IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. II (Mar – Apr. 2015), PP 59-66
www.iosrjournals.org

A Secure Framework for Cloud Computing With Multi-cloud Service Providers

Monali Shrawankar, Prof. Mahendra Sahare
NRI Institute of Information Science and Technology Bhopal, (MP) India
NRI Institute of Information Science and Technology Bhopal, (MP) India

Abstract: *Cloud computing conveys IT assets as a Service over web. The point of interest of cloud computing is everlasting anyway it brings a ton of issues together with security. ensuring the security of cloud computing may be a premier consider the computing climate, as clients generally store touchy data with cloud storage suppliers, however these suppliers could likewise be untrusted Customers don't have to lose their delicate data attributable to malignant insiders and programmers inside the cloud. Furthermore, the loss of administration accessibility has created a few issues for an oversized scope of as of late. Information interruption system create a few issues for the clients of distributed computing. The inverse issues like data burglary, data lost should be overcome to supply higher administrations to the customers. It's resolved that the investigation into the occupation of intercloud suppliers to deal with security has gotten less consideration from the examination group than has the livelihood of single mists. Multi-cloud environment has capacity to scale back the dangers further on the grounds that it will verify the security and responsibleness. We tend to propose protection and security to cloud clients with less calculation cost and most astounding security. Amid this paper, we've made a framework to give secure cloud data which will promise to stop security dangers confronting the cloud computing group. This schema connected multi-clouds furthermore the blowfish algorithm to scale back the chance information interruption furthermore the loss of administration accessibility inside the cloud and assurance information honesty. By using that Multi-cloud architecture we tend to actualize cryptography and coding of client data with 2 real clouds dropbox and cloudme. We tend to propose Blowfish algorithm as partner in nursing sample of hearty security framework with higher execution as an occurrence the anticipated multi-cloud schema.*

Keywords: *Cloud computing; single cloud; multi-clouds; cloud storage; data integrity; data intrusion; service availability.*

I. Introduction

1.1 CLOUD COMPUTING

Cloud computing can be depicted as the moving of enlisting assets like get ready force, framework and limit assets from desktops and limited servers to significant data focuses encouraged by associations like Amazon, Google, Microsoft et cetera. These profits are given to a customer or business on exceedingly adaptable, adaptable and pay-as-you-use premise. Figure 1. shows a consistent dispersed registering structural building. The two most crucial portions of disseminated registering building outline are:

1) Front end
2) Back end

The Front end is the part seen by the client i.e. the machine client. This incorporates the client's cross segment and the sections used to get to the cloud by method for a customer interface, for instance, a World Wide Web program. The Back end of the disseminated registering structural arranging is the "cloud" itself, including grouped machines servers and data stockpiling contraptions. As showed in Fig.1, The cloud incorporates levels for the most part the back-end levels and the front –end or client –end levels. The front-end levels are the ones you witness and join with when you get to your web message on Gmail for example. You are utilizing ventures running on the front-end of a cloud. The same is genuine when you get to your face book account. The Back-end incorporates the fittings and programming development demonstrating that invigorates the interface you sight front end. Since the machines are arranged up to work at the same time, the applications can exploit all that enlisting power just as they were running on one particular machine.

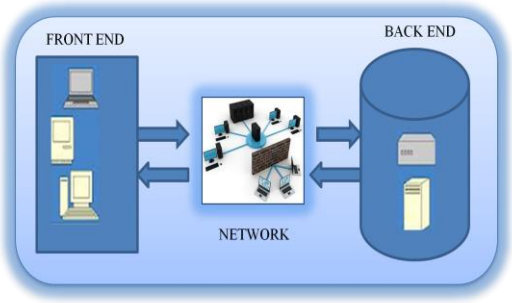

Figure 1. Cloud computing architecture

Cloud computing additionally allows for a ton of adaptability, relying on the interest, you can help how a great part of the cloud resources you use without the requirement for allocating particular equipment for the occupation or simply diminish the recompense of advantages apportioned to you when are not vital. Cloud administration suppliers ought to guarantee the clients' administration base. The utilization of distributed computing Subashini and Kavitha [1] contend administrations for various reasons including in light of the fact that this administration supply quick get to the applications and lessening administration charges. Cloud computing suppliers ought to address security and security as issue for higher and dire primary concerns. The considering with "single cloud‟ providers[13] is advancing less famous administration with clients because of guarantee troubles, for example, administration availability disappointment for quite a while and pernicious insider's assaults in the single cloud. So now single cloud move towards multi clouds, ‟interclouds‟ or" billow of clouds.

1.2 The Proposed Objective

This paper proposed a model which first checks trustworthiness of clients information utilizing Byzantine fault tolerance algorithm and discover flaw cloud in multi-cloud building design. In the wake of getting trustworthiness acceptance it applies encryption and unscrambling to client information with cloud storage suppliers. So once the information is put away in the application it is get scrambled and transferred to cloud storage supplier in encoded structure. This encoded information won't be available to outside clients. Therefore the capacity of the information will be in the encoded arrangement and the heads and the staffs have no learning about the scrambled keys and the storage suppliers of the encryption and decryption.

1.3. Proposed Objective Discussion

In cloud computing, the information will be put away given by storage suppliers. They must have a feasible approach to secure their customers' information, particularly to keep the information from revelation by unapproved insiders. Putting away the information in encoded structure is a typical technique for data security insurance. In the event that a cloud framework is in charge of both errands on capacity and encryption/decryption of information, the framework heads might at the same time acquire scrambled information and decoding keys. This permits them to get to data without approval and accordingly represents a danger to data protection.

1.4 Applied Methodology

To apparatus the proposed band-aid of the botheration that is getting taken affliction of in this a priorism work, the afterward alignment is used:

• To assay the assorted absolute Security Algorithm and acquisition their strengths and weakness by the abstract survey.

• To analyze the absolute techniques.

• A defended multi-cloud archetypal for billow accretion based on the abstraction of amid the encryption and decryption account from the online accumulator service.

II. Literature Review

Cloud computing is one of the fastest growing articulation of IT industry today .Companies are more application Cloud computing for their business. Cloud computing has become a above allotment in today's IT sector. They charge to assurance the Cloud provider that their advice will not be misused. With Cloud users and companies are common victims of hacking and abstracts loss. Hence It is all important to assay the aegis issues in Cloud computing and accomplish it defended and safe. [4]

2.1. Data Privacy In The Cloud

In the Cloud computing environment, the accessories acclimated for business operations can be busy from a individual account provider forth with the application, and the accompanying business abstracts can be stored on accessories provided by the aforementioned account provider. Storing the company's abstracts on the account provider's accessories raises the achievability that advice may be break appear to others. Some advisers accept appropriate that user abstracts stored on account provider's accessories accept to be encrypted. However, if the decryption key and the encrypted abstracts are captivated by the aforementioned account provider, the high-level administrators aural the account provider would accept admission to both the decryption key and encrypted data, appropriately presenting a accident for the crooked acknowledgment of the user abstracts and may actualize vulnerability to clandestine data.

2.2. Existing Methods For Protection

In absolute Cloud computing mechanisms, client's data is encrypted afore storage. Applicant affidavit action occurs above-mentioned to accumulator or retrieval. All the advice channels are encrypted for defended data transmission. Common data encryption methods cover symmetric (private or secret key encryption) and asymmetric (public key encryption) cryptography algorithms. In case of symmetric cryptography a secret key is acclimated for both encryption and decryption. In the added duke asymmetric key cryptography uses two altered keys, "public key" for encryption and "private key" for decryption. Some of the symmetric key algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3-DES), and Advance Encryption Standard (AES) [3] etc. asymmetric key algorithms are RSA cryptography [4] and Elliptic Curve Cryptography (ECC) [5]. Countersign affidavit is a accepted affidavit action acclimated by every cloud service provider (CSP). During registration, applicant gives own user id and countersign and these will abundance anon in countersign book of database.

III. Proposed Methodology

3.1 Proposed System Architecture

Figure 2. Is an overview of the architectonics where storage and encryption/decryption/hash casework (security services) are separated. For example small and medium calibration business who ambition to abundance all its annual accompanying data in cloud storage, will aboriginal account the assortment of the data, encrypt the data application encryption account and again abundance the data storage provided by service provider. The arrangement a swell provides functionality area added users from baby calibration business Company will be able to admission abstracts which is stored in cloud storage. The sessions amid applicant and security server is anchored application Key and Blowfish as the encryption algorithm.

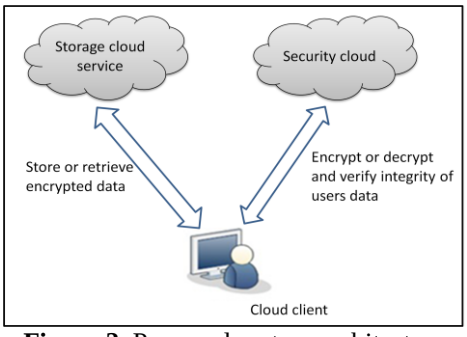

Figure 2. Proposed system architecture

3.2 Proposed Algorithm

This security framework for Cloud Computing is based on two algorithms. The concept uses multi-clouds for security purpose so four CSPs are designed for every cloud client to transfer data from one CSP to another.

3.2.1 Algorithm-I: Integrity verification with Byzantine fault tolerance algorithm

This algorithm (BFT) provides safety and liveness over an multi-cloud model.

a) **Safety:** the system maintains state and looks to the client like a non-replicated remote service. Safety includes a total ordering of requests.

b) **Liveness:** clients will eventually receive a reply to every request sent, provided the network is functioning.

It is based on state machine replication and messages signed by public key cryptography. Message digests created using collision-resistant hash functions and uses consensus and propagation of system views: state is only modified when the functioning replicas agree on the change

- For n clients, there are n 'views', {0..n-1}.

- In view i, node i is the primary node
- View change is increment mod n
- View change occurs when 2f nodes believe the primary has failed
- Guaranteed safety and liveness provided less than $\frac{n-1}{4}$ = f replicas have failed.
- **Step 1:** The client sends a request to the primary cloud.
- **Step 2:** The primary assigns the request a sequence number and broadcasts this to all replicas (pre-prepare).
- **Step 3:** The replicas acknowledge this sequence number (prepare).
- **Step 4:** Once 2f prepares have been received, a client broadcasts acceptance of the request (commit).
- **Step 5:** Once 2f +1 commits have been received, a client places the request in the queue.In a non-faulty client, the request
- queue will be totally ordered by sequence number.
- **Step 6:** Once all prior requests have been completed, the request will be executed and the result sent directly to the client.
- **Step 7:** All these messages are logged.[10]

3.2.2 Algorithm-II: Encryption and decryption with Blowfish algorithm
Blowfish uses a ample amount of subkeys. These keys have to be precomputed afore any abstracts encryption or decryption. The A-array consists of 18 32-bit subkeys : A1, A2,..., A18. There are four 32-bit S-boxes with 256 entries 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.
Encryption: Blowfish is a Feistel arrangement consisting of 16 circuit
The ascribe is a 64-bit abstracts element, x.
Divide x into two 32-bit halves: xL, xR
For i = 1 to 16:
xL = xL XOR Ai
xR = F(xL) XOR xR
Swap xL and xR
Swap xL and xR (Undo the endure swap.)
xR = xR XOR A17
xL = xL XOR A18
Recombine xL and xR
Function F (): Divide xL into four eight-bit quarters: a, b, c, and d F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232 Decryption is absolutely the aforementioned as encryption, except that A1, A2,..., A18 are acclimated in the about-face order. Implementations of Blowfish that crave the fastest speeds should disclose the bend and ensure that all sub keys are stored in cache.
The subkeys are affected application the Blowfish algorithm. The exact adjustment is as follows:
Initialize aboriginal the P-array and again the four S-boxes, in order, with a anchored string. This cord consists of the hexadecimal digits of pi (less the antecedent 3).
For example:
A1 = 0x243f6a88
A2 = 0x85a308d3
A3 = 0x13198a2e
A4 = 0x03707344
XOR A1 with the aboriginal 32 $.25 of the key, XOR A2 with the additional 32-bits of the key, and so on for all $.25 of the key (possibly up to A14). Repeatedly aeon through the key $.25 until the absolute A-array has been XORed with key bits. (For every abbreviate key, there is at atomic one agnate best key; for example, if A is a 64-bit key, again AA, AAA, etc., are agnate keys.)
Encrypt the all-zero cord with the Blowfish algorithm, application the subkeys declared in accomplish (1) and (2). Replace A1 and A2 with the achievement of footfall (3).
Encrypt the achievement of footfall (3) application the Blowfish algorithm with the adapted subkeys.
Replace A3 and A4 with the achievement of footfall (5) Continue the process, replacing all entries of the A-array, and again all four S-boxes in order, with the achievement of the continuously-changing Blowfish algorithm. In total, 521 iterations are appropriate to accomplish all appropriate subkeys. [8]

IV. Implementation Review

The concept is based on checking data integrity and encryption/decryption of user data, as shown in Figure 3. In this model, two modules are designed for double security purposes. First module named as Integrity verification module which uses Byzantine fault tolerance algorithm. Second module named as Encryption/decryption module which uses blowfish algorithm with real clouds as dropbox and cloudme. Both these clouds are online storage clouds where cloud users can store their data in a secured manner.

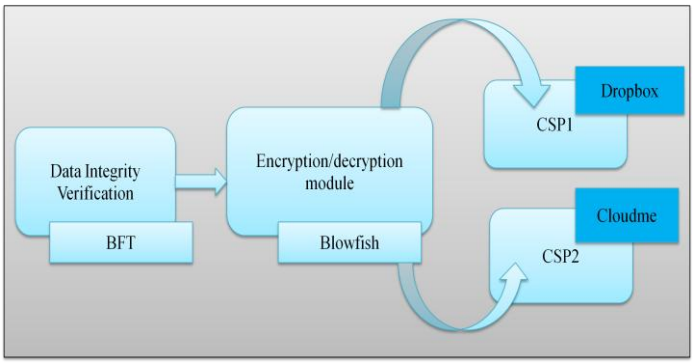

Figure 3: Workflow of a proposed architecture

4.1 Data Retrieval From Cloud Service Provider

When a user wants to access the online Cloud Service, accept to aboriginal assassinate the Login Program as apparent in step 1. This step can use accepted e-commerce or added casework which accept already deeply absolute the user's registration, such as symmetric key-based claiming and acknowledgment login verification, or through a One-Time Password. After the user's login has been auspiciously verified, if the System requires applicant advice from the user, it sends a appeal for advice to the Storage Service System, as apparent in step 2. In this step, the System transmits the user ID to the Storage Service System area it searches for the user's data. This data is encrypted so, already found, a appeal accept to be beatific to the Encryption/Decryption Service System forth with user ID. step 3 shows the Storage Service System active the manual of encrypted applicant data and the user ID to the Encryption/Decryption Service System. Since the Encryption /Decryption Service System can serve assorted users and the encryption/decryption for anniversary user's data requires a different key, accordingly user's different ID and keys are stored together. Therefore, in step 4, the Encryption/Decryption Service System uses the accustomed user ID to basis the user's data decryption key, which is again acclimated to break the accustomed data. Using the actual decryption key to break the data is analytical to abating the data to its aboriginal state. After the Encryption/Decryption Service System has decrypted the client's data, in step 5 the decrypted user data is provided in step 6, commutual the Data Retrieval Program.

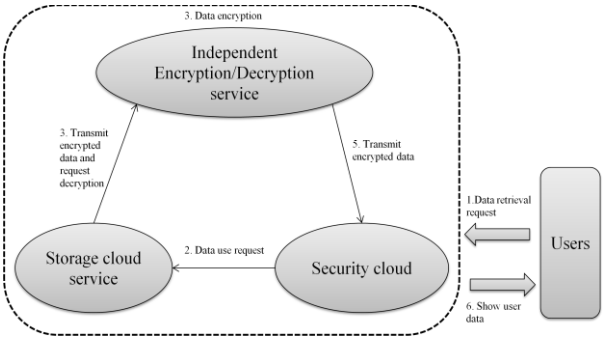

Figure 4: Data Retrieval from Cloud Service Provider

Next, we describe the Data Storage Program, as shown in Fig. 5. This program also involves the collaboration of three cloud service systems: Security cloud, Encryption/Decryption Service System, and Storage Service System.

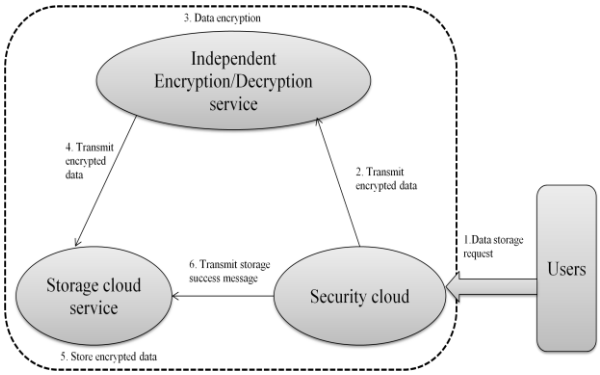

Figure 5: Data storage diagram

Step 1 of Fig. 5 shows the client sending a Data Storage Request to the security cloud which then initiates the Data Storage Program, requesting data encryption from the cryption/Decryption Service System as shown in Step 2. In Step 2, the security cloud and the Encryption/Decryption Service System establish a secure data transfer channel to transmit the user ID and the data requiring storage from the security cloud to the Encryption/Decryption Service System.

V. End Results & Upshot

This section illustrates the highest outcome & upshots that square measure bought with the aid of jogging the procedure victimization absolutely one-of-a-kind information plenty. The results exhibit nevertheless understanding is secure in Cloud service supplier facet atmosphere. Following determine illustrate cloud client browse understanding which is ready to get keep on cloud service provider.

Figure 6: cloud client browse data

Once the data is browsed then byzantine fault tolerance algorithm is applied to check data integrity as illustrated in figure

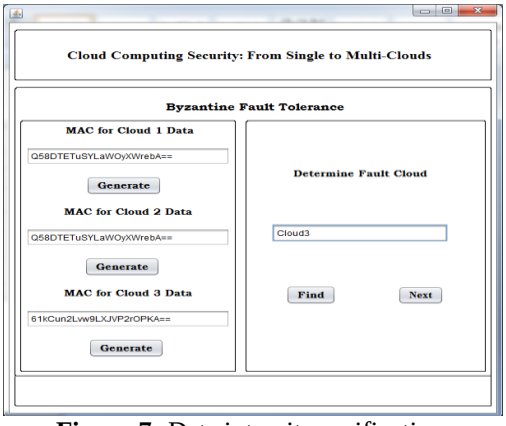

Figure 7: Data integrity verification

Once the default cloud found, then blowfish algorithm applied to data to encrypt and upload on csp1 i.e; dropbox cloud service provider as illustrated in figure.

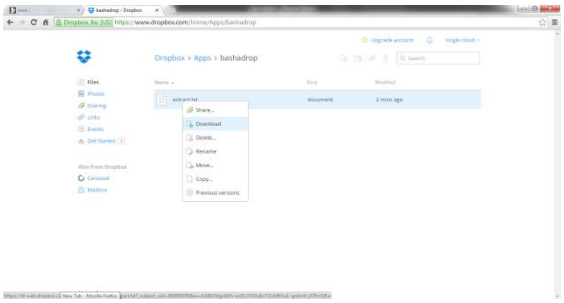

Figure 7: Encrypted Data in CSP1 as Dropbox real cloud

Again applying BFT algorithm, data integrity verified. then blowfish algorithm applied to data to encrypt and upload on csp2 i.e; cloudme cloud service provider as illustrated in figure.

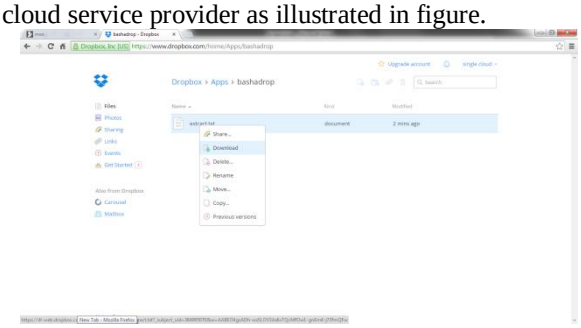

Figure 8: Encrypted Data in CSP2 as Cloudme real cloud

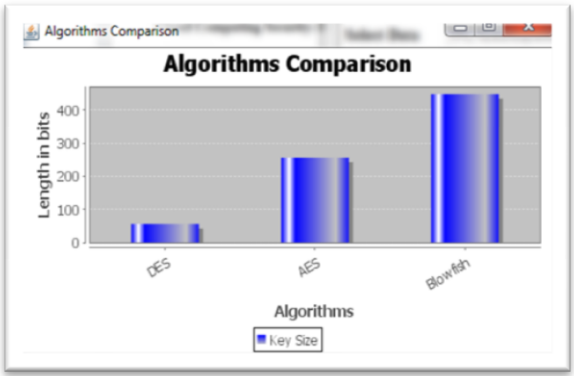

Figure 9: Comparison length in bits for various common symmetric encryption algorithms for Cloud Computing

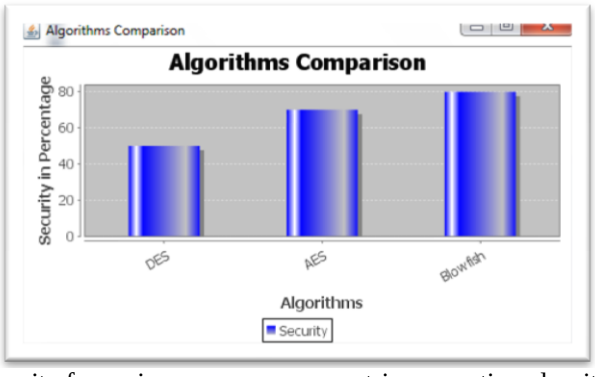

Figure 10: Comparison security for various common symmetric encryption algorithms for Cloud Computing

Table 1. Comparison Of Blow-Fish With Different Algorithm In Cloud Computing

Algorithm	Data	Time(In Seconds)	Average MB/Sec	Performance
DES	256 MB	10-11	22-23	Low
3DES	256 MB	12	12	Low
AES	256 MB	5	512	Medium
Blowfish	256 MB	3.5-4	64	High

VI. Conclusion

It's clear that whereas the use of cloud computing has rapidly developed; cloud computing protection is still considered the main matter in the cloud computing traditional atmosphere. Customers don't need to misplace their private knowledge as a final result of malicious insiders within the cloud. In supplement, the slash of provider availability has initiated many difficulties for a significant quantity of purchasers lately. In addition, data intrusion directs to numerous problems for the customers of cloud computing. In this paper, we have now proposed answers for three most trendy safety threats in cloud storage. We now have confirmed that our approach performs better in decreasing the safety threat on cloud For cloud computing to unfold, customers need to have a high degree of believe in the methods by which provider providers guard their knowledge. This learn proposes a Multi-cloud model for Cloud Computing situated on a Separate Encryption and Decryption service, emphasizing that authorization for the storage and encryption/decryption of user information must be vested with two distinctive carrier providers. On this new model, person knowledge in the Storage provider method is all saved encrypted. Without the decryption key, there is no approach for the provider supplier to access the consumer information. Inside the Encryption/Decryption provider approach there is not any stored consumer data, hence removing the probability that person data probably improperly disclosed.

VII. Future Scopes

The info storage security in Cloud Computing, an area stuffed with challenges and of paramount significance, are nonetheless in its infancy now, and plenty of research problems are yet to be identified is to enhance the extra protection points by using making use of different stronger systems of data protection via cryptosystems and other approaches. Cloud computing does provide us with tangible advantages however today we still haven't any definite solutions on a proper protection platform for cloud computing, best recommendations and theories are being fashioned but we're but to see a practical protection measure for cloud computing to be a safer platform for businesses and members.

References

[1]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.
[2]. “Cloud security An enterprise perspective” Hewlett-Packard Development Company, L.P. The information, 2012. Available from https://h30613.www3.hp.com/media/files/.../BB237 _Nielson.pdf
[3]. O.P. Verma, “Performance analysis of data Encryption Algorithm”, IEEE 3rd International Conference on Electronics Computer Technology (ICECT), vol.5, April 2011, pp. 399-403.
[4]. R. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM, vol. 21, No.2, 1978, pp. 120-126.
[5]. Miller, “Uses of elliptic curves in cryptography”, Advances in cryptology-CRYPTO ’85, Lecture Notes in Computer science, 1986, pp. 417- 426.
[6]. M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111
[7]. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
[8]. Atul Kahate “Cryptography and Network Security”, Tata Mc-graw Hill, 3rd Edition 2008
[9]. ”Cloud computing security: From Single to Multi-clouds”, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia. Mohammed A. AlZain, Eric Pardede, Ben Soh,James A.
[10]. G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K. Reiter, "Efficient Byzantine-tolerant erasure-coded storage",DSN'04: Proc.Intl. Conf. on Dependable Systems and Networks,2004, pp.1-22.