Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm

Swarna C[#1], Marrynal S. Eastaff[*2]

[#1]PG Scholar, PG Department of IT, Hindusthan College of Arts and Science, Coimbatore,
[*2]Asst Professor, PG Department of IT, Hindusthan College of Arts and Science, Coimbatore
[1]swarna.karishma99@gmail.com , [2]marrynalhindusthan@gmail.com

***Abstract*— In the cloud environment, resources are shared among all of the servers, users and individuals. So it is difficult for the cloud provider to ensure file security. As a result, it is very easy for an intruder to access, misuse and destroy the original form of data. In case of compromise at any cost; entrusting cloud is of no use. A need for "practically strong and infeasible to get attacked" technique becomes vital. The paper presents the file security model which uses the concept of hybrid encryption scheme to meet security needs. In the proposed model, encryption and decryption of files at cloud servers done using blowfish and modified version of RSA. Further, it is tested in cloud environment: Open Nebula.**

***Keywords*— Cloud computing, Data Security, Hybrid Cryptosystem**

I. INTRODUCTION

Cloud computing is originated from earlier large-scale distributed computing technology. NIST defines Cloud computing as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g.,networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

In Cloud computing, both files and software are not fully contained on the user's computer. File security concerns arise because both user's application and program are residing in provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted by blowfish coupled with file splitting and SRNN (modified RSA) is used for the secured communication between users and the servers.

A. Data Security Issues

Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.
- According to service delivery models of Cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.
- Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

II. HYBRID CRYPTOSYSTEM SCHEME

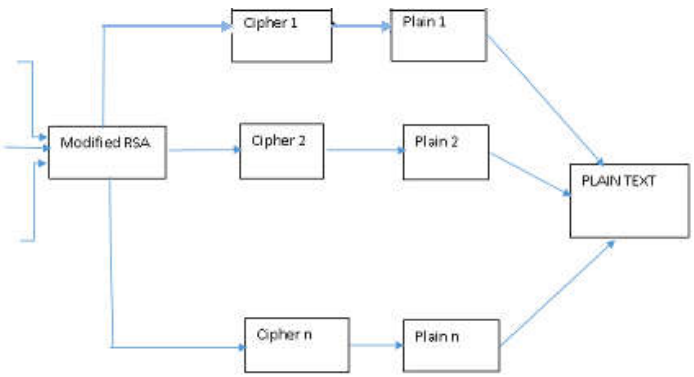
In order to ensure file security on cloud, hybrid cryptosystem is being used. We assume that the remote server is trusted, so files are encrypted by server and finally encrypted files are stored at the server end. The hybrid cryptosystem uses a combination of:

- Blowfish Algorithm coupled with File Splitting andMerging mechanism
- SRNN Algorithm

In a hybrid scheme, the performance of symmetric algorithm is integrated with security of asymmetric algorithm. The symmetric algorithm (Blowfish) used in hybrid cryptosystem has best practice to avoid data misuse when compared with other symmetric algorithms. Also, in terms of throughput, Blowfish has best performance. The SRNN used serves as a good balance between speed and security. In hybrid cryptosystem, firstly, files uploaded files are sliced and each slice is encrypted by the corresponding key Blowfish key provided by the user. Secondly, each of the n keys are encrypted using SRNN where n is the number of slices.

A. Blowfish

Blowfish is a symmetric block cipher which uses a Fiestal network, 16 rounds of iterative encryption and decryption functional design. The block size used is of 64-bits and key size can vary from any length to 448.Blowfish cipher uses 18 sub arrays each of 32-bit commonly known as P-boxes and four Substitution boxes each of 32-bit, each having 256 entries. The algorithm design is shown in figure. It consists of two phases: one is Key Expansion phase another is Data Encryption phase. In Key expansion phase, key is converted into several sub-keys and in Data Encryption phase, encryption occurs via 16-round networks. Each round consists of a key dependent permutation and a key and data-dependent substitution.



B. SRNN

The SRNN algorithm is a public key cryptography algorithm similar to RSA with some improvement. In this algorithm, extremely large number having two prime factors (similar to RSA) is used. In addition to, this, two short range natural number in pair of keys are used. This improvement increases the security of cryptosystem. SRNN is used for secure communication between user and cloud servers.

III. HYBRID CRYPTOSYSTEM PHASES

The hybrid cryptosystem used to maintain security of the files has two phases:

- Encryption Phase
- Decryption Phase

A. *Encryption Phase*

At the encryption end,

- On the specification of user, the file being encrypted will be sliced into n slices. Each of the file slices is encrypted using Blowfish key provided by the user for each slice.
- The key will be encrypted using SRNN public key
- After encryption, we have encrypted files slices and the corresponding encrypted keys.

B. *Decryption Phase*

At the decryption end,

- The user will provide n SRNN private keys, according to the number of slices (n) created during the encryption phase. Blowfish key is decrypted at the server end using the SRNN private key specific to the slice.
- Using the corresponding decrypted Blowfish keys, file slices stored at server are decrypted.
- The decrypted slices will be merged to generate original file.

IV. PROPOSED CLOUD COMPUTING SECURITY ARCHITECTURE

In order to ensure file security on cloud, the above hybrid cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form.

We broadly classify the scheme deployed on cloud in three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

We used Open Nebula toolkit to set up cloud environment. In Open Nebula, we have one front node and n cluster nodes. The VM's are deployed from front node to the corresponding cluster node. Open Nebula has been designed in such a way that it allows integration with many different hypervisors and environments. There is a front-end that executes all the process in OpenNebula while the cluster nodes provide the resources that are needed by VM. There is at least one physical network joining all the cluster nodes with the frontend.

A. *Registration Phase*

In the Registration Phase, the client registers himself in order to upload and view his files to/from the cloud server. In the registration process, the client sends its request to front node and in return, front node assigns the VM of the cluster node, which has minimum load among other VM's on the network to the client. At the end of registration phase, the client is registered with IP address of corresponding VM. Whenever he again issues his request, the request is transferred to its corresponding VM. The encrypted files, encrypted blowfish keys, public SRNN keys are stored at his registered VM.

B. *Uploading Phase*

In the Uploading Phase, steps are as follows:

Step: 1: The client will send request to front node to authenticate himself.
Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user was registered.
Step 3: The files are uploaded by the client to the registered server (VM).
Step 4: The encryption of uploaded files is done using the hybrid cryptosystem.
Step 5: The encrypted slices and Blowfish encrypted keys remain stored in VM's data store.

Step 6: The SRNN private keys are send to user and finally they are deleted form the server so that only the authenticated user is able to view his uploaded file.

C. Downloading Phase

In the downloading phase, the steps are as follows:

Step 1: The client will send request to front node to authenticate himself.
Step 2: On successful authentication, the front end which send the corresponding IP address of the VM against which user
was registered
Step 3: The client will upload n SRNN private keys for the corresponding n slices.
Step 4: The SRNN private keys will decrypt the corresponding encrypted Blowfish keys and the encrypted slices are decrypted by Blowfish keys.
Step 5: The decrypted files are merged to generate original file.
Step 6: The decrypted file is downloaded and viewed at client end.

V. DESIGN AND IMPLEMENTATION

For the purpose of simulating the proposed cloud security model, we used Open Nebula open source toolkit. Here we created one front node and two cluster nodes. At each of the Cluster node 2 VM's are deployed. The allocation of VM at the time of registration is implemented in java which is well known for its platform independence. The hybrid cryptosystem is also implemented in java 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: audio, image, text, word, pdf file.

VI. BENEFITS OF PROPOSED MODEL

The proposed model is liable to meet the required security needs of data center of cloud. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. Modified RSA(SRNN) has increased security than RSA. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. The various benefits are as summarized:

- The public key cryptography used helps to facilitate authorization of user for each file.
- The need of more light and secure encryption system for file information preserving system on cloud is satisfied.
- The file splitting and merging makes the model unfeasible to get attacked.

VII.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. Data Security and privacy issues exist in all levels in SPI service delivery models. The above mentioned model is fruitful in data as a service, which can be extended in other service models of cloud. Also it is tested in cloud environment like Open Nebula, in future this can be deployed in other cloud environments and the best among of all can be chosen.

REFERENCES

[1] Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010.

[2]]Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies ,pp. 217-222, Dec. 2011.

[3] Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[4] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[5] Jitendra Singh Adam et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.

[6] Manikandan.G et al., "A changed cryptographic plan improving information", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.

[7] Niles Maintain and Subhead Bhingarkar, " The examination and Judgment of Nimbus, Open Nebula and Eucalyptus", International Journal of Computational Biology , vol. 3, issue 1, pp 44-47, 2012.