iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41081

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Secure Cloud Data Storage Using Hybrid Cryptography

Nidhi Kumari[1], Prof. Vimmi Malhotra[2]
[1]*Master of Technology, Computer Science Engineering*
[2]*Professor, Computer Science Department, Dronacharya College of Engineering, Gurugram*

Abstract: ***Nowadays a huge number of organizations use the cloud for storing Big data. And some of the sectors have sensitive data, for example, Military, Agencies, Colleges, Industries, etc. The data can be retrieved when the user requests it. And others can also access the data. Cloud computing provides a lot of features with affordable prices and knowledge accessibility by using the Internet. Security is the main concern in the cloud computing environment as clients store secret information with cloud providers, but sometimes these providers may not be trustful. Splitting data in a safe approach while protecting data from an untrusted cloud is still a demanding topic. In this paper we ensure the right approach for data security and privacy, using Blowfish, and RSA/SRNN algorithms.***
Keywords: Cloud Computing, Data storage, RSA/SRNN algorithm, Blowfish algorithm, Data storage.

I. INTRODUCTION

Cloud computing security is becoming a prominent study topic these days. The majority of businesses have begun using cloud storage in place of traditional data storage, which gives a well-organized approach to access data from anywhere at any time. The biggest issue in authorizing cloud computing for any corporation is data security. This study presents a multi-tiered cryptography-based cloud computing security approach. Cloud computing arose from the large-scale distributed computer technology of the past.
As a solution, the cloud provider can encrypt the attached files/document using an authenticate algorithm. This paper describes a file/document security model that provides a cost-effective solution to the fundamental security issues in the cloud. The technique uses a cross-cryptography technique in which files/documents are securely enciphered with a middleware interface.

A. Data Security Issues

There are many security issues with cloud data and applications because of their open nature and multi-tenancy. There are several issues to consider:

1) Cloud computing's dynamic scalability, service, and location transparency make it possible for any type of application or data to run on any platform or infrastructure.
2) The task is challenging to implement a single security plan due to conflicts of interest in cloud computing service delivery models. Various providers can own resources and cloud services.
3) The cloud's openness and the shared virtualization of resources between multiple tenants may allow unauthorized users to access user data.

II. HYBRID CRYPTOGRAPHY SCHEME

Hybrid cryptosystem work on cloud to secure data. Secluded servers are presumed to be trustworthy, server-side encryption is used for files, and then after files are encrypted on the server, they are stored there. Hybrid cryptography combines:

1) Using Blowfish algorithms combined with file splitting and merging
2) RSA Algorithm

Hybrid techniques combine symmetric algorithms with asymmetric algorithms to provide efficiency and security. When compared with other symmetric algorithms, hybrid cryptosystem (Blowfish) has the better method of avoiding data/file exploits. Blowfish has the highest bandwidth performance. RSA/SRNN's speed and security are well balanced. The user provides the equalizing key Blowfish key using which each slice of uploaded files is encoded. RSA/SRNN is then used to encrypt each of the n keys with n being the number of slices.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

A. Blowfish Algorithm

The Luby-Rackoff block cipher network used in Blowfish was designed to provide 16 repeating encryption and decryption rounds. There are five different key sizes: four to four hundred and forty-eight bits for block size and 64 bits for the key. Each P-box of the cipher is 32-bits with 256 entries, and each Substitution box is 32-bits, with 256 entries. Two phases are involved in the encryption process: The key Expansion Stage and Data Encryption Stage. Data encryption is carried out with 16-round networks during the Key Expansion and Data Encryption phases. During the permutation and substitution process, permutations are performed based on the key, and substitutions are performed based on the data.

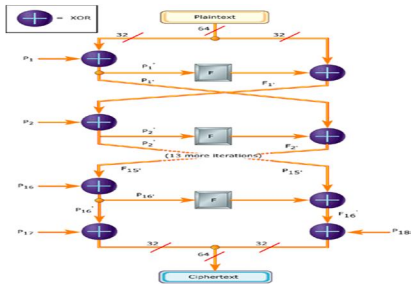


Fig.1.Blowfish Algorithm

B. RSA Algorithm (Revist-Shamir-Aldeman)

There are two distinct keys contemplated in RSA, which are public and private. A public key is added to all of them, but a private key is kept secret. It is used encryption and authentication algorithms. Based on prime numbers, RSA encrypts and decrypts data steadily using positive integer prime numbers. This process is in fig.2.

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}
Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig.2.RSA Algorithm

C. SRNN Algorithm

SRNN algorithm is an upgraded version of RSA algorithm. Whenever a number is extremely large and has two prime factors, it is used in this algorithm. Additionally, a pair of keys are based on short-range natural numbers. Cryptography security is increased. Cloud storage and remote backup are made safe.

III. HYBRID CRYPTOGRAPHY SYSTEM STAGES

For maintaining the integrity of files, a hybrid cryptosystem is used has two stages:

A. Encryption Stage

When encryption process is complete:

1) Slices are made according to the requirement of the user for the encryption of the file. The users provide Blowfish keys for each slice that is encrypted.
2) RSA/SRNN public key will be used to encrypt the key.
3) Our encoded files slices then correspond to the matching encrypted keys.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

B. Decryption Stage

When decryption process is complete:

1) In accordance with the number of slices created at the time of encryption stage (n), the user will provide (n)SRNN private keys. SRNN private keys for each slice are used to decrypt the blowfish key at the server end.
2) Slices of files stored on a server are decrypted by using corresponding Blowfish keys
3) Original file will be generated by merging decrypted slices.

IV. PROPOSED MODEL ARCHITECTURE

A hybrid cryptosystem such as the one described above is deployed on cloud in order to guarantee file security. Generally, cloud servers are assumed as trusted, but for security reasons, the data in encrypted format to prevent tampering, misuse or leakage by intruders. The implementation of cloud schemes can be broadly categorized into three stages:

A. Registration Stage

Clients register themselves for the purpose of uploading and downloading files on the cloud server during the Registration Stage. Clients send requests to the front node, in turn, assigns the client the VM that has least load among all other VMs on the network. Clients are assigned IP addresses of corresponding VMs at the end of registration. A new request is sent every time he issues it to the corresponding VM. SRNN public keys, encryption blowfish keys, and encrypted blowfish keys are all stored on his registered virtual machine.

B. Uploading Stage

As part of the Upload Stage, need to do the following:

1) *Step1:* A client sends an authentication request to the front node requesting authentication.
2) *Step2:* During step two, the front end sends an IP address of the virtual machine associated with the user's registration on successful authentication.
3) *Step3:* The client uploads the documents to the registered server (VM).
4) *Step4:* Hybrid cryptography is used to encrypt uploaded files.
5) *Step5:* The encrypted slices and Blowfish encrypted keys both are stored in virtual machine data storage.
6) *Step6:* It's only the user that can view his uploaded file because the SRNN private keys are sent to him and they're finally deleted from the server.

C. Downloading Stage

The following steps are involved in the downloading stage:

1) *Step1:* Authentication will be requested by the client from the front node.
2) *Step2:* The front end which sends the corresponding IP address of the VM to which authentication is successful.
3) *Step3:* SRNN private keys for each slice will be uploaded by the users.
4) *Step4:* SRNN private keys are used to unlock the Blowfish encryption keys; these keys are then used to decrypt the encrypted slices.
5) *Step5:* A merged version of the decrypted files is made.
6) *Step6:* This is done by downloading and viewing the decrypted file on the client's end.

V. BENEFITS OF PROPOSED MODEL

Cloud data centers need adequate security. The proposed model addresses their security needs. In comparison with other symmetric algorithms, using blowfish to encrypt file slices takes less time and has a lower latency than others. An improved SRNN can provide greater security than RSA. It contributes to the security of data by splitting and merging. In a cloud environment, hybrid techniques enhance security for the remote server and help cloud providers gain more user confidence. Separation of sensitive data and access control, in terms of data security and privacy, fulfills the first principle challenge. Here are a few of the advantages:

1) This method of public key cryptography facilitates the permission process for every file.
2) File information in cloud is protected by a secure encryption system.
3) This makes the model impossible to attack due to the split and merge files.

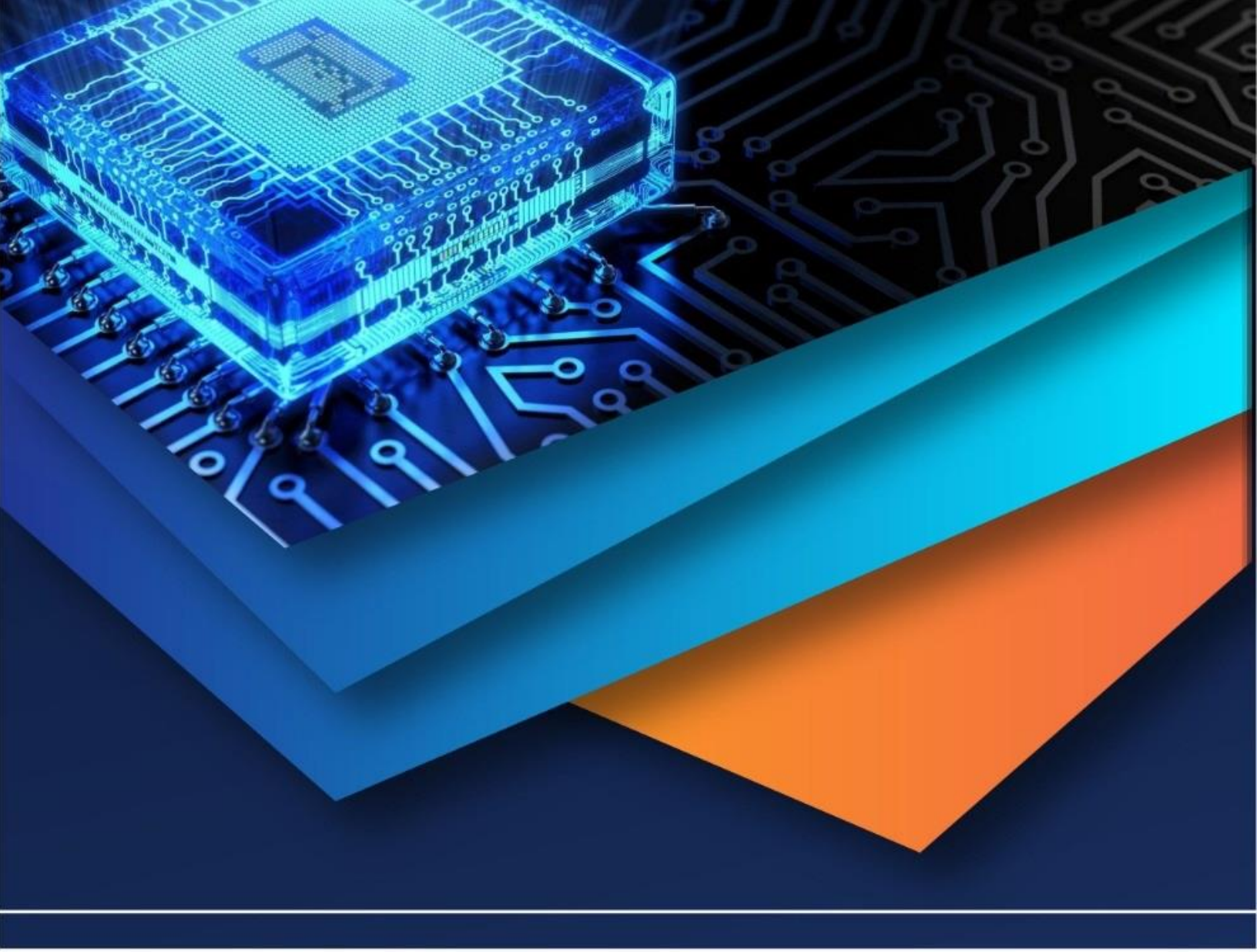
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

VI. CONCLUSION

Getting data security and privacy protection right is the main concern for cloud service delivery models and deployment models. In SPI model service delivery models, security concerns are at all levels. This model promotes data as a service, a feature applicable to other models of cloud service delivery. This approach could be applied to other cloud environments as well. Hopefully, they will be able to choose from among them in the future

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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY