6) **Social Engineering Attack:** By heavily relying on human interactions, victim is tricked into disclosing valuable information such as password.
7) **Malware Injection Attack:** In this attack, an adversary attempts to inject malicious service or code, which appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping [7].
8) **Phishing Attack:** Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. It may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud.

4. Security Algorithms

4.1 Blowfish

Blowfish is block cipher 64-bit block- can be used as a replacement for the DES algorithm. Its structure is similar to IDEA algorithm[8][9]. It takes a variable length key, ranging from 32 bits to 448-bits [10]. Blowfish is successor of Two fish. The blowfish algorithm was first introduce in 1993 by Bruce Schneider, and has not cracked until now. It is also noteworthy to point out that this algorithm can be optimized in hard ware applications, is often used in software applications, although it is like most other ciphers. The encryption is simply like feistal network of 16 rounds.

Blowfish is a symmetric block encryption algorithm designed in consideration with,
Fast : It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.
Compact: It can run in less than 5K of memory.
Simple: It uses XOR, addition, lookup table with 32-bit operands.
Secure: The length of key is variable, it can be in the range of 32~448 bits: default 128 bits key length.
It is useful for applications where the key does not change often, like an automatic file encryptor or communication link.
Royality-free and unpatented

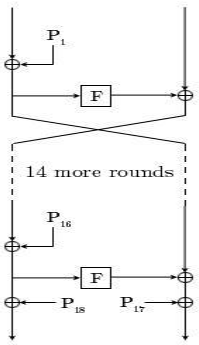

Figure 1: The Feistel structure of Blowfish
[Source: http://en.wikipedia.org/wiki/File:BlowfishDiagram.png]

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follows the feistel network and this algorithm is divided into two parts : Key-expansion and Data Encryption.

1) **Key Expansion**
It will converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses big number of subkeys and these keys are generate earlier to any data encryption or decryption.
The p-array consists of 18 subkeys of 32 bit :
P1,P2,……..,P18
Four 32-bit S-Boxes consists of 256 entries for each:
S1,0, S1,1,……. S1,255
S2,0, S2,1,…….. S2,255
S3,0, S3,1,…….. S3,255
S4,0, S4,1,.....S4,255

2) **Data Encryption**
It is having a function to iterate 16 times of network. Every round consists of key-dependent permutation and data-dependent substitution and a key. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.

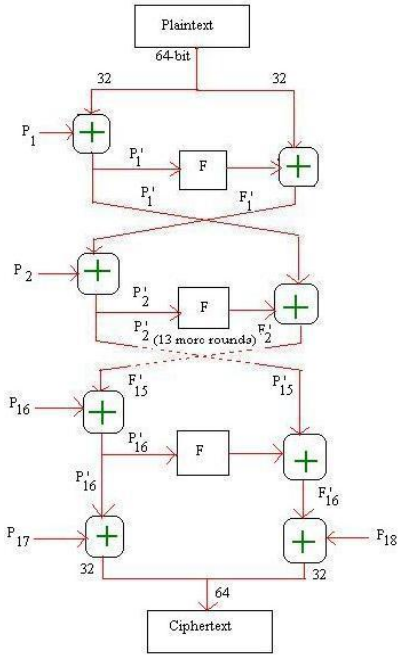

Figure 2: Blowfish Encryption

Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

4.2 MD5

A message-digest algorithm is also called a cryptographic hash function or a hash function. It accepts a message as

input and generates output of a fixed-length, which is commonly less than the length of the input message. The output is called a message digest, a fingerprint or a hash value.

There are three kinds of operations in MD5: Cyclic Shift Operation, Modular Addition and Bitwise Boolean Operation. All these three operations are very fast on a 32-bit machine. Hence MD5 is quite fast.

MD5 algorithm developed by Ron Rivest and introduced in the year 1991. It is used to verify the integrity of the message. The main goal of this algorithm is security, speed, simplicity, compactness, and little-endian architecture. It processes block of 512-bit and generates 128-bit message digest. The processing consisting of the following steps:

1. Append padded bits
2. Append length
3. Initialize MD buffer
4. Process blocks.
5. Hashed Output

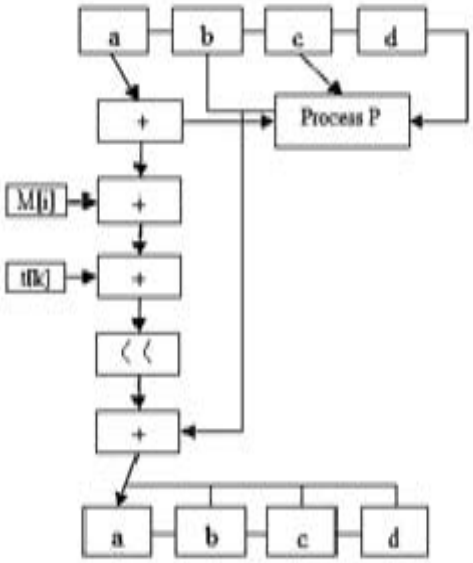

Figure 3: One MD5 Iteration

Step 1:- Append padded bits
The message is padded so that its length is congruent to 448, modulo 512 means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.
Step 2:-Append length
A 64 bit representation of b is appended to the result of the step 1. The resulting message has a length that is an exact multiple of 512 bits.
Step 3:- Initialize MD buffer
A four-word buffer (A,B,C,D) is used to compute the message digest. Here each of A,B,C and D is a register of 32 bit. These registers are initialized to the following values in hexadecimal:
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10
Step 4:- Process blocks
Four auxiliary functions that accept as input three 32-bit words and produce as output one 32-bit word.
F(X,Y,Z) = XY v not(X) Z
G(X,Y,Z) = XZ v Y not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X v not(Z))
The bits of X, Y, and Z are totalitarian and balance the each bit of F (X, Y, Z) will be totalitarian and balance. The functions (X, Y and Z) = P, in that they do job in "bitwise parallel" to produce the reliable output from the bits of X, Y and Z. If the bits of X, Y, and Z are independent and unbiased, the each bit of G(X,Y,Z), H(X,Y,Z), I(X,Y,Z) and F(X,Y,Z) will be independent and unbiased.
Step 5:- Hashed Output
The message digest produced as output is A, B, C and D. That is, output begins with the low-order byte of A, and end with the high-order byte of D.There are 4 rounds performed in MD5 which is of 128 bits. Fig 3 shows One MD5 iteration **[11] [12].**

5. Conclusion

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including platforms, infrastructure and applications that are available from cloud service providers as online services. People may be confused by the range of offerings and the terminology used to describe them and will be unsure of the benefits and risk. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed MD5 and Blowfish algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of MD5 and Blowfish.

References

[1] Anthony Bisong, Syed, M. Rahman "An overview of the security concerns in Enterprise cloud computing," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.
[2] I. Foster, Y. Zhao, I. Raicu, and S. Lu, 2008, "Cloud Computing and Grid Computing 360-Degree Compared, In: Grid Computing Environments Workshop", 2008. GCE '08, p. 10, 1.
[3] Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Chirag Modi,Muttukrishnan Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," Springer Science+Business Media New York 2012.
[4] E.Anitha, Dr.S.Malliga, "A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks," Information Communication and Embedded Systems (ICICES), 2013 International Conference
[5] Christof Kauba, Stefan Mayer, "When the Clouds Disperse Data Confidentiality and Privacy in Cloud Computing," University of Salzburg

[6] Te-Shun Chou , "SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES" International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013
[7] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds ," The University of Alabama
[8] S. Basu, "International Data Encryption Algorithm (IDEA) – A Typical Illustration", Journal of Global Research in Computer Science, vol. 2, no. 7, pp: 116-118, July 2011.
[9] M. Leong, O. Cheung, K. Tsoi and P. Leong, "A Bit Serial Implementation of the International data Encryption Algorithm IDEA", Proc. IEEE Symposium on Field-Programmable Custom Computing Machines, pp:122-131, 2000.
[10] Vinaya.V, Sumathi.P," Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, May 2013.
[11] Rivest R., 1992, "The MD5 Message-Digest Algorithm,"RFC 1321,MIT LCS and RSA Data Securit y, Inc.
[12] Kahate, Atul, 2003, "Cryptography and Network Securit y", Tata McGraw-Hill ,India.
[13] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State university, Columbus, GA, 2010
[14] Rahul Bhatnagar, Suyash Raizada, Pramod Saxena, SECURITY IN CLOUD COMPUTING,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December - 2013.
[15] Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master Thesis Electrical Engineering School of Computing Blekinge Institute of Technology SE – 371 79 Karlskrona Sweden, November 2011.
[16] Sanjana Sharma, Sonika Soni, Swati Sengar, Security in Cloud Computing, National Conference on Security Issues in Network Technologies, 2012.