Feb 2014 )

**Byong John Han, In-Yong Jung, Ki-Hyun Kim, Do-kwang Lee, Seungmin Rho and Chang-sung Jeong(2013)**

Collaboration organization becomes more typical and increases day by day. Through networks, it needs more collaboration platform. Today's soft-wares for content collaborations support web applications for business based on old software system that is enterprise content management (ECM) or repository software. Those content collaboration system reduces the network traffic for collaboration content transfer. Traditional collaboration policies were evolved to provide private, isolated and unique scheme used for specific organization. Collaboration in organization with different system needs additional costs and makes security problems. This disadvantage makes collaboration between separated organizations harder. In this work, they propose a new active content collaboration platform (ACCP) which support automated event driven service known as active work on cloud. Active content collaboration platform also provides content centric collaborative work space called active content repository (ACR). This is called active content because it stores all content, which managed automatically through collaboration policy. In this work there are three features. First is that is provides virtual collaborative content work space, with which collaboration users can connect with each others. Other feature is that it used to execute unique task flow with automated management system on event driven property for content spaces. The last feature is that it provides modularized architecture to support flexibility and quality of services through cloud infrastructure system. With this architecture the manager can build various multimedia processing functions for each organization. for the evolution, they show the result of implementing the collaborative medical application on their system where computation intensive application is used for MRI. (Han, Jung, Kim, Lee, Rho, & Jeong, march 2013)

**Aziz Mohaisen, Huy Tran, Abhishek Chandra and Yongdae Kim (2014)**

Cloud computing is a new model, that solves the restrictions of the computing through calculating the new technological and economical features such as elasticity and pay per use

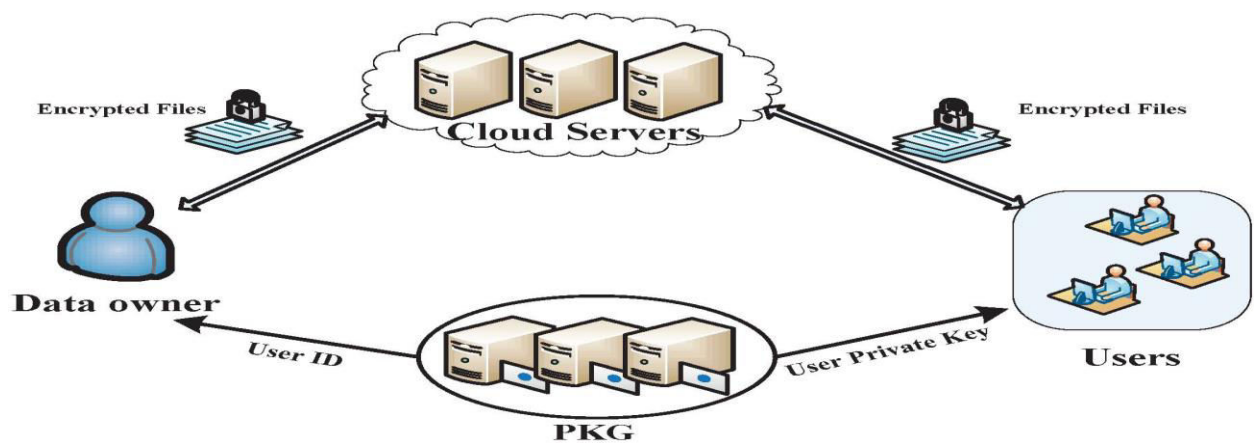
service, which free users from long responsibilities and duty towards service providers. With so many advantages or benefits, also there are so many challenges that hamper its usability. These difficulties like require architectures to support various application and security and data privacy protection. In this paper they propose new computing model known as social cloud. The proposed modal is the interesting part of the ordinary cloud and increased aspects of other distributed computing model name as grid computing model, where group of users draw a pool of resources perform their computational task in place of their social contact. The proposed model has the same features to the normal grid computing model as well as the proposed model is different from the ordinary grid computing. Most important part is that, the proposed work utilizes the trust revealed in social network as a guarantee for the good behavior of the other workers in system. So the most important parts of this work is a social bootstrapping graph that used for perform tasks in social cloud. Through this they investigate the prospective of the social cloud computing modal, then they apply standard model instead of older such as grid computing model. Also investigate the prospective of the proposed model using simulation set-up and real word social graphs with social characteristics that show different and possibly counter trust model. (Mohaisen, Tran, Chandra, & Kim, Dec 2014)

**Xin Dongt, Jiadi Yut, Yuan Luot, Yingying Chen, Guangtao Xueta, and Minglu Lit (2013)**

Cloud computing is the most appearing technologies, in which cloud service provider provides efficient data, storage and services to the users. As all know that cloud computing is more beneficial than other data computing to store data without any formality and without any care of management of the infrastructure. But with so many benefits there are some problems of security challenges. So a data service provider needs some high security and confidentiality to share the data to the cloud. Even old cryptographic algorithms are not enough to achieve security. In this work, they work on the security and privacy protection of data to share on cloud under various systems and security models. They focus only on security and user's privacy without taking a complexity on the user decrypted stage. To solve this problem, they either exploit key policy attribute based attribute based encryption (KP-ABE) for secure access control or employ hierarchical identity-based encryption (HIBE) for



data security. The KE-ABE based process still disclose users access attributes to the cloud ant that cannot fully protects the user’s privacy and also not fully collaborate resistant. The other side, HIBE tells too many keys and cannot manage efficiently. For effective and privacy preserving data storing services there should be some needs like data owner should be able to know that user is authenticated or not, privacy should be protected and accessing users can access the data using connected terminals with low computing ability such as smart phone and tablets. In this work, to solve these problems, they propose an flexible privacy protecting method that is PE2. CP-ABE connects it with the technique of identity based encryption (IBE). For full privacy protecting and collaborate secure, PE2 tell about public key which is fix with the private key. To minimize the key management problem PE2 compared with HIBE based method. The users have the same public key to encrypt the data while sharing the data on cloud and all users have their own private or secret key to get the original data from the cloud. Each private key have their own attributes, when the attributes of private key matched with the public key, then the user can get the original data.



**Figure 14 : System model (Dongt, Luot, Chen, G., & Lit, Dec 2013)**

PE2 make sure fine-grained data access control and security against collaboration of users with the cloud. PE2 keep the privacy protection because it does not release the attributes of the users. In further one can perform the privacy protecting and effective cloud data storing services in a real cloud service providers (CSP) platform. (Dongt, Luot, Chen, G., & Lit, Dec 2013)

#### **3.1 Problem Formulation**

In this proposed work, implement Elgamal scheme for security of data. In this scheme create a virtual environment using CloudSim simulator. In earlier work another scheme was implemented for the security of data that share in public cloud. User authentication and partial decryption of data will be done from cloud. Evaluation of the performance parameters will be done in this work. The work is that we want to share the important data to the public cloud securely, but when we store the data to the public cloud there is problem of key escrow. So to solve that problem this scheme implemented.

In this work the important data share on the public cloud securely. This made possible by the combination of the Elgamal algorithm and hashing function algorithm. In this work before sharing important data to the cloud the data encrypted through Elgamal scheme using public key. The private key is also encrypted through SHA algorithm and convert key into hash codes. After encryption the data is saved to the cloud. For the decryption the user authenticates itself and matches the local key to the hash code. When they matched successfully, then the decryption made possible and it means that our data is safe on cloud, there is not any changes occurs. Data that stored on cloud will be safe.

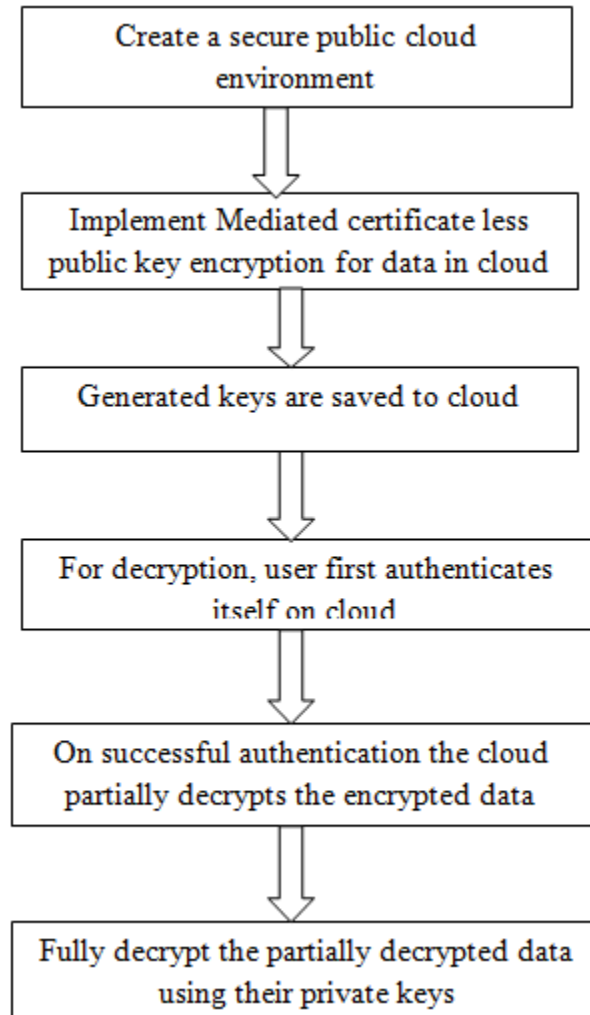
### **3.2 Objectives**

The main aim of this research topic is to implement Elgamal algorithm for security of data, and creating a virtual cloud environment using CloudSim simulator. There is user authentication and partial decryption of data done from cloud. In this we also calculate the performance using encryption decryption time parameters. In this research work these objectives are very helpful for the security of the important data that store on the public cloud environment. The main task we have to do in this are:

- i. Creating a virtual environment using CloudSim simulator
- ii. Implement Elgamal algorithm scheme for encryption using public key
- iii. User authentication and decryption of data using private key on which SHA algorithm is used
- iv. Evaluate performance parameters.

### 3.3 Methodology

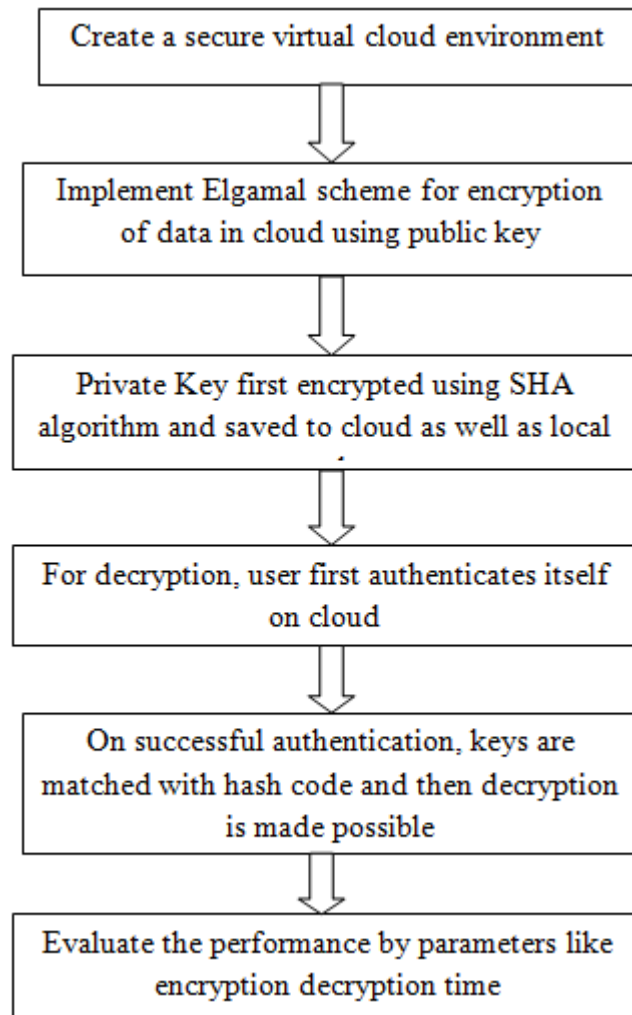
In existing system a mediated certificateless scheme without pair for securely sharing important data in public cloud and this scheme use to solve the problem of key escrow and revocation.



**Figure 15 : Flow chart of Existing methodology**

In the proposed system there are some changes. Firstly we have to create virtual cloud environment to protect data with policy based management and valid solutions. Then before storing data on cloud we encrypt that and then implement Elgamal algorithm for encryption.

In our work the private key that we are using to decrypt is also encrypted using SHA algorithm.



**Figure 16 : Flow chart of proposed methodology**

With the storage of data cloud also generate the keys. So in our work data owner encrypts the important information with the help of that key based on access policies and then store that information to the cloud, after that user need to decrypt that data. For decryption the client have to authenticate itself on cloud. After that keys are matched using SHA algorithm and decryption made possible. In the last step we evaluate the performance using parameters like

encryption decryption time. Using this scheme we solve the problem of key escrow in identity based encryption and the revocation problem in public key cryptography.

**3.3.1 Elgamal scheme:** Elgamal is a asymmetric key encryption based on Deffie Hallman key exchange algorithm. When the important data is stored on cloud, then the data is encrypted through public key using Elgamal algorithm. The encrypted data decrypted using private key. The advantage of Elgamal encryption algorithm is that, if there is same plaintext then it gives different cipher text each time it is encrypted. The limitation of this algorithm is that the cipher text is double or twice than the plaintext or original data. The Elgamal algorithm has of three parts that are, key generation, the encryption algorithm and decryption algorithm. When two users want to exchange key, then some elements that used in Elgamal scheme are

- i. Global public elements
- ii. Key generation by one user
- iii. Encryption
- iv. Decryption

**Elgamal Algorithm:**

1. Tom generates a random integer  $k$ .
2. Tom generates a one-time key  $K$  using Aana's public-key components  $Y_A, q,$  and  $k$ .
3. Tom encrypts  $k$  using the public-key component  $\alpha$ , yielding  $C_1$ .  $C_1$  provides sufficient information for Aana to recover  $K$ .
4. Tom encrypts the plaintext message  $M$  using  $K$ .
5. Aana recovers  $K$  from  $C_1$  using her private key.
6. Aana uses  $K^{-1}$  to recover the plaintext message from  $C_2$ .

The encryption process requires two modular exponentiations (extra time).

**Key generation:** Receiver A must do the following:

- 1- Generate a large random prime number (p)
- 2- Choose a generator number (a)
- 3- Choose an integer (x) less than (p-2), as secret number.
- 4- Compute (d) where

$$d = a^x \text{ mod } p$$

- 5- Determine the public key (p, a, d) and the private key (x)

**Generator number:** How to test (a) generator or not:

**Assumptions:**  $\phi$ = Euler number; p=prime number;

f and q= factors of  $\phi$  (Euler number)

- 1- (a) must be between 1 and p-1
- 2- Find  $\phi = p-1$
- 3- Find the all factors of  $\phi$  {f1, f2... fn} - {1}
- 4- Find {q1, q2,.....,qn} where  $q_i = f_i$

For the redundant factors  $q_i = f_i^{\text{freq}}$

- 5- (a) generator number if and only if

$$w_i = a^{\phi/q_i} \text{ mod } p \neq 1, \text{ for all } q_i$$

**Encryption:** Sender B must do the following :

- 1- Obtain the public key (p, a, d) from the receiver A.
- 2- Choose an integer k such that:  $1 < k < p-2$
- 3- Represent the plaintext as an integer m where  $0 < m < p-1$

- 4- Compute (y) :  $y = a^k \text{ mod } p$
- 5- Compute (z) :  $z = (d^k * m) \text{ mod } p$
- 6- Find the cipher text (C):  $C = (y, z)$
- 7- The sender B sends C to The receiver A

**Decryption:** Receiver A must do the following:

- 1- Obtain the cipher text (C) from B .
- 2- Compute (r):  $r = y^{p-1-x} \text{ mod } p$
- 3- Recover the plaintext as follows:

$$m = (r * z) \text{ mod } p$$

**3.3.2 Private Key encryption using SHA:** Data is encrypted using Elgamal scheme before share on cloud because of security purpose through public key. For decryption private key is used, but while we store the data on cloud using public key the private key is also encrypted using hash function algorithm that is SHA and then stored on cloud. At the decryption time the data is the key at local and at cloud should be matched, if the hash code is matched with the local, means there is no change in the data or data is safe that stored on cloud and authentication is successful.

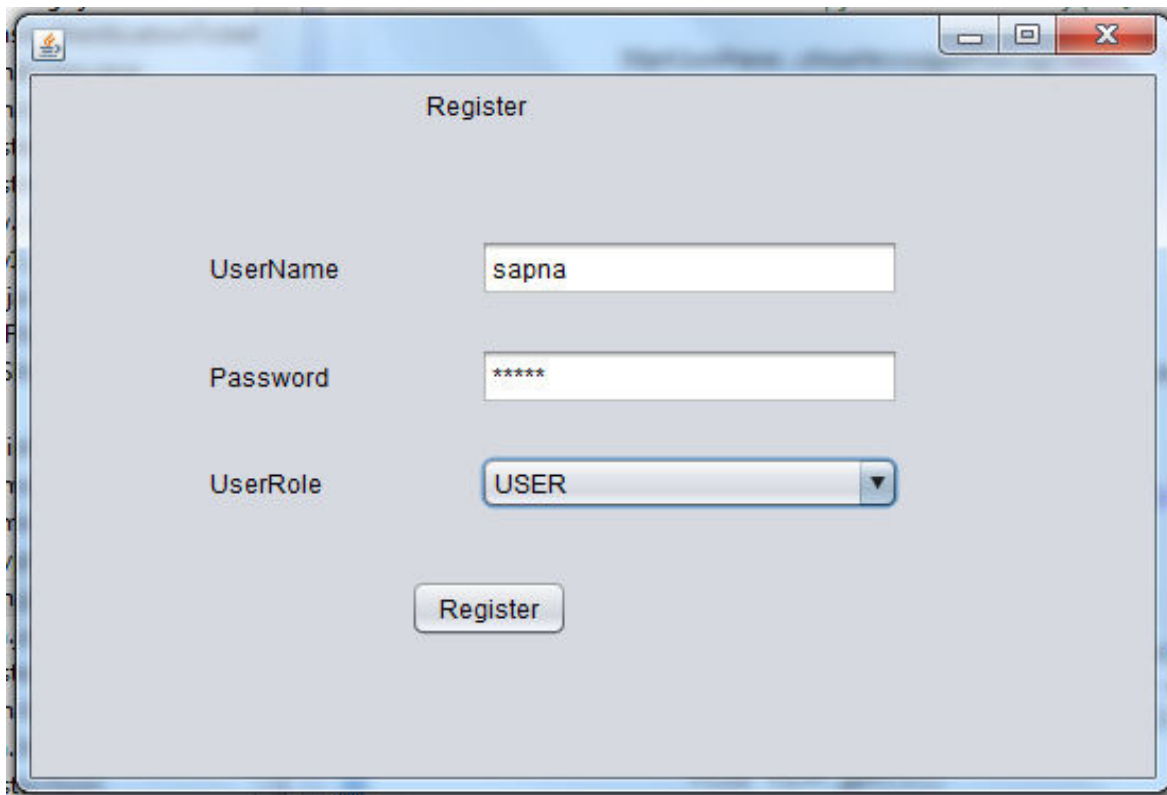
**3.3.3 Authentication:** when encrypted data is decrypted, then user needs to be authenticated. Authentication means, when user going to share data on cloud, he should be register on the cloud with user name and password. Then can login to cloud and upload his data on cloud. So when data is decrypted then that authenticated user can only decrypt the data using private key. Before using that key should be matched with local key. If the hash code is matched, then the data is secured, there is no changes occur in data that is stored on cloud and data is decrypted successfully.

**3.3.4 Performance evaluation:** In this work, the parameters also evaluate. There are two parameters, encryption time and decryption time parameter. In which time of encryption of the data is calculated and the time at which the decryption takes place is calculated.



**i. Registration**

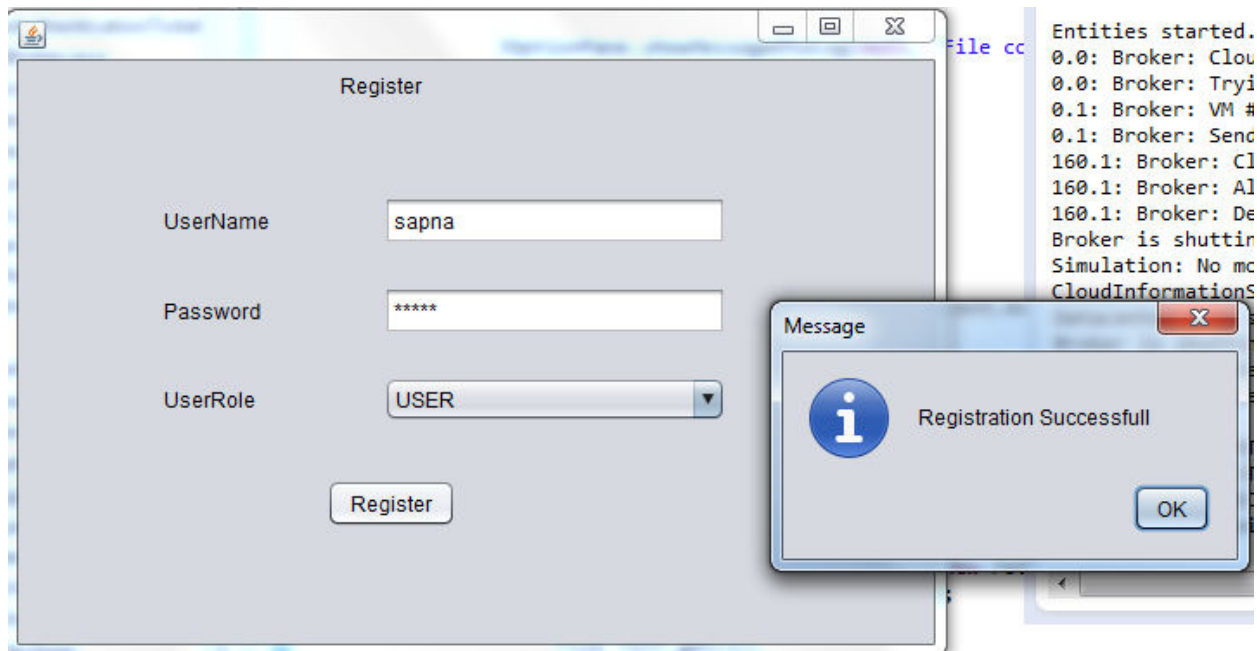
To create virtual cloud environment CloudSim simulator is used. This work is done to secure the data that share on cloud. Before uploading the file on cloud, user has to register himself on cloud with name and password and authenticate himself.



The image shows a screenshot of a 'Register' dialog box. The dialog has a title bar with standard window controls (minimize, maximize, close). The main area is titled 'Register' and contains three input fields: 'UserName' with the text 'sapna', 'Password' with six asterisks, and 'UserRole' with a dropdown menu showing 'USER'. A 'Register' button is located at the bottom center.

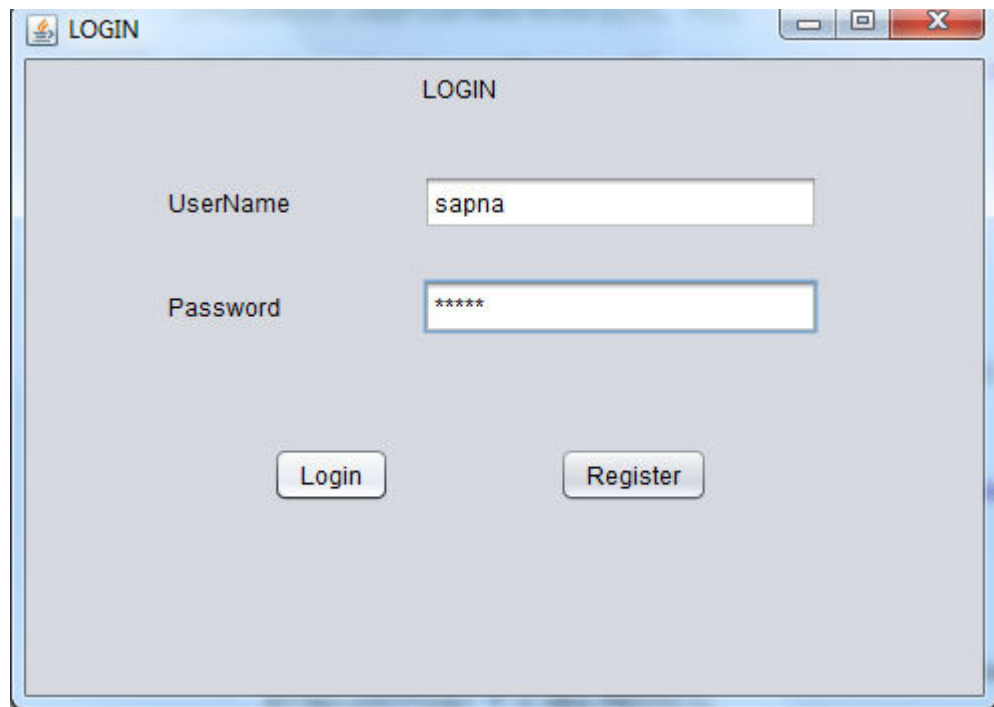
**Figure 17 : Registration of user on cloud**

After entering username and password user click on register and registration will be successful. The user cannot register with same name and password on cloud.



## ii. Login

After registration, user can login into cloud with the name and password and can upload data to the cloud.

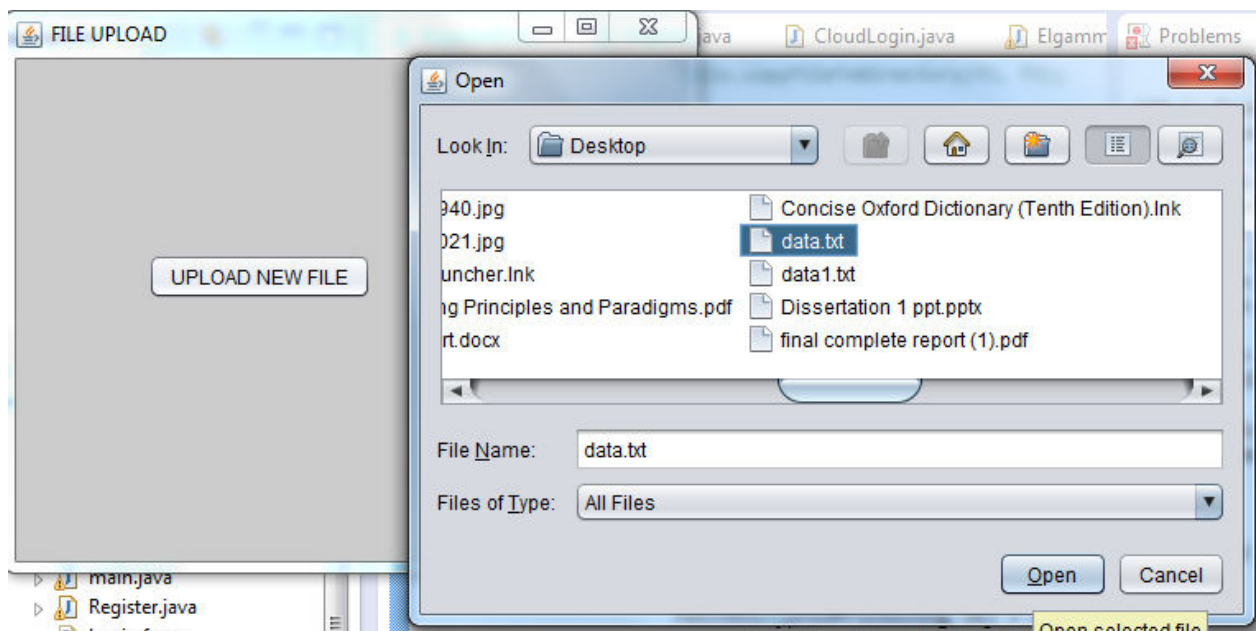


**Figure 18 : Login before uploading data**

After successfully login the ticket has been granted and user can upload data on cloud.

### iii. Upload

The ticket has been granted and user can upload a file on cloud. Click on upload, select a file or data that user want to share on cloud and then click on ok.

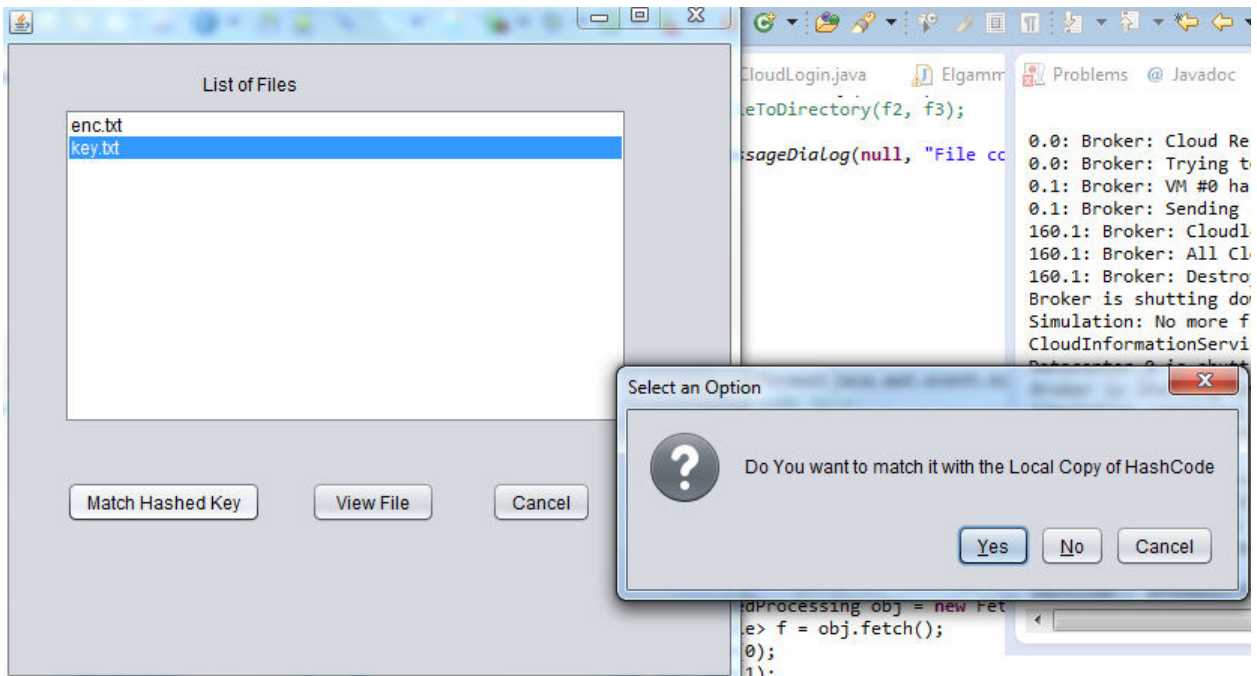


**Figure 19 : Upload encrypted file on cloud**

On the click of the upload file, a window will appear in which we enter the name of the encrypted data and then enter the name of the hashed key, then the file will successfully uploaded on cloud.

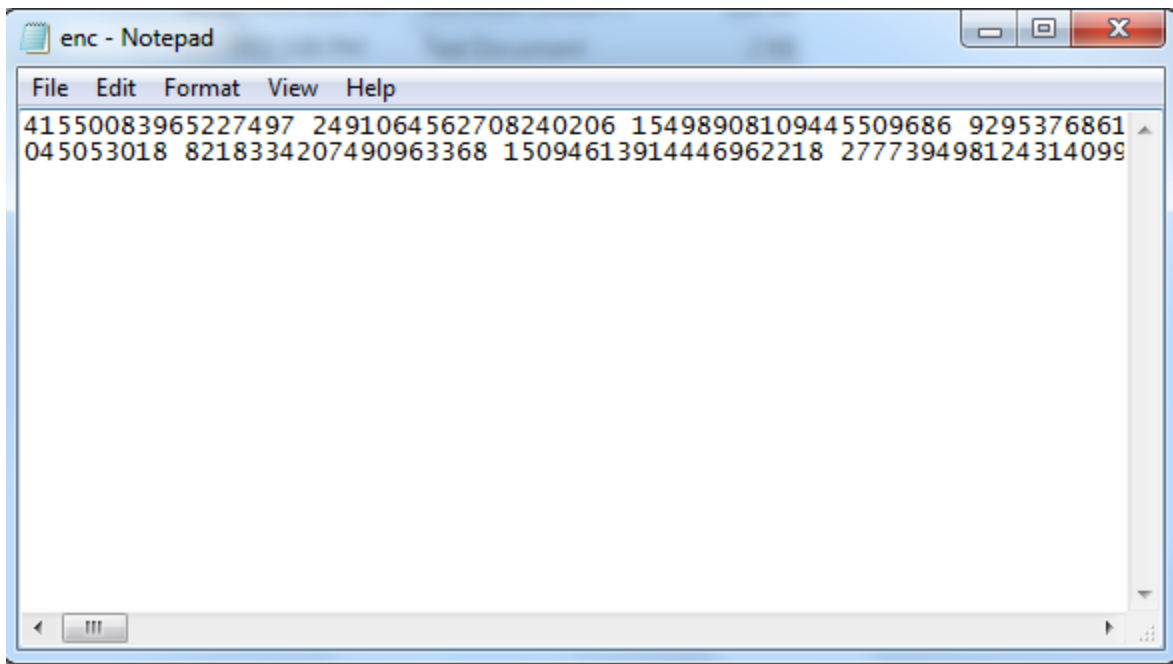
### iv. Encryption and Decryption

If user wants to view the data or decrypt the data then click on view. The window will appear. In which, key should be match with hash code. If key matched then user can decrypt the data successfully.



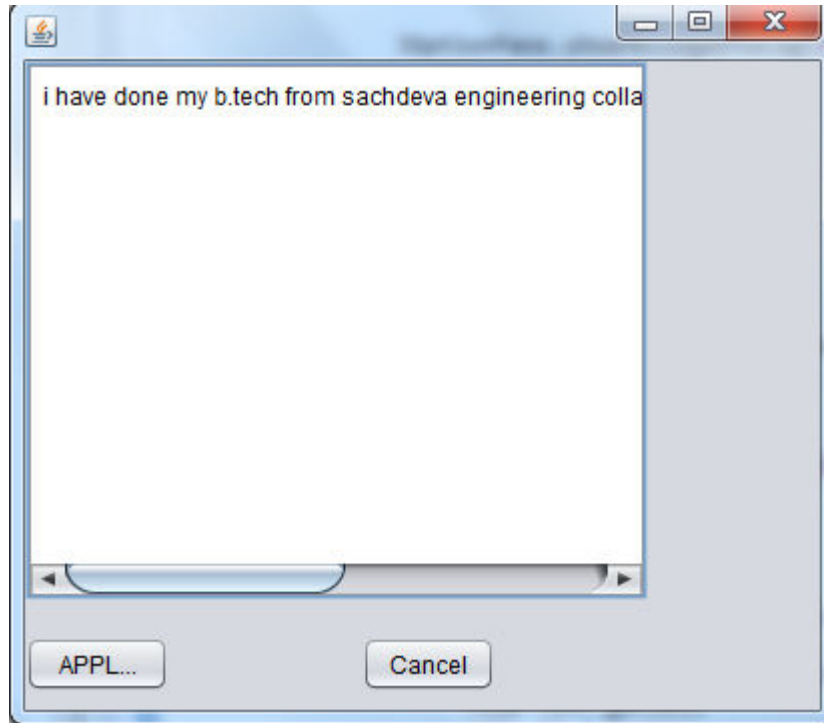
**Figure 20 : Match hash code**

Then the encrypted data is:



**Figure 21 : Encrypted data**

As we know that the when user encrypt data using Elgamal algorithm the cipher data is double than the original data.



**Figure 22 : Decrypted data**

- v. The time taken by algorithm to upload data on cloud is:

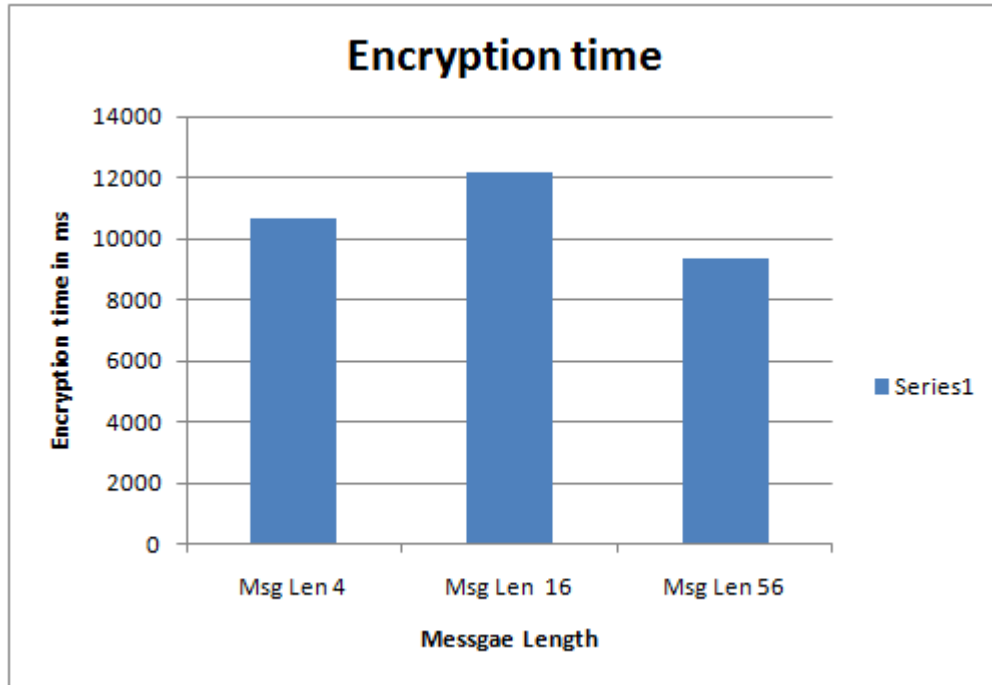
TOTAL FILE UPLOADING TIME TO CLOUD 18889 ms

- vi. The total time taken during decryption is:

TOTAL DECRYPTION TIME 8425 ms

vii. **Performance parameters:**

There are two performance parameters evaluated, encryption time parameter and decryption time parameter. In which we measure the time, that how much time data taking during uploading according to data and measure the time while decrypting.



**Figure 23 : Encryption time graph**

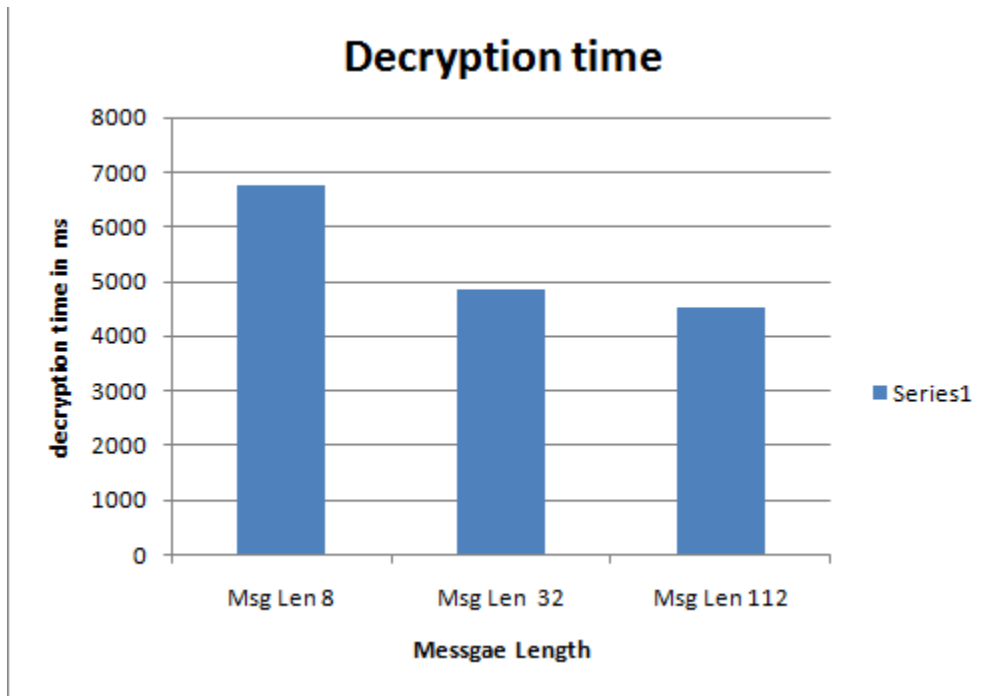


Figure 24 : Decryption time graph

This work is done for the security of the important data or we can say that sensitive data. In this work to share the important data in the public cloud securely. So to protect that data in this work the Elgamal algorithm used. This scheme is also solve the problem of the key escrow and revocation problem. In this to create virtual cloud environment the CloudSim simulator is used. Before storing or uploading the important data to the cloud environment that data is encrypted.

The Private Key that generated on cloud also encrypted using SHA algorithm before storing the data. After encryption process the encrypted keys and the data saved on the cloud. Now for decryption process the user firstly authenticate itself on cloud. After authentication the key matched with the hash code, if it matched the decryption of the data made possible. So the data can share on the public cloud securely.



#### Papers:

Artigas, M., & Virgili, U. (Nov 2013). Towards efficient data access privacy in the cloud. *IEEE and communication magazine*, Vol. 51, Issue 11 .

Chang, B., Tsai, H., Tsai, Y., & Chang, Y. (Feb 2014 ). Applying authentication and network security to in-cloud enterprise resource planning system. *Vietnam journal of computer science*, Vol. 1, Issue 2, .

Chen, D., Chen, L., Fan, X., He, L., Pan, S., & Hu, R. ( 2014). Securing patient-centric personal health records sharing system in cloud computing. *Communication and china*, Vol.11, Issue 13 .

Chen, F., Xiang, T., Yang, Y., & Chow, S. (2014). Secure Cloud Storage Meets with Secure Network Coding. *INFOCOM and proceedings IEEE* .

Chen, Z., Han, F., Cao, J., Jiang, X., & Chen, S. (Feb 2013). Cloud computing-Based forencic analysis for collaborative network security management system. *IEEE Tsinghua science and technology*” Vol. 18, Issue 1 .

Dongt, X., Luot, Y., Chen, Y., G., X., & Lit, M. (Dec 2013). P2E: Privacy-preserving and Effective Cloud Data Sharing Service. *Global Communications and Conference (GLOBCOM) and IEEE* .

Du, Y., Zhang, R., & Li, M. (12 July 2013 ). Research on security mechanism for cloud computing based on virtualization” Springer Telecommunication systems, Vol. 53, Issue 1. *Springer Telecommunication systems, Vol. 53, Issue 1* .

Ge, X., Yao, B., Guo, M., Xu, C., Zhou, J., Wu, C., et al. ( 01 June 2014). LSShare: an efficient multiple query optimization system in cloud. *Springer Distributed and Parallel Databases, Vol. 32, Issue 4* .

Han, B., Jung, I., Kim, K., Lee, D., Rho, S., & Jeong, C. (march 2013). Cloud-based active content collaboration platform using multimedia processing. *EURASIP Journal on wireless communication and networking* .

Jung, Y., Lim, D., Koo, Y., Lee, E., & Choi, H. (6 July 2013). A real-time responsiveness measurement method of Linux-based mobile system for P2P cloud system. *Springer Peer-to-Peer Networking and Applications, Vol. 7, Issue 4* .

Kang, A., Barolli, L., Park, J., & Jeong, Y. (September 2014). A strengthening plan for enterprise information security based on cloud computing. *Springer cluster computing, vol. 17, Issue 3* .

- Kouril, D., Rebok, T., Cegan, J., Drasar, M., Vizvary, M., & Vykopal, J. (2014). Cloud based testbed for simulation of cyber attacks. *IEEE and network operation and management Symposium (NOMS)* .
- Lee, J., Son, J., Hussain, R., & Oh, h. (Jan 2014). Media cloud: A secure and efficient virtualization framework for media service. *consumer electronics (ICCE) and IEEE international conference* .
- Lee, K., Teng, W., Wu, N., Huang, K., Ko, Y., & Hou, T. (December 2013). Multicast and customized deployment of large-scale operating system. *Springer Automated software engineering, Vol. 21* .
- Mohaisen, A., Tran, H., Chandra, A., & Kim, Y. (Dec 2014). Trustworthy Distributed Computing on Social Networks. *IEEE transaction on and services computing”, Vol. 7, Issue 3* .
- Mukundan, R., Madria, S., & Linderman, M. (June 2014). Efficiency integrity verification of replicated data in cloud using homomorphic encryption. *Springer Distributed and Parallel Database* .
- Naresh Kumar, M., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A., & Kumar, M. (2012). Mitigating economic denial of sustainability (EDoS) in cloud computing using In-cloud scrubber service. *IEEE Fourth International Conal International Conference on Computational Intelligence and Communication Networks* .
- Pan, Y., Xiaolin, G., Jian, A., Jing, Y., Jiancai, L., & T., F. (Aug. 2014). A Retrievable Data Perturbation Method Used in Privacy-Preserving in Cloud Computing. *Communications and China”, Vol. 11, Issue 8* .
- Seo, S., Nabeel, M., Ding, X., & Bertino, E. (5 August 2013). An efficient certificateless encryption for secure data sharing in public clouds. *IEEE Knowledge and Data Engineering”, Vol. 26, Issue 9* .
- Wang, Y., Chen, I., & Wang, D. (14 october 2014). A survey of mobile cloud computing applications: Perspectives and Challenges. *Springer Wireless personal communications, Vol. 2, Issue 3* .
- Wang, Y., Luo, J., Song, A., & Dong, F. (January 2014). OATS: online aggregation with two-level sharing strategy in cloud. *Springer Distributed and Parallel Databases, Vol. 32* .
- Xu, P., Chen, H., Zou, D., & Jin, H. (16 July 2014). Fine grained and heterogeneous proxy re-encryption for secure cloud storage. *Springer Chinese Science Bulletin, Vol. 59* .

**Books:**

Gnanasundaram, S.; Shrivastava, A. (2009) “Information storage and management”, *John Wiley and sons, Inc.*, Mumbai

Stallings, W. (2006) “Cryptography and network security”, *Pearson Education, Inc.*