ISSN NO: 2350-1146 I.F-5.11

A Survey on Cloud Computing Parameters

Mrs.Sonali A Patil Research Scholar, Department of CSE BSAR Crescent University, Vandalur Chennai .
Dr.M.Sandhya ,Professor ,HOD Department of CSE BSAR Crescent University ,Vandalur Chennai

Dr.Sharmila Sankar, Professor, Department of CSE BSAU Crescent University, Vandalur Chennai

***Abstract*—In today's technological world, virtual resources and services are more demanded over the network and internet. Cloud Computing (CC) is an on-demand service over network servers which are hosted on Internet to process, store and organize the data. Cloud computing is the best solution in all terms like scalability, cost, flexibility, and efficiency. Cloud computing have various parameters and different aspects. The different aspect of cloud computing like security, integrity, confidentiality, reliability and availability are explained in this survey. As there are many advantages of cloud, there are also some disadvantages of cloud. In this paper some issues and algorithms related to every parameter are reviewed. For every aspect of cloud computing, after studying many algorithms one of them is chosen as solution and discussed in this paper.**

***Index Terms*—Availability,Cloud Computing, Confidentiality, Integrity,Security.**

I. INTRODUCTION

Cloud computing can be explained in simple word as, it is an internet based service or computing which gives access to the large shared resources from many computers, at any time and at any point of location , where internet is reachable. Cloud computing reduces the physical infrastructure need for information access and for storage. This term of cloud computing is invented from the need of shared resources and then need of zero infrastructure. At very starting stage of computers, the organizations need large storage like mainframe to each employee, but this couldn't possible to give such large resources to every employee, so that result in shared access to mainframe, which further leads, VPN the concept, so that many users can have their own connections at reduced cost. Since after VPN the concept of cloud computing come in front, which provide the virtual resource that can use from anywhere, at any time. So this offers no need of physical infrastructure, not needed to carry extra hardware like pen drives for accessing data at other place. That is why cloud computing is becoming so popular now a days, SoftLayer is one of the largest global providers of cloud computing infrastructure [1].

Cloud computing has four types or four deployment models as public cloud, private cloud, community cloud, and hybrid

cloud. Cloud computing has characteristics as on-demand self-service, broad network access, resources pooling, rapid

elasticity. These benefits to reduce IT cost, flexible the scaling, increase the availability, and business agility[3].In further sections we will study different parameters of cloud computing like security, integrity, reliability, confidentiality and availability. Issues related to these parameters and the algorithms for achieving these issues.

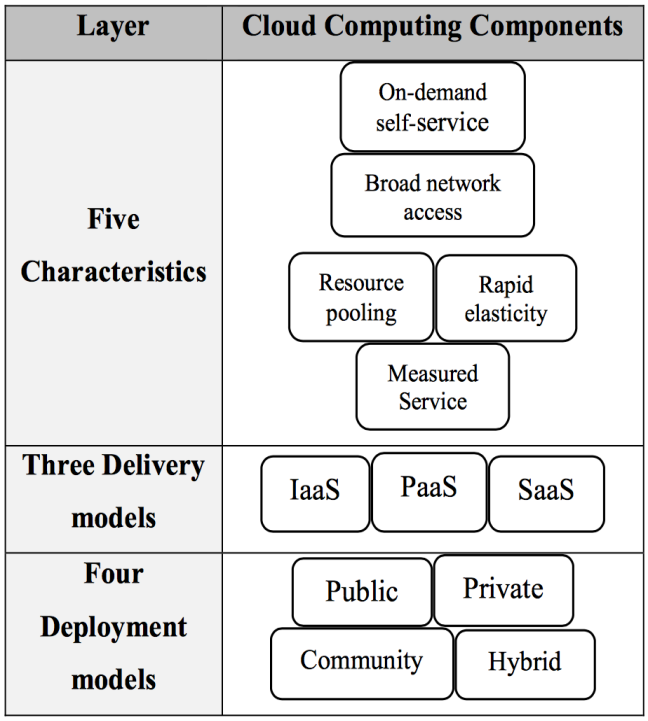

Fig. 1.Cloud computing components.

ISSN NO: 2350-1146 I.F-5.11

II. LITERATURE SURVEY

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Because of this organizations can work on large resource available for every employee at a time, users can use same data simultaneously instead of waiting for data will be saved, and emailed, then can do the work. Users not needed to install any software or upgrade the software because the cloud can be accessed from any web browser regardless of device user uses like computer, laptop, tablet or phone. User can connect to cloud through internet from anywhere it may be far away from organization or while travelling. They can easily access the cloud and work on the storage information stored on cloud, the storage location is regardless as it is off site, any third party may handle the cloud storage.Cloud providers typically use a "pay as you go"model.[2].

Cloud computing has four types or four deployment models as public cloud, private cloud, community cloud, and hybrid cloud. When a Cloud is available in a pay-as-you-go manner to all the general public, it called as a Public Cloud. Another term is Private Cloud which refers to internal data centres or reserved locations of a business or other organization, these can be owned, or managed, but not made available to the general public. Private cloud again has two types as on-promise private cloud and externally hosted private cloud. In community cloud the access is provisioned to specific clients from organizations that have shared concern. The last type of cloud is hybrid cloud, is the combination of two or more clouds form other cloud types like public cloud, private cloud, community cloud. Cloud computing enabling technologies are Grid computing, Utility computing, Virtualization and Service Oriented Architecture (SOA). Grid computing is distributed computing with heterogeneous computers, utility computing is service based model available whenever needed. Virtualization is the abstract of physical characteristic of IT resources, service oriented architecture is set of services. The cloud used generally is public cloud and the service being sold usually is Utility Computing[3].

Cloud computing have many aspects like data security, confidentiality, integrity, availability and reliability. Out of which first aspect and most important is security. This aspect becoming important with increasing use of cloud. Many researches have going on to find the solution over this issue. Some important and effective solution we will see in section 3. In this, the solutions are studied from the research papers and solutions are like cryptographic algorithms, symmetric key cryptographic algorithm, and asymmetric key cryptographic algorithm. The best symmetric key cryptographic algorithm is BLOWFISH and asymmetric cryptographic algorithm RSA are explained in further section. Some websites and Wikipedia information helped in this [1][2][4][9]. The research papers referred for this are [5],[6],[7],[8],[10],[11].

While using cloud data it is very important to keep our data intact that is mean by without loss or damages of data like corrupted, hacked or altered. For this purpose the next aspect of cloud computing that is integrity is proposed in section 4.The issues related to integrity and solution over those is explained in this section. For this solution papers studied are from [12],[13],[14],[15],[16].

Cloud computing technology is nowadays used every where any one can use it at any place for any time. This increase the risk of data privacy. That is new aspect of cloud computing is confidentiality. This can be achieve by allowing to only authenticated user, for this user login is important. Different methods of getting the confidentiality are presented in section 5. These approaches are referred from [17],[18].

The last aspects of cloud computing those are availability and reliability are proposed in section 6 and section 7. These aspects directly effect on cloud service.[19],[20].

III. CLOUD SECURITY

Cloud security is obtained by using cryptographic algorithms. In pure science terms [4b], Cryptography is the science of using mathematics for making plain text information(P)that is original data which is input to algorithm into an unreadable cipher text (C) format that is scrambled message output as random stream of unintelligible data. This process iscalled encryption and reconverting that cipher text back to plain text calledas decryption. This done with some the set of Cryptographic encryption Algorithms (E) using encryption keys (k1 and k2) and the decryptionalgorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as

Cipher text C = E {P, Key} and Plain text C = D {C, Key}

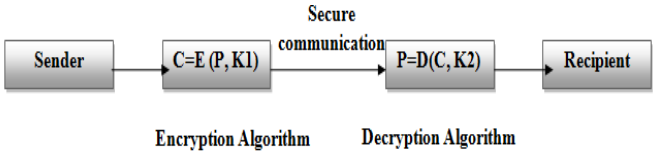

Fig. 2.Cloud data encryption.

Security Algorithms are classified broadly as:

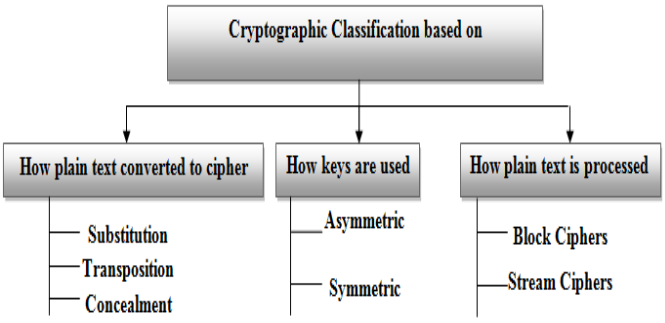

Fig. 3.Cryptographic algorithms classification

1. *Symmetric Algorithms:*
   Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver.RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.
2. *Asymmetric Algorithms:*
   Use a key pair for cryptographic process, with public key for encryption and private for decryption. These

ISSN NO: 2350-1146 I.F-5.11

algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public key algorithms.

3. *Signature Algorithms:*
   Used to sign and authenticate use data are single key based. Examples include: RSA, DH
4. *Hash Algorithms:*
   Compress data for signing to standard fixed size. Examples include: MD5, SHA

A. Symmetric Algorithms

Symmetric algorithms involve a single shared secret key [4b] to encrypt as well as decrypt data and are capable of processing large amount of data. Also from computing standpoint algorithms are not very power intensive, so has lower overheadon the systems and have high speed for performing encryption and decryption.

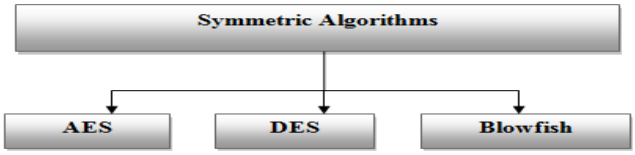

Fig. 4.Symmetric algorithms.

By the survey of all symmetric algorithms on different attribute [4c], if the demand of any application is the smallest memory size the Blowfish is the best option. Blowfish consumes the least time amongst all. Blowfish is efficient in software, at least on some software platforms. After evaluating DES, 3DES, AES, Blowfish and RSA based on parameters entropy, Blowfish scores highest; hence they conclude that Blowfish is strongest against guessing attacks. Results shows
If time and memory isa major factor in the application, Blowfish is the best suited algorithm.

B. Blowfish Algorithm

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.[4d] It isa 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resemblesCAST-128, which uses fixed S-boxes.

The diagram above shows Blowfish's encryption routine. Each line represents 32 bits. Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption ordecryption. The P-array consists of 18 32-bit subkeys: P1,P2,..., P18(denoted as K in the diagram, to avoidconfusion with the Plaintext).There are also four 32-bit S-boxes with 256 entries (S0, S1, S2 and S3).It is having a function to iterate 16 times of network. Each round consists of key-dependentpermutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round. Every round *r* consists of 4 actions:

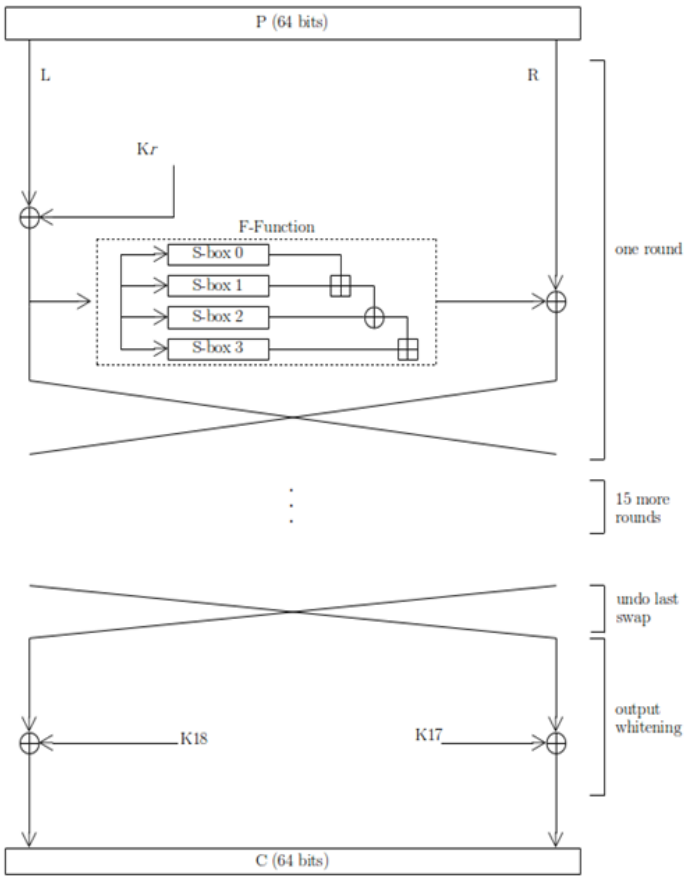

Fig. 5.Blowfish algorithm.

1) First, XOR the left half (L) of the data with the *r*th Parrayentry.PL = PL XOR Ki
2) Second, use the XORed data as input for Blowfish's F-function.
3) Third, XOR the Ffunction'soutput with the right half (R) of the data.PR = F(PL) XOR PR
4) And last, swap L and R i.ePL and PR

The F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters asinput to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 232 and XORed to produce the final 32-bit output.[4]After the 16th round, undo the last swap, and XOR left L with K18 and right R with K17.Decryption is exactly the same as encryption, except that K1, K2...K18 are used in the reverse order.

Sub keys can be generated using Blowfish algorithm by initialising these strings with some hexadecimal digits and XOR with key. In total, 521 iterations are required to generate all requiredsub keys. Because of this applications can directly store the subkeys rather than execute this derivation process every time.

C. Asymmetric Algorithms

Asymmetric Algorithms [4b] a pair of related key, one key for encryption called the Public key and a different butinter related key for Decryption called the Private keys.When performing transformation of plain text into ciphertext both key are used alternatively. The main asymmetric algorithms are ECC, Diffie-Hellman and RSA.

ISSN NO: 2350-1146 I.F-5.11

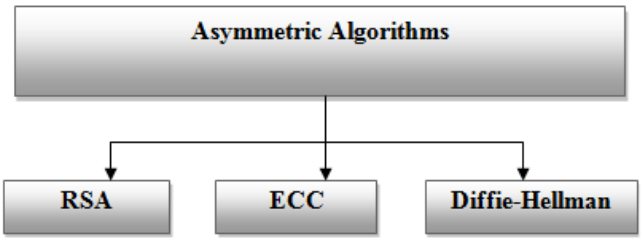

Fig. 6.Asymmetric algorithms.

D. *RSA Algorithm*

RSA is a public key algorithm invented by Rivest, Shamir and Adleman.It uses different keys for encryption and decryption. Therefore it is called as asymmetric.RSA involves a public key and private key. The public key can be known to everyone; it isused to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key of the own decrypting person's. The keys for the RSA algorithm are generated the following way:

1.Choose two different large random prime numbers ***p***and***q***
2. Calculate n=***pq***
3. Calculate the to tient = $\phi(n) = (p-1)(q-1)$
4. Choose exponent an integer e such that $1 < e < \phi(n)$, and $\gcd(e,\phi(n)) = 1$.
5. Calculate the private exponent a value for d such that $d = e^{-1} \bmod \phi(n)$
6. Public Key = [e, n]
7. Private Key = [d, n]

The pair of numbers (e,n) is known as the public key and can be published.The pair of numbers (d,n) is known as the private key and must be kept secret.nis the modulus for the public key and the private keys and e is released as the public key exponent and d is released as the private key exponent.

1) *generate the prime integer pand q:*

If RSA requires a modulus of size B bits. Using a high-quality random number generator,first generate a random number of size B/2 bits. Now check the resulting integer is prime or not. If not, increment the integer by 2 and check again. This becomes thevalue of p. Do the same thing for selecting q. Start with a randomly generated number of size B/2 bits, and so on.

2) *generate the public exponent e:*

The mathematical requirement of e is that $\gcd(e,\phi(n)) = 1$, since otherwise e will not have a multiplicative inverse that is modϕ(n).Since $n = p \times q$, this requirement is equivalent to the two requirements $\gcd(e, \phi(p)) = 1$ and $\gcd(e, \phi(q)) = 1$. In otherwords, $\gcd(e, p-1) = 1$ and $\gcd(e, q-1)=1$.Butdon't forget the basic requirement on e that it must be relatively prime to $p-1$ and $q-1$. Simultaneously we indeed have $\gcd(e, p-1) = 1$ and $\gcd(e, q-1) = 1$If either p or q is found to not meet these two conditions on relative primality of$\phi(p)$ and $\phi(q)$ vies-a-versa, we must discard the calculated pand/or q and start over.

3) *generate the private exponent d:s*

$d \times e \equiv 1 \pmod{\phi(n)}$ this can also write asd = $e^{-1} \bmod \phi(n)$. Calculating '$e^{-1} \bmod \phi(n)$' is referred to as modular inversion.Since d is the multiplicative inverse of e modulo $\phi(n)$, we can usethe Extended Euclid's Algorithm for calculating d. We know the value for $\phi(n)$ since it is equal to $(p-1)\times(q-1)$.

Note that the main source of security in RSA is keeping p and q secret and therefore also keeping $\phi(n)$ secret. It is important to realize that knowing either will reveal the other. That is, if we know the factors p and q, we can calculate $\phi(n)$ by multiplying $p-1$ with $q-1$. And if we know $\phi(n)$ and n, you can calculate the factors p and q easily.

RSA also used for digital signature.In digital signature technique, the RSA algorithm uses the private key to encrypt and the public key to decrypt in the encryption/decryption process. Anybody successfully decrypting such messages can be sure that only the owner of the secret key could have encrypted them.

IV. CLOUD INTEGRITY

As the cloud data is not physically accessible to user, cloud should provide way to check the integrity of data maintained or not. Integrity is simply means correctness of data. Different studies are performing for proving data integrity, it based on file or data retrieval. They use Different cryptographic algorithm to retrieve the file or data like RSA,HASH,SHA and challenges-response messages.

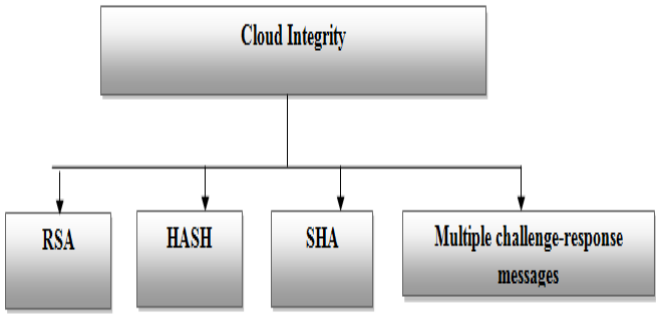

Fig. 7.Cloud integrity algorithms.

From all cryptographic algorithms the most used and secure with more efficiency result for data integrity is the SHA algorithm. The Secure Hash Algorithm (SHA) is the most widely used hash function. A prime motivation for the developing of the SHA was the Digital Signature Standard, in which it is incorporated. The four SHA algorithms are structured differently and are named as SHA-0, SHA-1, SHA-2, andSHA-3.

A. *SHA-0*

This is the original version of Secure hash Algorithm. SHA-0 produces the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

B. *SHA-1*

A 160-bit hash function this resembles the earlier MD5 algorithm.SHA-1 is very similar to SHA-0, but alters the original SHA hash specification to correct alleged weaknesses.In Data integrity, Source control management systems such as Git and

ISSN NO: 2350-1146 I.F-5.11

Mercurial use SHA-1 not for security but for ensuring that the data has not changed due to accidental corruption.

C. SHA-2

A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size. SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. SHA-1 and SHA-2 are the secure hash algorithms. These also can use within other cryptographic algorithms and protocols, for the protection of sensitive unclassified information.

D. SHA-3

In 2012, NIST selected an additional algorithm, Keccak, for standardization under SHA-3. It supports the same hash lengths as SHA-2, but its internal structure differs significantly from the rest of the SHA family.

E. SHA-512 Algorithm

SHA-512 is a variant of SHA-256 which operates on eight 64-bit words. Preprocessing consists of three steps: padding the message, *M*, parsing the message into message blocks, andsetting the initial hash value, *H(0).*

Step 1: The purpose of the padding is to ensure that the padded message is a multiple of 1024 bits.
Step 2: The message and its padding must be parsed into 1024bit blocks.
Step 3: Set the initial hash value, *H(0).*
For SHA-512, the initial hash value, *H(0),* shall consist of the following eight 64-bit words, in hex:

$H_0^{(0)}$ = 6a09e667f3bcc908 $H_1^{(0)}$ = bb67ae8584caa73b
$H_2^{(0)}$ = 3c6ef372fe94f82b $H_3^{(0)}$ =a54ff53a5f1d36f1
$H_4^{(0)}$ = 510e527fade682d1 $H_5^{(0)}$ = 9b05688c2b3e6c1f
$H_6^{(0)}$ = 1f83d9abfb41bd6b $H_7^{(0)}$ = 5be0cd19137e2179

These words were obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

It is essentially a 512-bit block cipher algorithm to encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe:

1) SHA-512 compression function,
2) SHA-512 message schedule.

Six logical functions are used in SHA-512. Each of these functions operates on64-bit words and produces a 64-bit word as output. Each function is defined as follows:

ROT R28(x) $\oplus$ *ROT R34(x)* $\oplus$ *ROT R39(x)*
Ch(x; y; z) = (x ^ y) $\oplus$ (:x ^ z)
Maj(x; y; z) = (x ^ y) $\oplus$ (x ^ z) $\oplus$ (y ^ z)
$\sum_0(x) = S^{28}(x) \oplus S^{34}(x) \oplus S^{39}(x)$
$\sum_1(x) = S^{14}(x) \oplus S^{18}(x) \oplus S^{41}(x)$
$\sigma_0(x) = S^{1}(x) \oplus S^{8}(x) \oplus R^{7}(x)$
$\sigma_1(x) = S^{19}(x) \oplus S^{61}(x) \oplus R^{6}(x)$
The hash computation proceeds as follows:

For i = 1 to N (N = number of blocks in the padded message)
{

- Initialize registers a; b; c; d; e; f; g; h with the (i-1)st intermediate hash value(Initially hash value fori = 1)

a = $H_0^{(i-1)}$
b = $H_1^{(i-1)}$
:
:
h = $H_7^{(i-1)}$

- Apply the SHA-512 compression function to update registers a; b; : : : ; h (For j = 0 to 79)

{

- Compute Ch(e; f; g), Maj(a; b; c), $\sum_0(a)$, $\sum_1(e)$, and Wj
- T1 = h+$\sum_1(e)$ + Ch(e; f; g) + Kj +Wj
- T2 = $\sum_0(a)$ + Maj(a; b; c)
- *h = g*
- *g = f*
- *f = e*
- *e = d + T* 1
- *d = c*
- *c = b*
- *b = a*
- *a = T*1 + *T*2

}

- Compute the i^{th} intermediate hash value H^i
  - $H_0^{(i)}$= *a* + $H_0^{(i-1)}$
  - $H_1^{(i)}$= b+ $H_1^{(i-1)}$
  - :
  - :
  - $H_7^{(i)}$= *h*+ $H_7^{(i-1)}$

}

$H^N = (H_0^{(N)}, H_1^{(N)}, \ldots, H_7^{(N)})$ is the hash of M.

- SHA-512 message schedule:
  Expanded message blocks W0;W1; : : : ; W79 are computed as follows
  - Wj=$M_i^{(j)}$ for j = 0; 1; : : : ; 15, and
  - For j = 16 to 79

{

- $W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$

}

A sequence of constant words, K0; : : : ; K79; is used in SHA-512. These are given by first sixty-four bits of the fractional parts of the cube roots of the first eighty primes.

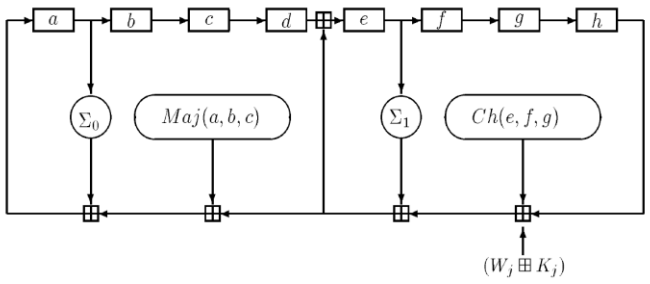

Fig. 8.SHA-512 compression function

ISSN NO: 2350-1146 I.F-5.11

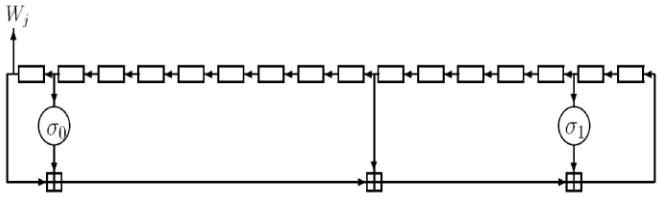

Fig. 9.SHA-512 message schedule

V. DATA CONFIDENTIALITY

Once the user host data to the cloud there should be some guarantee that data accessibility will be given only to the authorized user. Inappropriate access to customer sensitive data by cloud can pose potential threat to cloud data. The user should be assured that the data hosted on the cloud will be confidential. The assurances for the data security can be provided to the clients through proper practices and privacy policies. Also procedures should be in place to prevent data leakage and to provide data safety. Preserving confidentiality is one of the major issues faced by cloud systems, since the user data is stored at a remote location that the Service Provider has full access. There have been some methods of preserving the confidentiality of data stored in the cloud such as data encryption. The cloud seeker should be assured that data hosted on the cloud will be confidential.

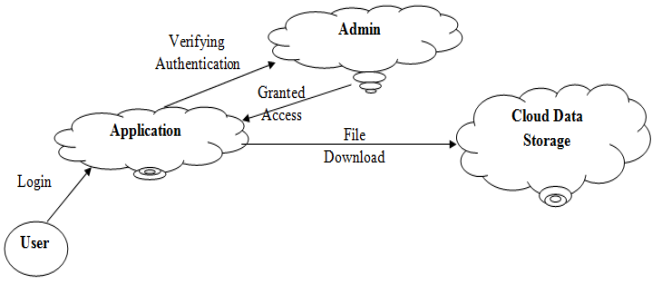

Fig. 10.Data Confidentiality

In order to provide security to the user data, the administrator performs encryption of the uploaded data. After the encryption, the administrator segments the encrypted data and stores at different locations, so that the storage provider even cannot misuse the data. This provides more confidentiality to the userdata. Also the flaws in the application logic will not lead to the data leakage.

1. The user login to access the cloud storage.
2.The administrator performs the authentication verification
3. User requests to upload the data.
4.When the user uploads the data, the administrator encrypts the data using encryption algorithm.
5. If the user wants to download the data, the user requests the administrator to download the file.
6. Administrator first verifies the authority of user then allow access.
7. The encrypted data is sent to the administrator. The administrator performs decryption before sending the data to the user.
8. The data in its original form is sent to user.

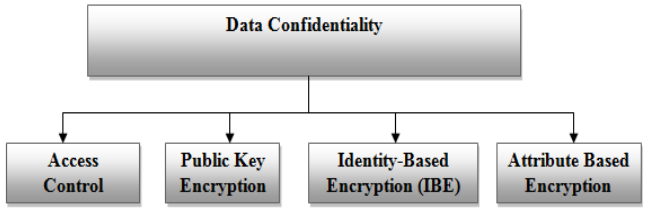

Fig. 11.Data Confidentiality algorithms

A. Access control:

When data is outsourced to the cloud, which is untrusted because it is in a domain where security is not managed by the data owner, data security has to be given more attention. When more than one entity want to share data, there has to be a mechanism to restrict who can access that data. Many techniques have been discussed in the literature[17]. Those techniques were proposed to keep data content confidential and keep unauthorized entity from accessing and disclosing the data by using access control while permitting many authorized entities to share those data. The following are some cryptographic techniques for data confidentiality.

B. Public Key Encryption:

Public key encryption is used to encrypt the data by using the public key. Only the one who has the private key can decrypt this data. This makes data secure and confidentiality is maintained. In [60], Sana et el. proposed a lightweight encryption algorithm by utilizing symmetric encryption performance to encrypt files and utilizing asymmetric encryption efficient security to distribute keys. But here one disadvantage using this method is key management issue and the need to get fine-grained access to file, such part of it. Also,
this solution is not flexible and scalable because encryption and decryption is needed when a user leave the group in order to prevent him from accessing the data.

C. *Identity-Based Encryption (IBE) :*

Shamir, in [61], has introduced identity-based encryption.T he owner of data can encrypt his data by specifying the identity of the authorized entity to decrypt it based on that entitys identity, which must match the one specified by the owner. Therefore, there is no key exchange.

D. Attribute Based Encryption (ABE)

In attribute based encryption, an identity of a user is identified by a set of attributes. This set of attributes generates the secret key. Also, it defines the access structure used for access control. This access control are using encryption to encrypt data for confidentiality and share it among group of users. It is a kind of integrating the encryption with the access control.

VI. CLOUD AVAILABILITY

The data availability mean a process of ensuring that data is

ISSN NO: 2350-1146 I.F-5.11

available to end user at any time, any place from any where. In [53], Fawaz, et al. developed a storage architecture, figure 7 which covers security, reliability, and availability. The underlying technique of their proposed architecture uses a storage method based on RAID 10. They used three server providers and stripped the data to two servers and the partybits in the third server provider. They followed a sequentialway to store the data after encrypting it and dividing the cipher into blocks. One block is in one server provider storage, the next block is in the next server provider storage and the parity bit in the third server provider. A Parity bit can be in any server provider storage while the other in the other server provider storage. In case the two server providers collide to collect the data, each one has, the encryption will protect the data from unauthorized access. In case one server provider service is distributed, by using a parity bit and an available server provider, the service will be available to all without any hit. Also, it is the same in case one service provider corrupts the data. The number of service provider in this storage architecture can be any number.

In [54], a HAIL (High Availability and integrity Layer) is designed to address the threat caused by a service provider being unavailable. A HAIL distributes the data across many cloud providers to keep their service available all the time. A HAIL leverages many cloud service providers to make a solution that is reliable out of unreliable components and it is cost effective. The idea behind the HAIL is inspired by RAID, which is reliable storage made from unreliable storage. The HAIL works when there is corruption. It does not detect the corruption but it remedies it by avoiding this corruption in a subset of storage providers by using the data in the other service provider storage.

In [55], Bessani et al. proposed Depsky which uses many clouds to build a cloud-of-clouds to address two security requirements in their storage system, which are confidentiality and availability of data. They combined the byzantine quorum protocol as well as secret sharing cryptographic and erasurecodes.

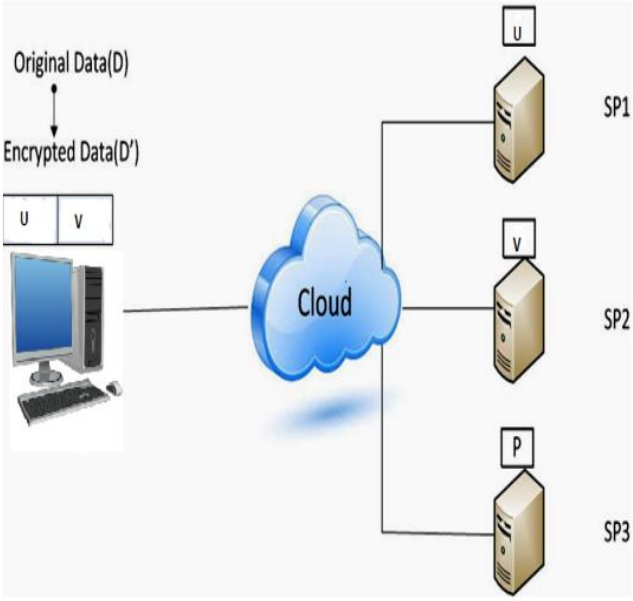

Fig. 12.Data availability algorithms

VII. CLOUD RELIABILITY

Cloud Service Reliability, which is defined as theprobability that a cloud service under consideration can be successfully completed for a user in aspecified period of time. In particular, this requires that the job request be successfully served bythe schedulers in time, the set of subtasks contained by the service be completed, the computing/data resources required by the subtasks be available; and the network be operational during the communications. While providing service there are two types of failure can occurs

1. *Request Stage Failures:* Overflow and Timeout.
2. *Execution Stage Failures:* Data resource missing, Computing resource missing, Software failure, Database failure, Hardware failure, and Network failure.

Therefore the cloud reliability can be calculated depending on these two attributes as modelling of Request Stage Reliability and modelling of Execution Stage Reliability.

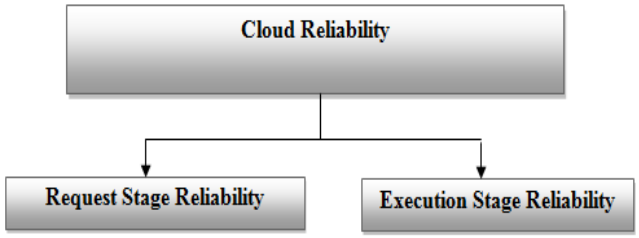

Fig. 13.Data Reliability algorithms

A *Request Stage Reliability*

This request stage contains two types of failures: overflow and timeout. The *due time* for a specific service is the allowed time spent from the submission of the job request to the completion of the job. The due time can be set by the user or by the service monitor. If a job request is not served by a scheduler before the due time, it will be dropped. If the waiting time is longer than the due time d T , the timeout failure occurs. Therefore if the failure not occurs the Request Stage is reliable.

B *Execution Stage Reliability*

To address various types of failures during the execution of a cloud service, [18] propose a new model as shown in figure.

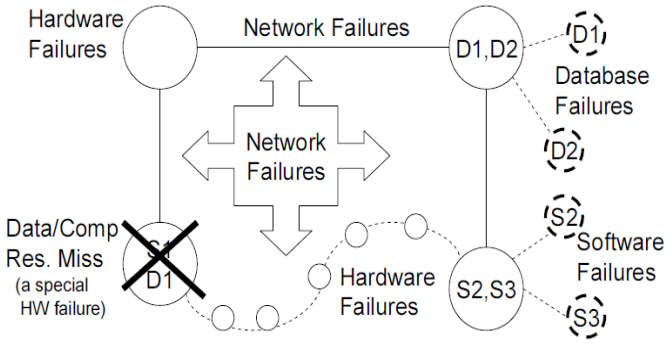

Fig. 14.Execution Stage Reliability

They further present a new algorithm for evaluating the overall cloud servicereliability considering all different factors during the execution stage given the new graph model

and the above parameters. The new evaluation algorithm based on Graph theory and Bayesiantheorem is presented to derive the reliability.

A. Minimal Subtask Spanning Tree (*MSST*)

B. Minimal Execution Spanning Tree (*MEST*)

Finally, if a cloud service needs to be successfully completed, both request stage andexecution stage should be reliable. After we derive the reliability for both stages, we can get the cloud service reliability ServiceR as

$$R_{\text{Service}} = R_{\text{request}} + R_{\text{execute}}$$

VIII. CONCLUSION

The objective of this paper is to study the cloud computing, types of cloud computing and its characteristics .Cloud computing is growing technology so it also comes with some security issues. Those issues can be storing data in a remote server leads to some security issues. Issues are also related to confidentiality of data from unauthorized people in remote sites, integrity of stored data in remote servers and the availability of the data when it is needed. Also, sharing data in cloud when the cloud service provider is mistrusted is an issue. However, we mentioned some techniques that protect data seen by the cloud service provider while it is shared among many users. Many studies have been conducted to discover the issues that affect security, integrity, confidentiality, availability and reliability of data and to find a solution for them. Those solutions will lead to more secure cloud storage, which will also lead to more people trust on the cloud data and service.

REFERENCES

[1] MaximillianoDestefaniNeto "A brief history of cloud computing", Cloud computing news online.

[2] "Cloud computing " online on Wikipedia.

[3] William Stalling,"Cryptography and Network Security-Principles and Practices", book, Page 314-328.

[4] "Blowfish Algorithm " online on Wikipedia.

[5] Tanjyot Aurora1, Parul Arora2. (2013). "Blowfish Algorithm". International Journal of Computer Science and Communication Engineering IJCSCE.

[6] MsNehaKhatri – Valmik1, Prof. V. K Kshirsagar2 .(March-April 2014)." Blowfish Algorithm".*IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2.www.iosrjournals.org*

[7] AviKakLecture Notes on "Computer and Network Security".

[8] Nareshvurukonda, B.ThirumalaRao, (ICCC-2016)"A Study on Data Storage Security Issues in Cloud Computing". 2nd International Conference on Intelligent Computing, Communication & Convergence.

[9] "RSA Algorithm " online on Wikipedia.

[10] AkashdeepBhardwaj, GVB Subrahmanyam, VinayAvasthi, HanumatSastry, "Security Algorithms for Cloud Computing", *ScienceDirect ELSEVIER, journal Procedia Computer Science 85*, 2016,pp. 535 – 542.

[11] PriyadarshiniPatil, PrashantNarayankar, Narayan D G, Meena S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish.", *International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015,Nagpur, INDIA*. ScienceDirect ELSEVIER 2016, pp 617-624.

[12] K.Devika, M.Jawahar, " Review On: Cryptographic Algorithms for Data Integrity Proofs in Cloud Storage",*International Journal of Engineering Trends and Applications (IJETA)* – Volume 2 Issue 1, Jan-Feb 2015, pp. 14-19.

[13] RajatSaxena∗and SomnathDey, "Cloud Audit: A Data Integrity Verification Approach for CloudComputing",*ScienceDirect ELSEVIER*, Twelfth International Multi-Conference on Information Processing-2016.

[14] NikolayNikolova,∗, Alessandro Rossinia, KyriakosKritikosb, "Integration of DSLs and migration of models:a case study in the cloud computing domain",*ScienceDirect ELSEVIER*,Procedia Computer Science 68 (2015) 53 – 66.

[15] DilliRavilla, Chandra Shekar Reddy Putta, "Enhancing the Security of MANETs Using Hash Algorithms", *Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015). ScienceDirect ELSEVIER journal*, 2015, pp 196-206.

[16] Piyush Gupta, Sandeep Kumar, "A Comparative Analysis of SHA and MD5Algorithm", Piyush Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4492-4495.

[17] M Sulochana1 ,OjaswaniDubey, "Preserving Data Confidentiality using Multi-Cloud Architecture",*ScienceDirect ELSEVIER*Procedia Computer Science 50 (2015) 357 – 362.

[18] Sultan Aldossary,William Allen, "Data Security, Privacy, Availability and Integrity inCloud Computing: Issues and Current Solutions",*(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 4, 2016*

[19] Eric Bauer Randee Adams, "RELIABILITY AND AVAILABILITY OF CLOUD COMPUTING", IEEE IEEE PRESS ©WILEY A JOHN WILEY & SONS, INC., PUBLICATION

[20] Yuan-Shun Dai * a c, Bo Yang b, Jack Dongarra a, Gewei Zhang, "Cloud Service Reliability: Modeling and Analysis" , University of Tennessee, Knoxville, TN, USA