Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

File Security in Cloud using Two-tier Encryption and Decryption

Tanisha , Reema Gupta, Dr. Rajesh Kumar

SMCA, Thapar University

India

Abstract- Cloud computing is a model that offers incredible processing power and on-demand network access to a shared pool of computing resources. In the new era of the modern world, corporate structures and individual consumers are all switching to the magnificent world of cloud computing. With the increasing popularity of the cloud technology, security of information becomes much important in data storage and transmission. It is important to ensure that the stored data is neither compromised nor corrupted, thus making authentication and authorization for data access, a necessity. The proposed methodology suggests a new security scheme for the files to be uploaded on the cloud. The integrity and confidentiality is ensured by encrypting the data using a combination of two tier hybrid encryption and the digital signature scheme and also, by providing access to the data only on successful authentication.

Keywords- Cloud Computing, IDEA, RSA, Improved ACBEA, Security, Encryption, Data Integrity.

I. Introduction

A cloud can be defined as a large pool of easily accessible virtualized resources such as hardware, development platforms and services [1]. These resources can be powerfully re-configured to arrange properly to a variable load scale, and also permitting for an optimum resource use. It is basically meant to give maximum throughput with the minimum resources i.e. the end user can enjoy maximum capability of computing with the minimum hardware requirement. Cloud computing is a network-based environment that focuses on sharing computations or resources among all of the servers, users and individuals. The concept of cloud computing is linked closely with those of Information as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS), all of which constitutes a Service-Oriented Architecture(SOA). As there is no need to store data at user's end, cloud computing allows consumers and corporate structures to use all the applications offered by the cloud without the extra effort of installation. So instead of buying the whole infrastructure required to run the processes, users are just required to rent the essential assets according to the requirement, hence, reducing the cost of hardware at the user's end. In the present world of networking system, cloud computing is one of the most important and developing concept for both the developers and the users [2]. In the cloud services, the stored data is easily drifted away from the user's control as the data is stored in the computers that are not owned or operated by users which lead to data security issues [3]. Whenever a data is on a cloud, anyone from anywhere can access data from the cloud anytime, hence making the data or files more vulnerable to attack. Although cloud architecture has its own security, but there exists an environment where the remote server can't be trusted and it is necessary to assure that the data has not been tampered with. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. A cloud is good only when a good level of security is provided by the service provider to the user. Therefore in recent days, providing security has become a major challenging issue in cloud computing.

A. Security Issues in Cloud

Cloud computing is the new era of the modern world. Corporate sector is rapidly moving onto cloud as the companies can now use the best resources in a cost effective way. As more and more information is moved to the cloud the, security concerns have started to develop. Though benefits of the cloud are enormous but cloud has got many issues when it comes to security. Some of the problems related to the cloud computing are described as below [1]:-

i) Data Integrity: Data stored in the cloud typically resides in the shared environment. When a data is on a cloud anyone from any location can access those data and information from the cloud. Cloud does not differentiate a sensitive data from a common data and thus, enables anyone to access the sensitive data. The cloud computing

service provider must make sure that the customer's private and sensitive data is well secured from other providers and users. The service provider should maintain control over access by imposing several access control rights and privileges to keep a check on who is accessing the data and who is maintaining the server. Besides access control, authentication is also required so that only a legitimate user can access the data not any malicious user.

ii) Data Stealing: Data stealing is a one of the serious issues in cloud computing environment. Data stealing refers to the illegal acquisition of information. Many cloud service providers do not provide their own server instead they lease server from other service providers due to it is cost effectiveness and flexibility. So there is a high probability that data can be stolen from the external server.

iii) Data Loss: Data loss is a common problem in cloud computing. A malicious hacker can wipe out the data or any natural/man-made disaster can destroy or corrupt the data leading to the loss of data. In such cases, having an offline copy is of great importance. Moreover, even the carelessness of the service provider can also lead to data loss e.g. if the service provider shut down his services due some financial or legal problems, then there will be a loss of data for the user.

iv) Infected Application: In the cloud computing environment**,** there exists a possibility where a malicious user can penetrate the cloud by acting as a legitimate user, there by infecting the entire cloud and thus affecting many customers who are sharing the infected cloud. It is the responsibility of the service provider to prevent any malicious user from uploading any infected application onto the cloud. Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server.

v) User Level Security: Even though the service provider takes necessary measures to provide a good security layer for the customer , it is also the responsibility of the customer to make sure that because of its own action, there shouldn't be any loss of data or tampering of data . The customer can take essential measures to protect the privacy of the sensitive data to be stored on the remote servers e.g. encrypting the documents before uploading to remote servers is one such measure that can be adopted.

B. Hybrid Cryptography and Digital Signature

Cryptography is the art and science of designing or generating the secret message i.e. code or ciphers of the original message for the secure communication between sender and receiver [4]. It can be used to store the sensitive information and transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Cryptographic algorithms can be classified either as asymmetric or symmetric algorithms. Asymmetric algorithms have the advantage of increased security and convenience but have the limitations of high resource and time utilization. In contrary, symmetric algorithms have the limitation of single key security; as a single key is used for both encryption and decryption process but comparatively have the advantages of low resource and time consumption. Hybrid cryptography is a cryptographic scheme that involves the combination of advantages of both asymmetric and symmetric cryptographies i.e. the fast encryption speed of symmetric algorithm is coupled with the high security of the asymmetric algorithm [5].

A combination of hybrid cryptography and the digital signatures provides a powerful solution to implement services that guarantee data protection and data integrity. Digital Signature is a digital equivalent of a physical signature that establishes the identity of the sender which sender cannot later revoke or deny. It is a function of the entire document; changing even a single bit produces a different signature. A Digital Signature Standard (DSS) uses asymmetric key cryptography to create digital signatures. In this scheme, firstly, the hash of document is taken using the one way hash functions. After that, hash is encrypted with the sender's private-key, thereby generating a digital signature. In this paper, we propose a new scheme for file security in cloud computing environment. The proposed scheme has all the features of symmetric, asymmetric algorithm and digital signature scheme thereby guaranteeing a more secure environment for data storage and transmission over a network.

II. Encryption Algorithms Used

A. IDEA Algorithm

The IDEA is a block cipher that operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The algebraic idea behind IDEA is the mixing of three incompatible algebraic operations on 16-bit blocks: bitwise XOR, addition modulo 2^{16}, and multiplication modulo $2^{16} + 1$ [6]. The algorithm is characterized by the symmetry of encryption and decryption process and the generation of decryption keys from encryption keys and vice versa. The only difference compared to encryption is that during decryption, different sub-blocks of 16-bit key are generated. More precisely, each of the 52 sub-blocks of 16-bit key used for decryption is the inverse of the key sub-blocks used during encryption in respect of the applied algebraic group operation. Additionally, the sub-blocks of 16-bit key must be used in the reverse order during decryption in order to reverse the encryption process. for the encryption process, the 64-bit plain text is divided into four 16-bit sub blocks. The encryption process comprises of eight identical rounds and a "half round" output transformation. 52 sub-blocks of 16- bit keys are computed from a 128 bit secret key. Each round uses six sub keys and remaining four sub-keys are used in output transformation. The algorithm converts the plain-text blocks into cipher-text blocks of same bit length divided into four 16 bit sub blocks.

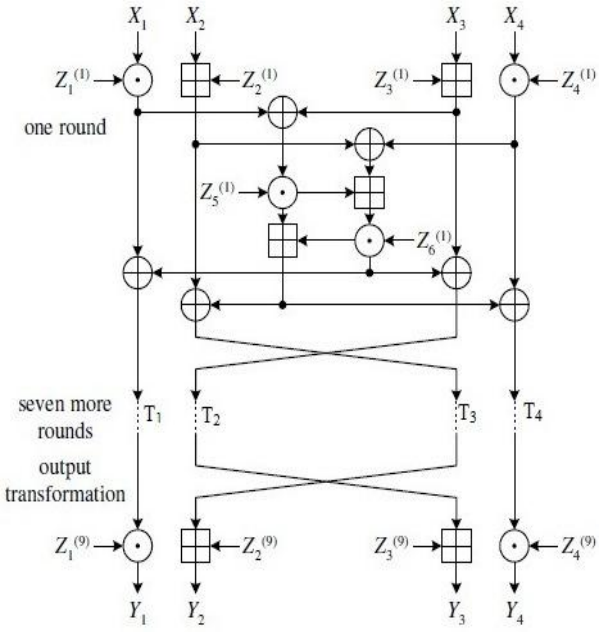

Fig. 1 Block Diagram of IDEA Algorithm [7]

1) Steps for Each Round of Encryption:

The input to the first round of IDEA is 64-bit plain text which is divided into four 16-bit sub blocks; X_1, X_2, X_3 and X_4. $Z_i^{(r)}$ is a 16-bit sub key where i and r are the sub key number and round number respectively. The steps for encryption are as follows [8].

1. Multiply X_1 and the first sub key $Z_1^{(1)}$.
2. Add X_2 and the second sub key $Z_2^{(1)}$.
3. Add X_3 and the third sub key $Z_3^{(1)}$.
4. Multiply X_4 and the fourth sub key $Z_4^{(1)}$.
5. Bitwise XOR the results of steps 1 and 3.
6. Bitwise XOR the results of steps 2 and 4.
7. Multiply the result of step 5 and the fifth sub key $Z_5^{(1)}$.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub key $Z_6^{(1)}$.
10. Add the results of steps 7 and 9.
11. Bitwise XOR the results of steps 1 and 9.
12. Bitwise XOR the results of steps 3 and 9.
13. Bitwise XOR the results of steps 2 and 10.
14. Bitwise XOR the results of steps 4 and 10.

Output of each round acts as an input for next round. This process is repeated for the next seven successive rounds.

2) Steps for the Final Output Round:

The input to the final output round is the output of the eighth round of encryption; T_1, T_2, T_3, T_4. $Z_i^{(r)}$ is a 16 bit sub key where i and r are the sub key number and round number respectively [8]. The steps for the final output round are as follows [8].

1. Multiply T_1 and the first sub key $Z_1^{(9)}$.
2. Add T_2 and the second sub key $Z_2^{(9)}$.
3. Add T_3 and the third sub key $Z_3^{(9)}$.
4. Multiply T_4 and the fourth sub key $Z_4^{(9)}$.

B. RSA Algorithm

RSA algorithm is a public key encryption algorithm, which contains a public key and a private key, the two appear as pairs, and the corresponding key must be used for encryption and decryption operation [9].

1) Key Generation:

The steps for key generation are as follows [9]:

i) Choose two distinct and large random prime numbers ‘p’ and ‘q’.

ii) Compute n = p * q, where n is used as the modulus for both the public and private keys
iii) Compute phi (n) = (p -1) * (q-1).
iv) Choose an integer e such that 1 < e < phi(n) , and e and phi(n) share no factors other than 1 , where e is released as the public key exponent.
v) Compute 'd' to satisfy the congruence relation d × e = 1 modulus phi(n); d is kept as the private key exponent.

Now,
(e, n) constitutes the Public Key
(d, n) constitutes the Private Key

2) Encryption and Decryption:

Suppose user 'A' wants to send a private message (M) to user 'B'.

i) User A gets User B's public key (e, n) from some public source.
ii) User A encrypts message M using B's public key. This produces a cipher text message, C using encryption function i.e.
$C = M^e \bmod n$
iii) Cipher text message C is sent over some communication channel
iv) Upon reception, user B decrypts message C using his private key (d, n). This produces original plain text message, M using decryption function i.e.
$M = C^d \bmod n$

C. Improved ASCII Code Based Encryption Algorithm (Improved ACBEA)

Improved ACBEA is the enhancement of ACBEA proposed by A. Mathur [4]. The main objective behind proposing this algorithm is to overcome the shortcomings of ACBEA and enhance the security of the algorithm at the whole. It uses ASCII values of the data to perform the encryption and decryption process. It can be used to encrypt every possible combination of characters including special symbols, alphabets and digits available in 8-it ASCII character set.

1) Encryption Process:

The steps to encrypt the plain text are as follows:-

i) Get the ASCII value of each character of the plain text and store it in an AsciiVal array.
ii) Find out the minimum value (min) from the AsciiVal array.
iii) Now perform the division and modulus operations on each ascii value i.e. AsciiVal[i] and save the result in the DivContent , ModContent, DivMod array as follows:
DivContent[i] = AsciiVal[i] / min
ModContent[i] = AsciiVal[i] % min
DivMod[i] = ModContent[i] / 16
If ModContent[i] >=16
Go to step 4.
Else
Go to step 5.
iv) Perform modulo 16 operation as
ModContent[i] = ModContent[i] % 16
v) Get the ASCII value of each character of the Secret Key and store it in an AsciiKey array.
vi) Now perform the modulus operation on each ascii value i.e. AsciiKey[i] and save the result in ModKey array as follows:
ModKey[i] = AsciiKey[i] % min
If ModKey[i] >=16
Go to step 7.
Else
Go to step 8.

vii) Perform modulo 16 operation as
ModKey[i] = ModKey[i] % 16
viii) Find out the minimum value (n) from the ModKey array
ix) Determine the binary equivalent (each 4 bit) of each element of ModKey and concatenate all values to form a binary string.
x) Perform the n bit left circular shift operation on binary string and determine the encrypt key after the shift i.e. Encrypt[i] by substituting decimal equivalent for each 4 bit binary string.
xi) Add min value to each element of Encrypt[i] to calculate the final cipher key as follows:

CipherKey[i] = Encrypt[i] + min

xii) Now, add each element of ModContent array to the corresponding element of CipherKey array as follows:
Cipher[i] = ModContent[i] + CipherKey[i]

xiii) Perform binary to gray code conversion on each element of Cipher array, convert the resultant value to corresponding decimal equivalent and update the Cipher array.

xiv) Substitute the ASCII character corresponding to each element of Cipher array to generate the final cipher text.

xv) Substitute the ASCII character corresponding to each element to of the CipherKey array to generate the final cipher key.

2) Decryption Process:

The steps for decrypting cipher are as follows:

i) Get the ASCII value of each character of the cipher text and store it in an AsciiCipher array.

ii) Perform gray to binary code conversion on each element of AsciiCipher, convert the resultant value to corresponding decimal equivalent and update the AsciiCipher array.

iii) Get the ASCII value of each character of the cipher key and store it in an CipherKey array

iv) Perform the subtraction of ascii values of cipher key from cipher text as follows:
Difference[i] = AsciiCipher[i] - CipherKey[i].

v) Add min value to each value of difference as follows:
DecryptVal[i] = Difference[i] + min * DivContent[i] + 16 * DivMod[i].

vi) Substitute the ASCII character corresponding to each element of DecryptVal array to generate the final plain text.

III. Proposed Cryptosystem

The proposed cryptosystem combines the security of the document by two-tier hybrid encryption and authenticity by digital signatures. A combination of hybrid cryptography and the digital signatures provides a powerful solution to implement services that guarantee data protection and data integrity. This scheme has all the features of symmetric, asymmetric algorithm and digital signature scheme, thereby guaranteeing a more secure environment for data storage and transmission over a network.

A. Encryption Phase

The various steps involved in the encryption are:

i) First, a secret IDEA key of length 128 bits is generated.

ii) Using this key, the message(M) is encrypted in a quick manner
E_M = IDEA (M)

iii) The IDEA key is encrypted at Level-I using Improved ASCII Code Based Encryption (IACBEA) Algorithm.
E_{K1} = IACBEA (IDEA Key)

iv) Afterwards, the encrypted IDEA key is passed to the RSA Encryption system for the Level-II Encryption
E_{K2} = RSA-Encrypt (E_{K1})

v) Thereafter, the encrypted message (E_M) acts as an input for SHA-512, which will produce 512-bit condensed version.
E_H = SHA-512(E_M)

vi) The message digest (E_H) will be signed using RSA Digital Signature algorithm using the private key of the sender, hence generating a digital signature.
D=RSA-Sign (E_H)

vii) The encrypted message (E_M) encrypted IDEA key (E_{K2}) and digital Signature (D) are transmitted across the communication channel.

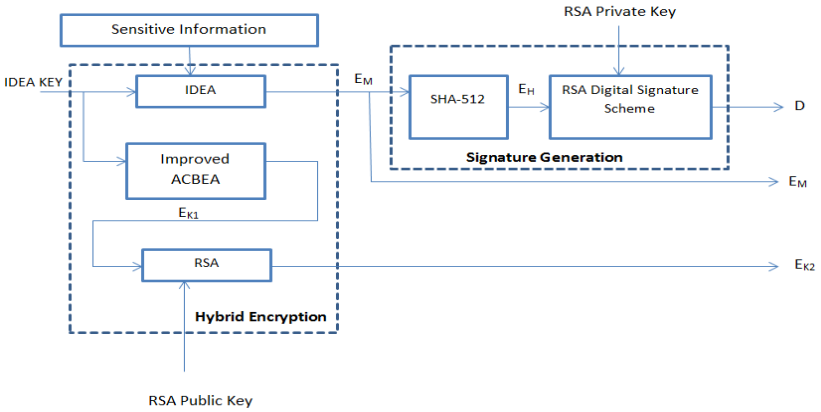

Fig. 2 Encryption Phase

B. Decryption Phase

The various steps for the decryption are:

i) The encrypted IDEA key (E_{K2}) is passed to RSA Decryption system for Level-I Decryption
E_{K1} = RSA-Decrypt (E_{K2})

ii) The Level-I decrypted IDEA key (E_{K1}) is decrypted using Improved ASCII Code Based Encryption Algorithm.
K = IACBEA (E_{K1})

iii) The original message (M) is retained by IDEA algorithm using the obtained IDEA Key (K).
M=IDEA (E_M)

iv) The encrypted message (E_M) acts as an input for SHA-512, which produces 512-bit condensed version (E_H)
E_H = SHA-512 (E_M)

v) The digital signature acts as an input to RSA Digital Signature Verification algorithm, which produces the expected hash (E_H) using the sender's public key.
E_H = RSA-Verify (D)

vi) In order to verify the origin and the integrity of data, the calculated hash (E_H) and expected hash (E_H) are compared.

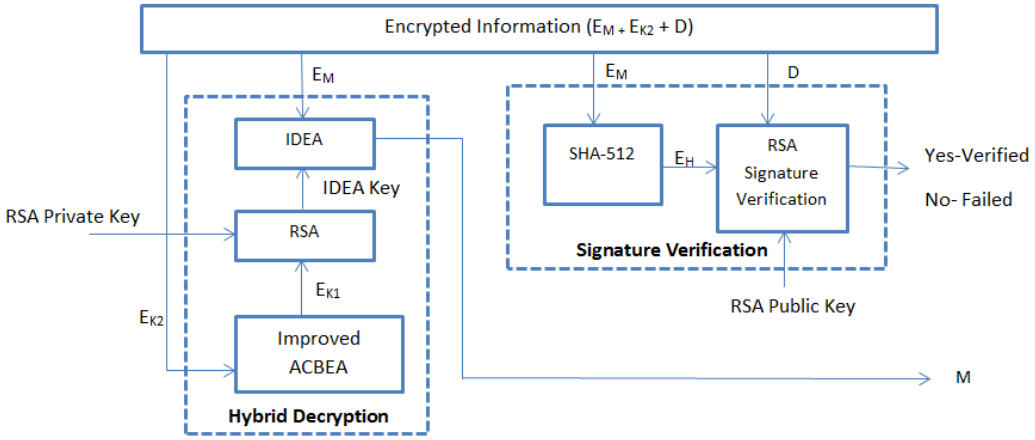

Fig. 3 Decryption Phase

IV. Security Architecture for Cloud Storage

The new trend of outsourcing data on the cloud; where users have reduced control of their own information, has given rise to many security threats. As the remote cloud server cannot be fully trusted, so one of the security measures is to encrypt the data before outsourcing. Thus, to ensure the security of data stored on the remote cloud servers, the proposed hybrid cryptographic scheme is employed.

The scheme can be broadly categorized into two phases:

i) Uploading Phase
ii) Downloading Phase

A. Uploading Phase

Various steps involved in the uploading phase are listed as below:

i) Client sends request to main server to authenticate himself.
ii) On the successful authentication, a secured connection is established with the cloud.
iii) Once the connection is established, the user encrypts the file using proposed hybrid cryptographic scheme.
iv) After the files are encrypted, client provides a unique ID and sends a request to main server to upload the files.
v) In response to client's request, server returns the IP address of VM having the minimum load among the available VM's on the network.
vi) Encrypted file(s) are uploaded to the VM server.
vii) Client disconnects the connection with the cloud, and the load on the VM is updated.

1-Request for Connection
2-Input to Hybrid Cryptosystem
3-Output from Hybrid Cryptosystem
4-Client provides a unique ID for event
5-Server returns VM IP
6-Upload Files to Server

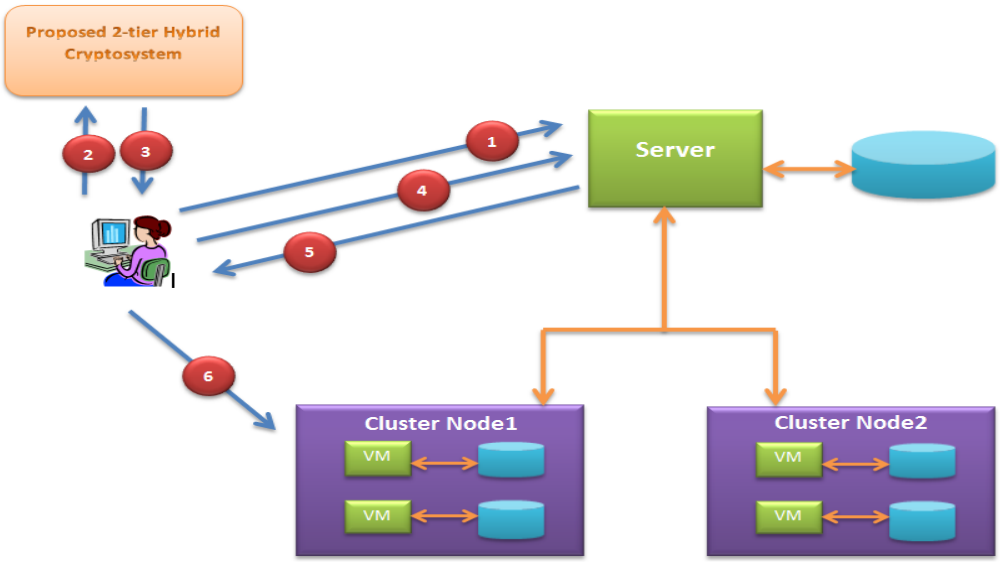

Fig. 4 Uploading Phase

B. Downloading Phase

Various steps involved in the downloading phase are listed below:

i) Client sends a request to main server to authenticate himself.
ii) On successful authentication, a secured connection is established with the cloud.
iii) Client is required to enter the unique ID which he had entered during the uploading of the file(s).
iv) Main server returns the IP address of VM corresponding to the unique ID.
v) Encrypted files are downloaded from the VM server whose IP address is returned from the main server.
vi) Decryption is carried out at the client end using the proposed hybrid cryptographic scheme.
vii) Client disconnects the connection established with the cloud and the load on the VM is updated.

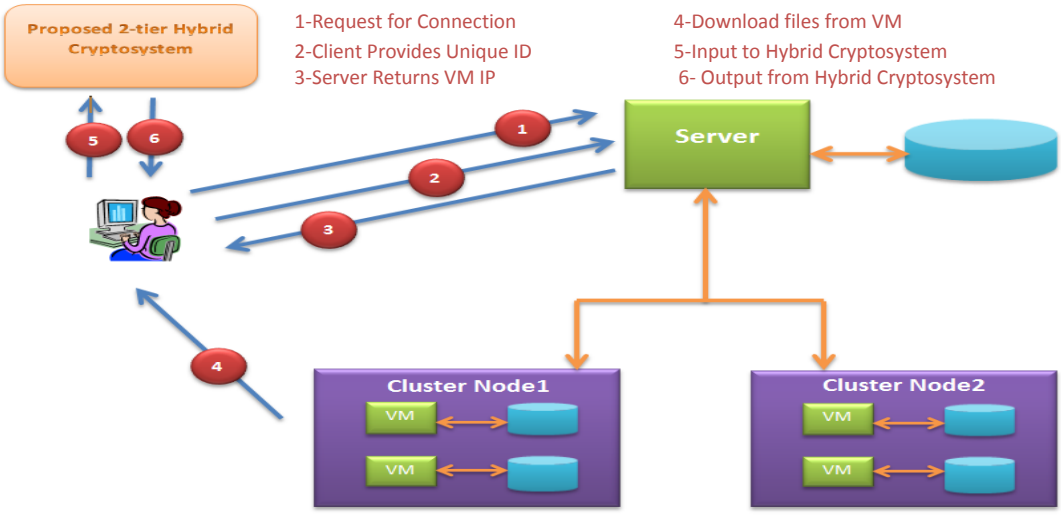

Fig. 5 Downloading Phase

V. DESIGN AND IMPLEMENTATION

For the purpose of simulating the proposed cloud security model, OpenNebula open source toolkit is used. We created a private cloud environment with one front node and two cluster nodes using OpenNebula. At each of the cluster nodes, 2 VM's are deployed. The allocation of VM is managed on the basis of the load i.e. VM with the minimum load is assigned to serve the client's request. The hybrid cryptosystem is implemented in java which is well known for its platform independence and deployed at each of the VM. Various libraries have been used like javax.crypto, java.security to implement hybrid encryption scheme. The cloud security model has been tested for various types of file:image,text,word and pdf files.

VI. CONCLUSION

According to service delivery models and deployment models of cloud, data security and privacy protection are the primary problems that need to be solved. The proposed methodology suggests a two-tier hybrid cryptographic scheme coupled with the digital signature scheme for encryption of the files to be uploaded on the cloud. A combination of hybrid cryptography and the digital signatures provides a powerful solution to implement services that guarantee data protection and data integrity. Secondly, the two tier encryption of symmetric key further adds to the security. IDEA algorithm in encryption/decryption process shows high efficiency and ease of implementation. Also, IDEA uses 128 bit key that is strong enough against various cryptographic attacks. In fact, there are no linear cryptanalytic attacks on IDEA and there are no known algebraic weaknesses in IDEA. RSA algorithm and Improved ACBEA, used to encrypt the symmetric key, ensures the safe delivery of symmetric key necessary for encrypting/decrypting data. RSA Digital Signature Scheme ensures authenticity and integrity of data.

VII. FUTURE SCOPE

The proposed framework has been implemented on image, word, text and pdf files. This can be enhanced to encrypt audio and video files. Also, the model is fruitful in data as a service, which can be deployed in other service models of cloud for enhancing the cloud security. The security model can be further improved by improving IDEA algorithm. IDEA uses a 64 bit block for encryption/decryption process. The greater will be size of block, the greater will be the security. Thus, a detailed analysis and work needs to be done so that block size in IDEA can be improved from 64 bit to ensure the maximum range of protection against attacks.

ACKNOWLEDGMENT

We would like to thank Dr. Rajesh Kumar for his immense support and guidance in this research.

REFERENCES

[1] P. Subhasri and A. Padmapriya, "Cloud Computing: Security Challenges & Encryption Practices", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, March 2013.

[2] K. Nafi, T. Kar, S. Hoque and M. Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 10, 2012.

[3] Z. Tang, X. Wang, L. Jia, and W. Man, "Study on Data Security of Cloud Computing", *Proc. IEEE Spring Congress on Engineering and Technology*, pp: 1-3, 2012.

[4] A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", *International Journal on Computer Science and Engineering* , vol. 4, no. 9, pp:1650- 1657, September 2012.

[5] Y.P. Singh and M. Khan, "On the Security of Joint Signature and Hybrid Encryption", *Proc. 13th IEEE International Conference on Networks*, vol. 1, 2005.

[6] 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.

[7] 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.

[8] N.Hoffman, "A Simplified IDEA Algorithm", *Journal Cryptologia*, vol. 31, issue 2, pp: 143-151, April 2007.

[9] W. Hui and M. Jun, "Research of the Database Encryption Technique Based on Hybrid Cryptography", *Proc. IEEE Symposium on Computational Intelligence and Design*, vol.2, pp: 68-71, 2010.

