Providing Confidentiality and Integrity for Data Stored on Cloud

Ms .Chaitali Jadhav, Ms .Chaitali Hake, Ms . Priyanka Shendage, Ms . Namrata Hake

Computer Science and Engineering, SKN Sinhgad College of Engineering Korti ,Pandharpur

chaitalijadhav77.cj@gmail.com

hakechaitali0@gmail.com

hakenamrata0@gmail.com

priyankashendage311@gmail.com

Abstract—

Cloud computing allows not only to obtain resources on demand but also store large amount of data. It uses the Internet for the tasks performed on the computer and it is visualized as the next generation architecture of IT Enterprise. The Cloud represents the Internet. In this , we focus on secure data storage in cloud; it is an important aspect of quality of service. To ensure the correctness of user's data in the cloud, We propose effective and adaptable scheme with salient qualities. This scheme achieves data storage correctness allow the authenticated user to access the data and data error localization, i. e. the identification of misbehaving servers. Cloud computing provides the way to share distributed resources and services that belong to different organizations or sites. Since cloud computing share distributed resources via network in the open environment thus it makes security problems.In this paper some important security services including authentication , integrity, confidentiality provided in cloud computing system.

.

***Keywords*— Encryption, Decryption, DES , SHA1,Cloud Provider**

I. INTRODUCTION

cloud computing is nothing but storing and accessing data and program over the Internet instead of from your own hard disk. The cloud computing is a very broad area and it covers about each and every online service. There are usually three models of cloud service.

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

SaaS is a software licensing and delivery model in which software is licensed on subscription basis and is a centrally hosted . SaaS is also called as application as a service. i. e Google Apps PaaS provide platform allowing customer to develop ,run and manage application without complexity of building and maintaining the infrastructure .i. e web server ,databases. IaaS is used to support to hardware , software & storage server mainly used for delivering software application environment. i .e Amazon ,Microsoft.

There are various types of cloud computing :

1 .Public
2 .Private
3 .Hybrid

A public cloud is basically the internet. Service providers use the internet to make resources, such as applications and storage, available to the general public, or on a _public cloud. private clouds are data center architectures owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as needed. There are three important parameter are considered for security of information over cloud. They are Confidentiality Ensure that only authorized users have access to data. Integrity Ensure that unauthorized changes to data are not allowed. Availability Ensure that authorized user have reliable and timely access to data Information.

II. Overview of Project

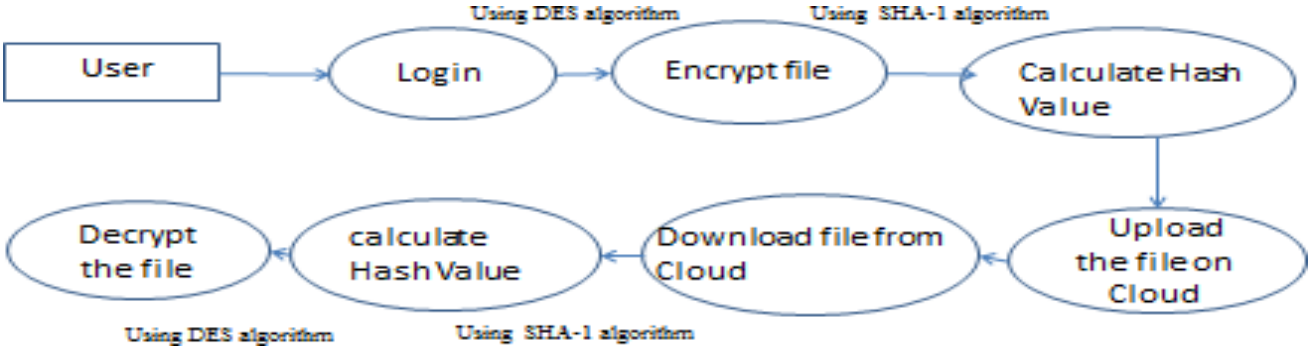

Fig 2.1:Data Flow Diagram

In this project we are using DES algorithm for encryption and decryption purpose and SHA-1 algorithm for calculating Hash value to achieve integrity .

III. ALGORITHM

DES Algorithm:

DES is a block cipher algorithm. It uses 56-bits key for the encryption. This key looks like 64-bits.but 1-bit from every octet is used as parity bit, hence actual key size 56-bits.DES takes 64-bits size block as input and performs substitution and permutation on that block .which is after Ex-OR with input. This process is repeated for 16 times with the help of sub keys. As this algorithm uses 16 rounds, it makes it secure. Decryption is done in reverse order with the same key. As this is Symmetric key algorithm so it uses same key for encryption and same key for decryption. We know that key size is 56 –bits so attacker will obtain plain text after 2^56 trials on an average. If key use for encryption is not stronger then it is easy work for attacker ,And also all sub key are same then after 16 round we get plain text as it in which not expected . [3]. Neha Jain and Gurpreet Kaur –Implementing DES Algorithm in Cloud for Data Security‖ VSRD International Journal of CS & IT Vol. 2 (4), 2012

SHA-1 Algorithm:

There are various steps involved in the SHA-1. They are listed as follows :

1. Message Padding
2. Append Length
3. Divide the Input into 512 bit blocks
4. Initialize chaining variables
5. Process Blocks
   - 5.1 Copy variables to register
   - 5.2 Divide one 512 bit block into 16 blocks of 32 bit each
   - 5.3 4 rounds, each round consisting of 20 steps.
   - 5.4 Diagram + process P + all chaining variables.

Step 1:

Adding padding bits to the original message is the first step of SHA-1 algorithm. The main objective of this step is to make the length of the original message equal to a value which is 64 bits less than an exact multiple of 512. For example, if the original message is 900 bits, then we add a padding of 60 bits which makes the message length 960 which is hence 64 bits less

than 1024 (1024=512 × 2). The padding consists of a single 1 bit followed by as many 0‘s bits as required. It is mandatory to add padding bits even if the original message length is itself 64 bits less than the multiple of 512.

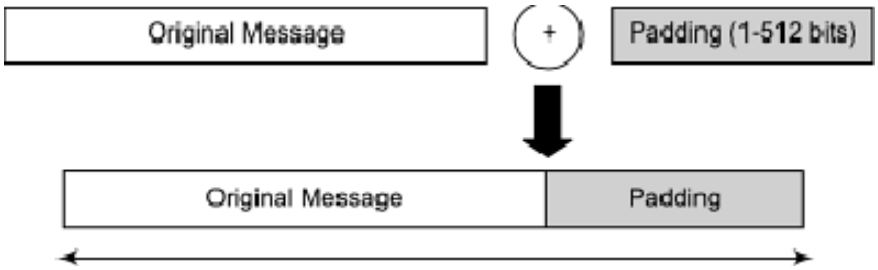

Fig 3.1: Padding

Step 2 :

The next step after adding padding bits is to calculate the original length of the message and append it to the end of the message after padding. Now the question is how is it done? The length of the message is calculated excluding the padding bits i.e. the length of the message before the padding bits were added. For example, if the original message was of 900 bits and a padding of 60 bits was added to make the length 64 bits less than the multiple of 512 then here the length is considered 900 bits instead of 960 bits. This length is now expressed as a 64 bit value and appended to the end of the original message padding. This process is better explained by the figure. Now if the length of the original message exceeds 264 bits then only lower order 64 bits are used here i.e. length mod 264 is calculated in that case. Hence the length of the message is now an exact multiple of 512. This becomes the message whose message digest will be calculated.

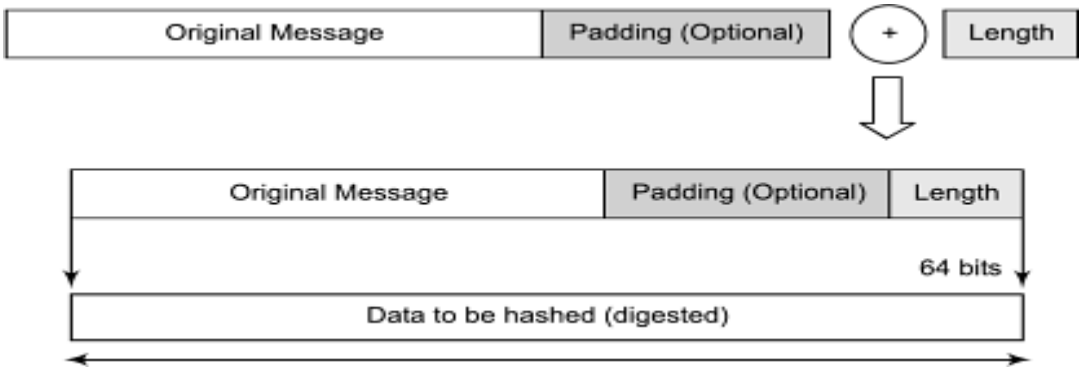

Fig 3.2 : Append Length

Step 3:

The next step is to divide the input message into blocks, each of length 512 bits. Now these blocks become the input to the message digest processing logic.

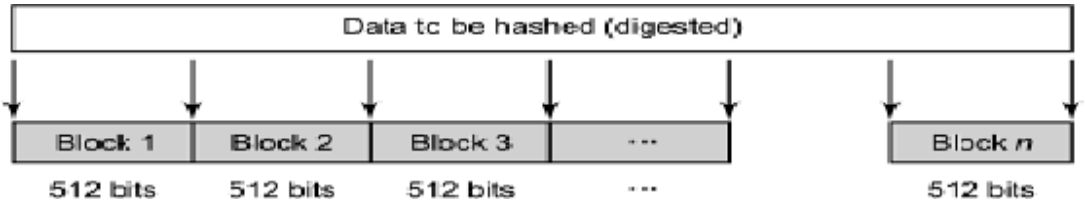

Fig 3.3 : divide input into 512 bit block

Step 4 :

There are five chaining variables A through E. These five chaining variables are initialized in this step. MD5 had four chaining variables each of 32 bits (total length will be 4 × 32=128 bits) but in the case of SHA-1 we need a message digest of 160 bits hence there are five chaining variables here making a total of 5 × 32=160 bits. The values for these chaining variables are as shown in the figure.

A	Hex	01	23	45	67
B	Hex	89	AB	CD	EF
C	Hex	FE	DC	BA	98
D	Hex	76	54	32	10
E	Hex	C3	D2	E1	F0

Fig 3.4: Initializing Chaining Variable

Step 5 :

Process Block

Step 5.1:

The chaining variables _A-E' are copied in five registers _a-e', resulting in a combined register _abcde' which will be considered as a single register for storing the temporary intermediate as well as the final results.

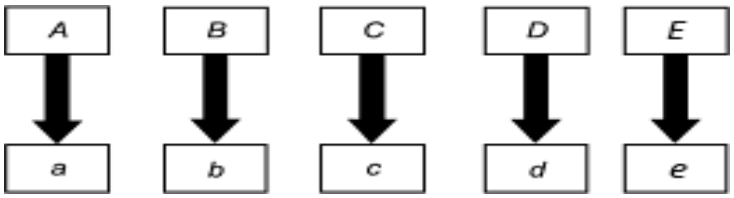

Fig 3.5.1: Register

Step 5.2 :

In this step the current 512 bit block is divided into 16 sub-blocks of 32 bits each.

Step 5.3 :

SHA-1 has four rounds each of 20 steps. As inputs to one round are current 512 bit block, the register abcde and a constant K[t] where t = 0 to 79. The contents of register abcde are updated using the SHA-1 algorithm steps. Here there are only four constants defined for K[t], one used in each round.

Step 5.4 :

The SHA-1 consists of four rounds each consisting of 20 iterations which makes a total of 80 iterations. The entire operation of SHA-1 is shown in figure

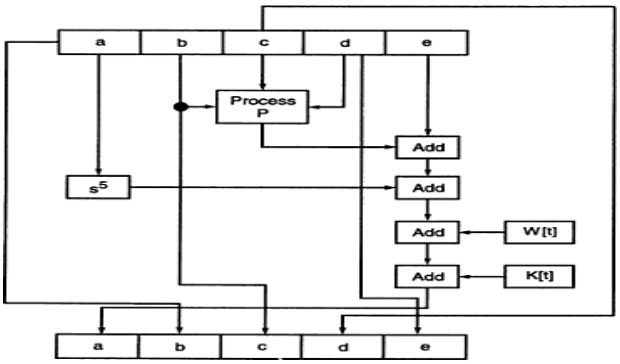

Fig 3.5.2 : Algorithm Operation

To represent mathematically the operations in one iteration,

a = (e + Process P + s5(a) + W[t] + K[t])
b = a
c = s30(b)
d = c
e = d

Combining all of these results ,
Abcde = (e + Process P + s5(a) + W[t] + K[t]), a, s30(b), c, d
Where, abcde = the register made of 5 chaining variables
Process P = logical operation.
S_t = circular left shift of the 32 bits sub-block by t bits
W[t] = a 32 bit derived from the current 32 bit sub-block calculated as follows,
1. For the first 16 words of W (i.e. t = 0 to 15), the contents of the input message sub-block M[t] become the contents of W[t] directly.
2. For remaining 64 values of W are derived using the equation:
W[t] = s_1 (W[t – 16] XOR W[t – 14] XOR W[t – 8] XOR W[t – 3])
s_1 = Circular-left shift by 1 bit position
[13] SHA1 Description, B Thomas Golisano College,http://www.cs.rit.edu/~ bcw5910/482 TeamFlux.pdf

IV. IMPLEMENTATION

Fig 4.1: operations

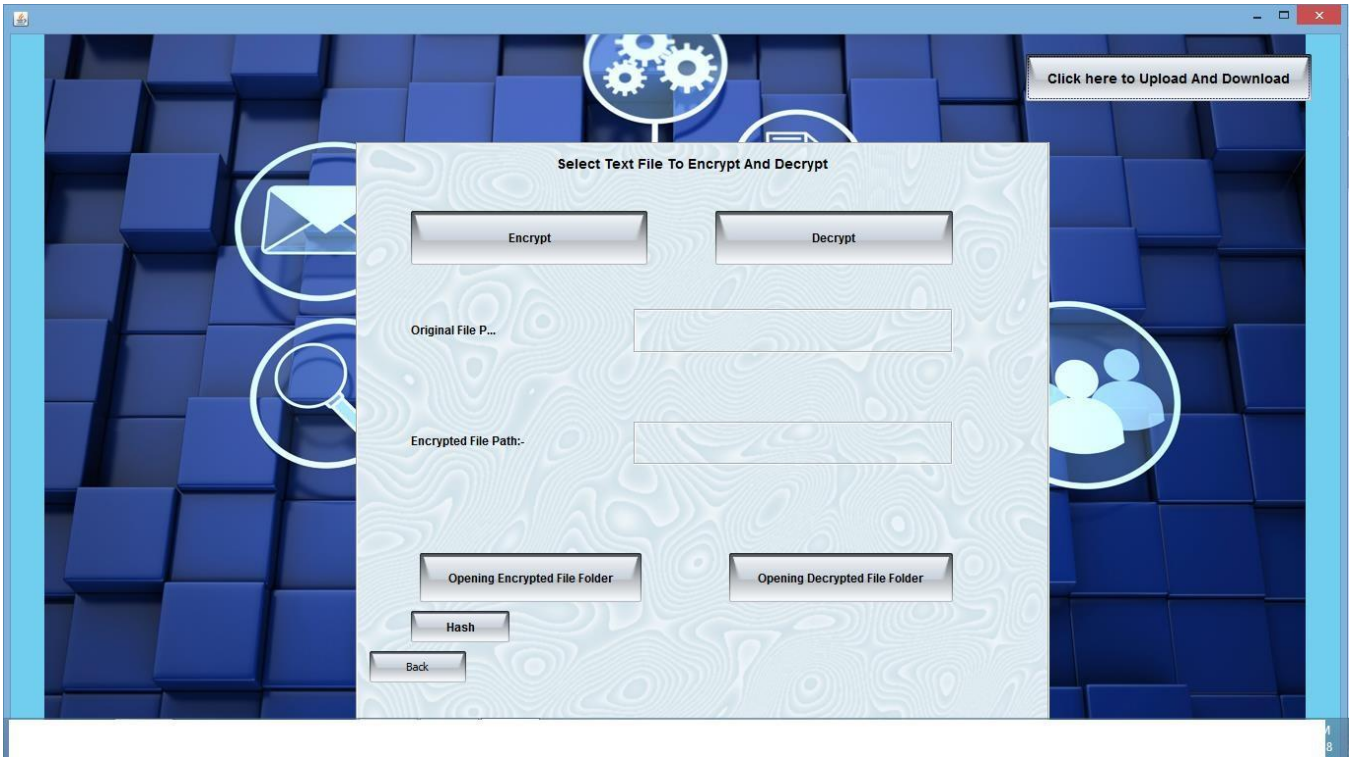

Fig 4.2: File Select for Encryption

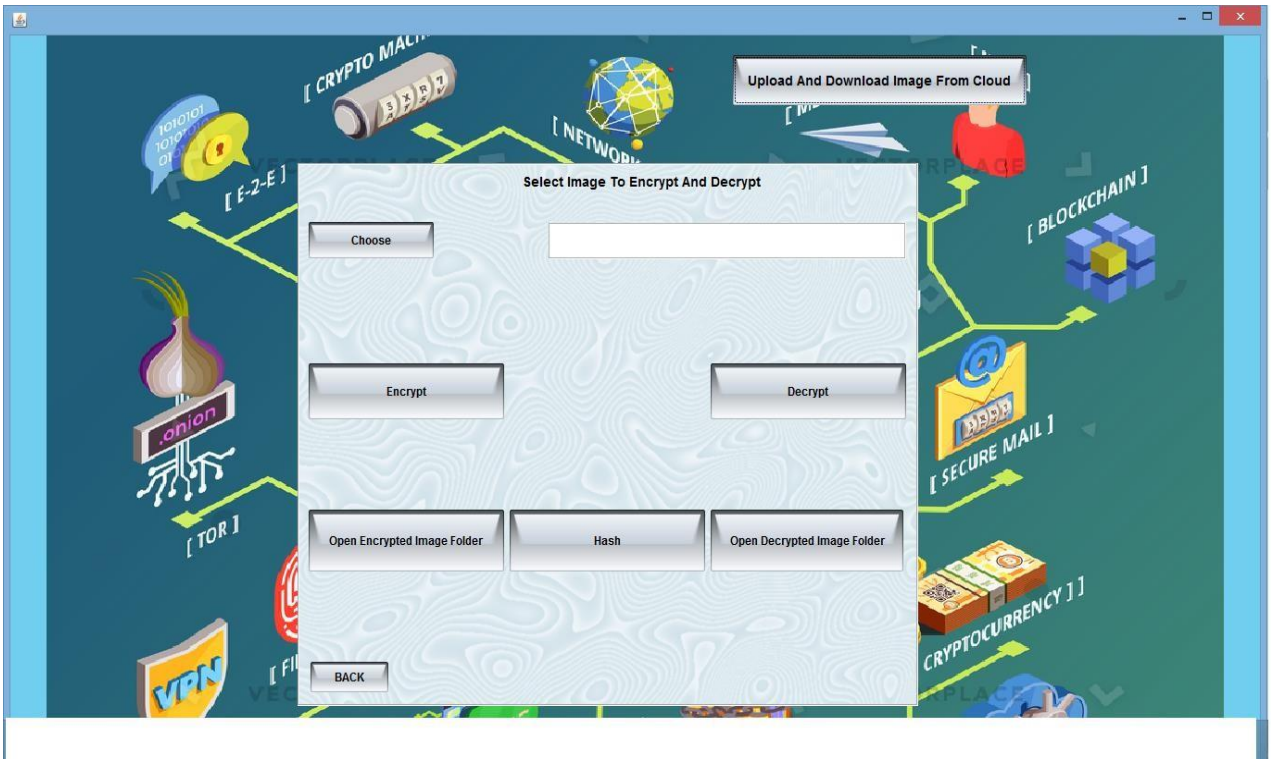

Fig 4.3: Encrypt Image

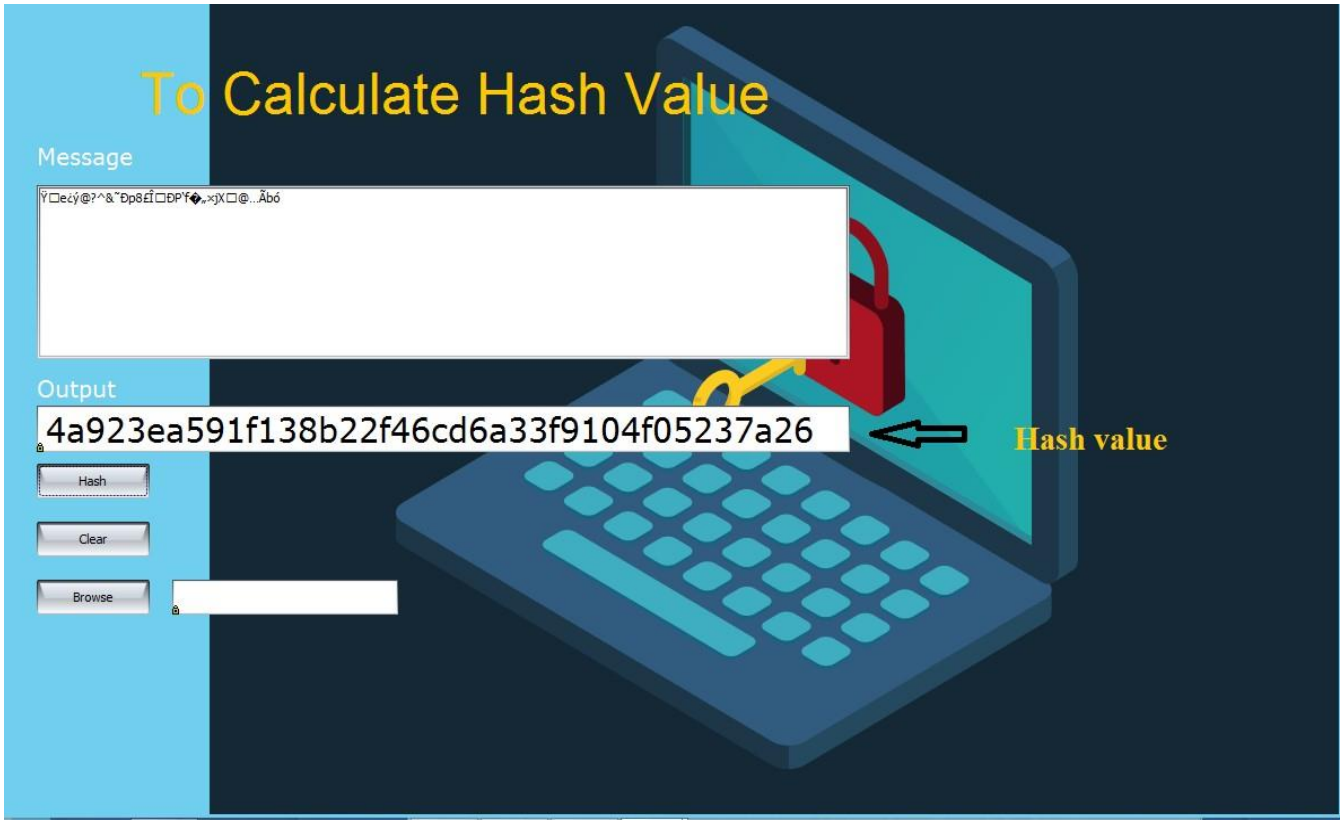

Fig 4.4 : To Calculate Hash Value

V. CONCLUSIONS

In this project, we investigated the problem of data security in cloud data storage, which is essentially in a distributed storage system. To ensure the correctness of user data in cloud data storage we proposed an effective and flexible distributed scheme with explicit dynamic data support ,including block update, delete and append.

ACKNOWLEDGMENT

We would like to express our deep sense of gratitude to our guide Prof. N.M.Sawant for his invaluable help and guidance for the duration of project. Project Coordinator for providing the support and giving his valuable time, indispensable support and his priceless suggestions. We are highly indebted to Prof.S.V.Pingale, HOD for constantly encouraging us by giving critics on our work.. We also express gratitude towards our all teaching & non teaching staff, family members and our friends for encouraging us with their valuable suggestions and motivating us from time to time.

REFERENCES

[1]. Ensuring data storage security in cloud computing- Cong Wang ,Qian Wang & Kui Ren Department of ECE
[2]. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com
[3]. Neha Jain and Gurpreet Kaur –Implementing DES Algorithm in Cloud for Data Security‖ VSRD International Journal of CS & IT Vol. 2 (4), 2012
[4]. Mandeep Kaur and Manish Mahajan –Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing‖ VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10 October 2012
[5]. Amir Mohamed Talib‖ Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review‖ Computer and Information Science Vol. 3, No. 4; November 2010
[6].Rachna Arora and Anshu Parashar ‖ Secure User Data in Cloud Computing Using Encryption Algorithms‖ International Journal of Engineering Research and (IJERA) Application sISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926
[7]. B. Ravi Kumar, Dr.P.R.K.Murti‖ Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology‖ B. Ravi Kumar et al. / International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 7 July 2011.
[8]. Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter Cloud Computing: A Practical Approach Copyright © 2010 by The McGraw-Hill Companies
[9]. Matthew J. Harmon Cloud Security (ISC)2 Twin Cities Area Chapter 2013 Annual Meeting 18 June 2013
[10] K Nava Jyothi Practical Approach to Cloud Centre for Development of Advanced Computing, Hyderabad 8/9/2010
[11]. Tobias Kurze_, Markus Klemsy, David Bermbachy, Alexander Lenkz, Stefan Taiy and Marcel Kunze Cloud Federation Karlsruhe Institute of Technology (KIT), Kaiserstrasse 12, 76131 Karlsruhe, Germany
[12]. N. M. Sawant, V. V. Pottigar, N. S. Mane, A Survey on Auditing Technique used for preserving privacy of data stored on cloud International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) 2016.
[13] SHA1 Description, B Thomas Golisano College,http://www.cs.rit.edu/~ bcw5910/482 TeamFlux.pdf