International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 4 Issue 4, April 2015

Cloud Computing Security: From Single Cloud to Multi-Clouds using Digital Signature

Sayali S. Satav Student
Ganesh Prajapati Student
Sonali Dahiphale Student
Sadhana More Student
Prof.N Bogiri Guide

K.J College Of Engineering And Management Research, Pune.

Abstract—

Cloud Computing is emerging technology which consist of existing techniques combined with new technology paradigms. Main aim of cloud computing project is to store the important data from cloud. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently.
In this survey paper recent research related to single and multi-cloud security and addresses possible solutions. This paper in the data storage we can provide the security using digital signature from single cloud to multi cloud. Here the data will be store in the encrypted format of the cloud, while downloading the data user known the digital signature to the data, otherwise it gate download data in encrypted format.

Index Terms— Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, service, Availability, DepSky System, RSA, Encryption, Digital signing, Decryption.

INTRODUCTION

Cloud computing is the concept of using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources. Cloud provides two main services: storage and computation The concept of cloud computing is linked closely with those of IaaS (Infrastructure as a Service); PaaS (Platform as a Service), SaaS (Software as a Service) and collectively *aaS (Everything as a Service) all of which means a serviceoriented Architecture They maintain database and applications for the user(s) at some remote server and provide independence of accessing them from any place through a network. These concerns origin from the fact that sensitive data are stored and processed in public clouds, which are operated by commercial service providers and shared by various other customers[15][14]. Data confidentiality is a desired property when users outsource their data storage to public cloud service providers. To protect users' data, encryption is used to secure the data in the Cloud Security [18] is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution.With the fast development of wireless technology, mobilecloud has become an emerging cloud service model , in which mobile devices and sensors are used as the information collecting and processing nodes for the cloud infrastructure.[18] Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds","intercloud" or "cloud-of-clouds".[2]

Problem statement:-
The main goal of this article is to provide the security of the data which is store in cloud and to take the backup of the data retrieve of the data using digital signature.

Background:-
The distinction between these classes is more easily identifiable by analyzing the definition of the essential cloud computing characteristics proposed by the NIST (National Institute of Standards and Technology) in , which also introduces the SPI model for services (SaaS, PaaS, and IaaS) and deployment (private, public, community, and hybrid). Cloud computing is the best solution for providing a flexible, on-demand, and dynamically scalable computing infrastructure for many applications In case of private cloud environment access is limited to a group of users or an organization In private cloud the Access, Identity and secured data storage becomes essential to address. It uses Digital Certificates as the main fundamental protection scheme[5][8].Encryption is the conversion of data into encrypted form called a cipher text that cannot be easily understood by unauthorized person and can be decrypted by the authorized person having a valid decryption key. Apart from this, the model positively handles the security issues by employing strict authentication parameters, like login-id and password.

Cloud Computing Overview

Definitions:-

What is Cloud Computing?[9]
Cloud computing is a way of leveraging the Internet to consume software or other IT services on demand. Users share processing power, storage space, bandwidth, memory,

ISSN: 2278 – 1323

and software.[1] With cloud computing, the resources are shared and so are the costs.

In Cloud Computing Components

Types of Cloud

Cloud computing is typically classified in two ways
1. Location of the cloud computing
2. Type of services offered

Location of the cloud

Cloud computing is typically classified in the following ways:

1. Public cloud: In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendor's premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations. [2]

2. Private cloud: The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds[2],[4]. Private clouds are of two types: On-premise private clouds and externally hosted private clouds.

3. Hybrid cloud Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. [6]

4. Community cloud involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California

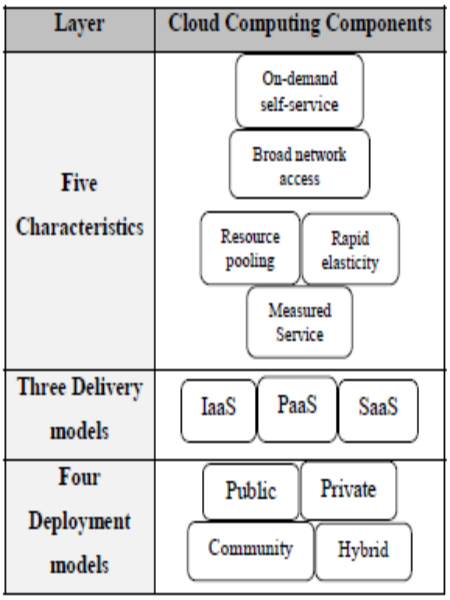


Fig1. layers model of cloud

This model represents the third layer in the cloud environment architecture.

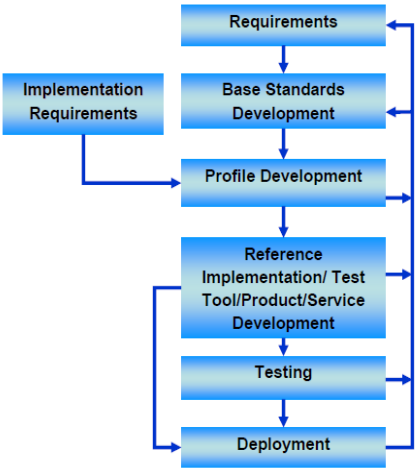


Fig2. Life cycle of the cloud in IT standared.

Asymmetric Algorithms :-

RSA :-The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption.

Algorithm

Key Generation: KeyGen(p, q)
Input: Two large primes – p, q
Compute n = p . q
φ (n) = (p - 1)(q - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)
Key:
public key = (e, n)
secret key= (d, n)
Encryption:
c = me mod n

where c is the cipher text and m is the plain text.RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying thecipher texts. The result of the operation will be the cipher text of the product.

Given ci = E(mi) = mi
e mod n, then
(c1 . c2) mod n = (m1 . m2)e mod n.

Digital Signatures with RSA Encryption Algorithm

In cloud computing where resources are shared and provided to the users. Security plays an important role in cloud paradigm. In case of IT infrastructure public cloud leads to the sharing of computing resources with other companies as well. Here is the risk of data or any other important asset, the risk of seizure[13][16]. Cloud computing makes use of virtualization where data and resources are stored in a virtual environment. Users will not know exact location of data or other source of data. To ensure data storage safety Confidentiality Integrity and Availability (CIA) should be provided. To extend further safeguards of data and its access encryption schema should be provided along with backup and auditing [2].

ISSN: 2278 – 1323

Digital signatures

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance [2] [17].

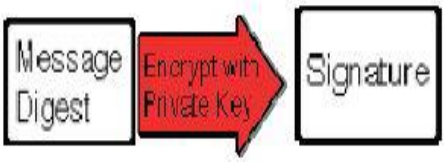


Fig.3 Encryption of message digest signature

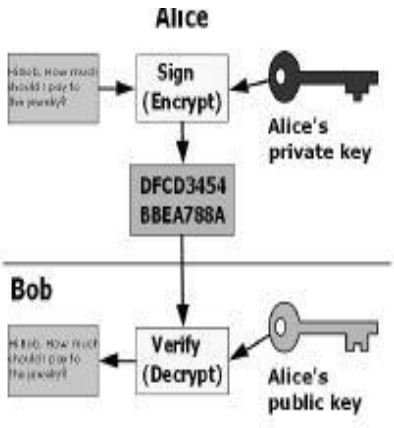


Fig.4 Encryption of Digital Signature into cipher text

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender[5][7][13].Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything represent able as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol [17].

RSA algorithm

RSA is most widely used public key algorithm over internet RSA is capable of supporting encryption and digital signatures. RSA gets its security by integer factorization problem. RSA is relatively very easy to understand and implement [10].

Today RSA is used worldwide to encrypt the data which is confidential and RSA gives best security policy that's why all the service providers such as gmail, hotmail, mediafire etc. are using RSA algorithm to ensure their users full of confidentiality.

Proposed algorithm

Step 1. Key Generation

Declare e as encryption exponent and d as decryption exponent.

p,q <-Integer numbers.
n <-Modulus for keys.
Ø (n) <-Euler"s Totient.
e <-Public key exponent.
Step 2. Compute Values
2.1 Choose two distinct large prime numbers p &q (Random prime no generation algorithm).
2.2 Compute n=p*q
2.3 Compute Ø(n)=(p-1)(q-1)
2.4 Choose e such that 1<e< Ø(n)
2.5 Compute d*e=1
2.6 Public key is (n,e),private key is (n,d)
Step 3. Digital signing
3.1 Sender A create message digest of information using hash function (MD5)
3.2 Hash Function:
3.2.1 Declare character „str of unsigned long type.
3.2.2 Declare & initialize hash of unsigned integer type.
3.2.3 Unsigned int hash=0
int q.
while (q=str+1)
hash=hash+q;
3.3 Represent this digest as integer m& it is having value between 0 to n-1
3.4 Uses private key (n,d) to compute the signature
S=md mod n
3.5 Send signature S to the recipients
Step 4. Encryption
4.1 Sender A obtain receiver B"s public key (n,e)
4.2 Plaintext message as integer m
4.3 Compute ciphertext c=me mod n
4.4 Sends this message (ciphertext) to B
Step 5. Decryption
5.1 Uses his private key (n,d) to compute m=cd mod n
5.2 Extract plain text
Step 6. Signature verification
6.1 Receiver uses senders public key (n,e) to compute V=Se mod n
6.2 Extract message digest from integer V
6.3 Independently computes the message digest of the information that has been signed
6.4 If both are identical the signature is valid
Download the data

ISSN: 2278 – 1323

System architecture of MD5

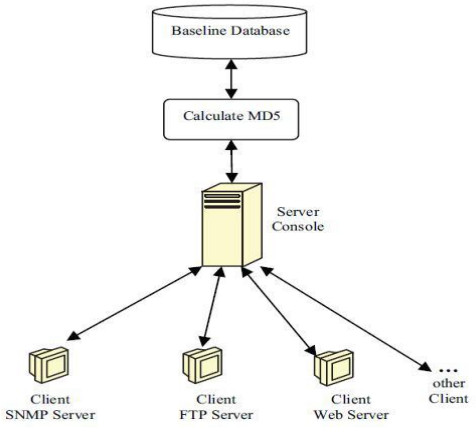


Fig.5 MD5

What is a message-digest algorithm(MDA)?

A message-digest algorithm is also called a hash function or a cryptographic hash function. It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a hash value, a fingerprint or a message digest. When all of the above properties are satisfied, we call the algorithm a collision-resistant message-digest algorithm.[4] It is unknown whether collision-resistant message-digest algorithm can exist at all.

For convenience, we describe the algorithm through the following five steps:

(a)Add padding bits behind the input message

(b)Add a 64-bit binary-string which is the representation of the message's length

(c)Initialize four 32-bit values

(d)Compress every 512-bit block

(e)Generate the 128-bit output

III. PROPOSED WORK

In this proposed work we want to secure our data in cloud. Because Security is the major issue which is faced by every user. Consider an organization where their are number of Employees(Users) are working. Each User has its own LOG IN ID and PASSWORD where they can store their data and all the organization is managed and operated by ADMIN. With the help of RBAC Admin restrict the system from unauthorized access because their are number of restriction to downloads the files of cloud with every user . If any unauthorized user wants to access the data due to downloading restriction they can effect some files rest of files will be saved.[11] RBAC helps to secure our data in Cloud. Secondly, Blowfish helps to encrypted the data and RSA works on these encrypted data and generate the public key and private key. Public key will be generated with every file and Private key helps to generate the digital signature which is required for downloading time.[8] This Digital Signature will be accessed by user via mail. It also provides a better storage and security technique over Cloud architecture.

Admin: In an organization, admin create roles for users & also specify the number of transactions per user as per their role.

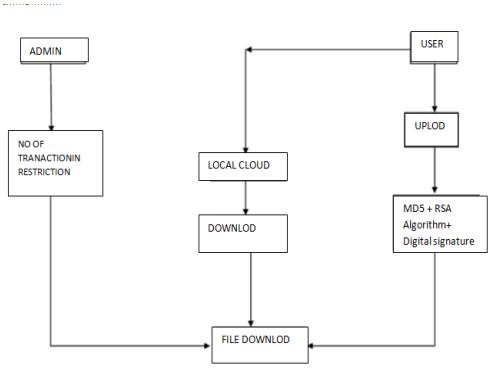


Figure 6 :- Represents the basic design of proposed work

User: A user can upload/ download file. When uploading file Blowfish, and RSA schemes are used to encrypt data & signature is included to lock that data and when downloading the files inversaly RSA are used to decrypt data

Local & signature is used to unlock the file.

Cloud: Local Cloud is used to store data in the encrypted form. Below we will explain RBAC,RSA and Digital Signature.

DepSky System: Multi-Clouds Model

Multi-Clouds Model The term "multi-clouds" is similar to theterms "interclouds" or "cloud -of-clouds" that were introduced by Vukolic. These terms suggest thatcloud computing should not end with a single cloud.Using their design, a cloudy sky incorporates unlikecolors and shapes of clouds which lead to different implementations and administrative domains.[5][7]The DepSky system addresses theavailability and the confidentiality of data in their storage system by using multi-cloud providers,combining Byzantine quorum system protocols,cryptographic secret sharing and erasure codes.[13]

DepSky Architecture

DepSky Architecture and Data Model

The DepSky architecture consists of four clouds and every cloud uses its own particular interface[13]. The DepSky algorithm exists in the client's machines as a software library to communicate witheach cloud. These four clouds are storage clouds, sohere no codes to be executed. The DepSky libraryauthorizes reading and writing operations with thestorage clouds. The use of diverse clouds requires theDEPSKY library to deal with the heterogeneity of the interfaces of each cloud provider. An aspect thatis especially important is the format of the dataaccepted by each cloud. The data model allows us toignore these details when presenting the algorithms.[2]

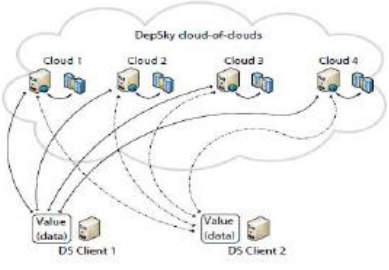
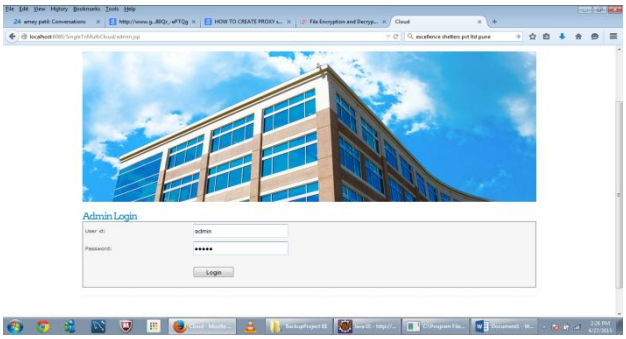


Fig.7 DepSky Data mode

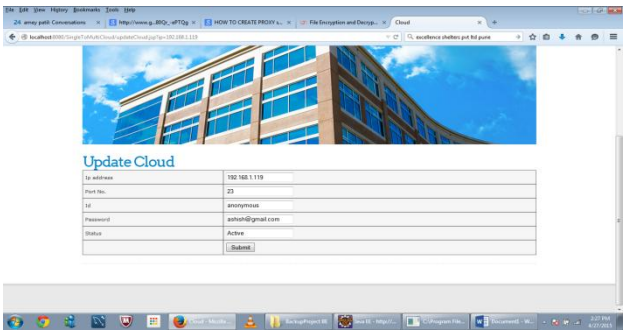
ISSN: 2278 – 1323

RESULTS:-

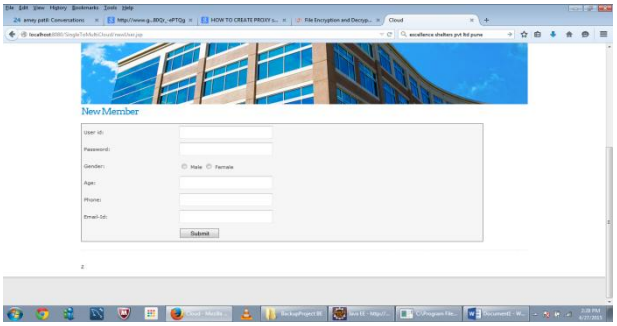
1] Admin login:-



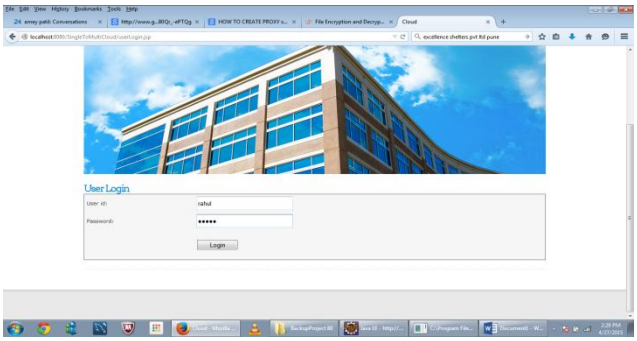
2] Admin can create and update cloud:-



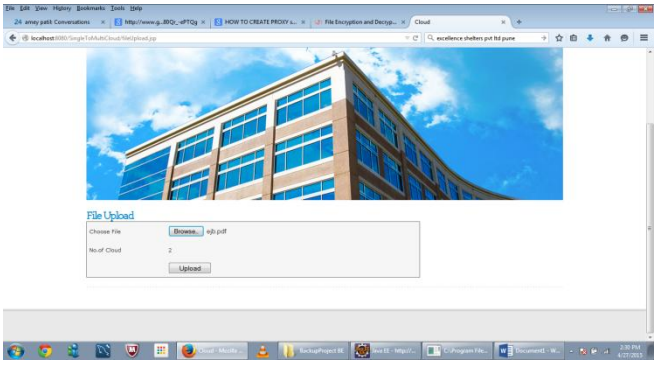
3] create member:-



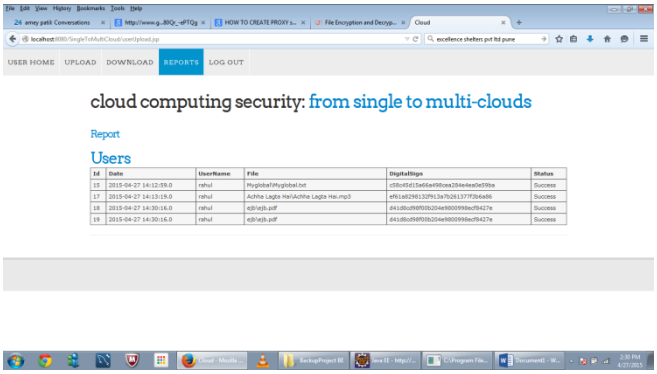
4] user login:-



5] Sending data to cloud from the user.

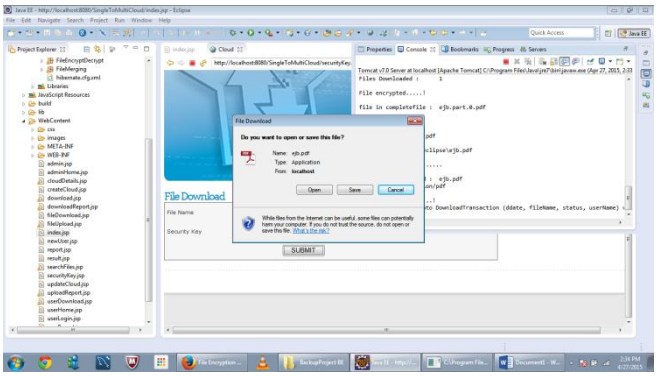


6] After sending the data to the cloud.



5] Downloading the file:-

6] download file successful:-



ISSN: 2278 – 1323

Conclusion:-

Use of cloud computing is increased rapidly; cloud computing security is still considered the major issue in the cloud computing environment. User do not want to lose their private information as a result of malicious insiders in the cloud. By using digital signature and RSA and MD5 algo. We provide the security of the data.The loss of service availability has caused many problems for a large number of customers recently.We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

References:-

[1] Access, Identity and Secure Data Storage in Private Cloud using Digital Signature International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014.

[2]Mohammed A. AlZain , Eric Pardede, Ben Soh , James A. Thom,"Cloud Computing Security: From Single to Multi-Clouds" IEEE Computer socity 45th Hawaii International Conference on System Sciences, 2012.

[3] Musthaler L (2009) Cost-effective data encryption in the cloud. Network World.

[4] Analysis of Security Algorithms in Cloud Computing International Journal of Application or Innovation in Engineering & Management (IJAIEM)Volume 3, Issue 3, March 2014.

[5] Pearson S (2009) Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09.

[6] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.

[7] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: A research survey," in 2011 International Conference on Communication Systems and Network Technologies, CSNT 2011, June 3, 2011 - June 5, 2011, Katra, Jammu, India, 2011, pp. 115-119.

[8] TO ENHANCE THE DATA SECURITY OF CLOUD IN CLOUD COMPUTING USING RSA ALGORITHM Bookman International Journal of Software Engineering, Vol. 1 No. 1 Sep. 2012

[9] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed, Md. Mahmudul Hasan Rafee "An Advanced Survey on Cloud Computing and State-of-the-art Research Issues" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012

[10] IMPLEMENTING VARIOUS ENCRYPTION ALGORITHMS TO ENHANCETHE DATA SECURITY OF CLOUD IN CLOUD COMPUTING VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10 October 2012

[11] Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for Cloud Computing. In: Proceedings of the 1st International Conference on Cloud Computing, CloudCom '09

[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[13] A. 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.

[14] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198

[15] R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy, 1980, pp. 122-134.

[16] ENHANCEMENT FOR DATA SECURITY IN CLOUD COMPUTING ENVIRONMENT International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, ISS- 3 2012

[17] "A quantitative analysis of current security concerns and solutions for cloud computing" Gonzalez *et al. Journal of Cloud Computing: Advances, Systems and Applications* 2012.

[18] Zhibin Zhou and Dijiang Huang "Efficient and Secure Data Storage Operations for Mobile Cloud Computing",2011.

ISSN: 2278 – 1323