International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V67I4P124

Volume 67 Issue 4, 118-123, April 2019
© 2019 Seventh Sense Research Group®

Original Article

Security to the Cloud using RSA and Blowfish Algorithm

Rakshith N [1],RaushaniKumari[2],Srividya M S[3], Shreeraksha M R[4],Pratik Jha[5]

[1]*Assistant Professor, Information Science and Engineering Mandya, Karnataka, India*
[2]*Student, Information Science and Engineering Mandya, Karnataka, India*

Abstract *- Cloud computing uses a set of available services and resources through the internet. Data centers located around the world provide cloud services. Cloud Computing has become an eminent part of the IT industry in the past couple of years. As a result of its economic benefits, more and more people are heading toward Cloud adoption. Cloud computing is characterized by on-demand self-service, ubiquitous network accesses, resource pooling, elasticity, and measured services. The characteristics mentioned above of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. Cloud Computing is today's generation of advanced technology services made available for customers per utilization basis. Servers are being utilized on the cloud to outsource their highly valuable data. Though cloud computing has many benefits, it has security threads of pivotal confidential data. There are numerous Cloud Service providers (CSP) allowing customers to host their applications and data in the cloud. As technology has seen rapid growth recently, security has been a major concern. The information might be personal or organizational data stored in the cloud is facing a potential threat from hackers, and there is a need to identify the proper security. So the data stored in the cloud will be secure. In this paper, we provide security to the cloud data using the RSA algorithm and add the salt using the blowfish algorithm to provide extra security to the cloud data. Here we divide a file into fragments and provide security to each fragmented part and upload it into the cloud in different buckets that ensure that no meaningful information is revealed to the attacker even in case of a successful attack.*

Keywords *- Cloud security, fragmentation, RSA, blowfish, buckets.*

I. INTRODUCTION

We are living in a digital era. Cloud computing has become an eminent part of the IT industry in the past couple of years. As a result of its economic benefits, more and more people are heading towards cloud adoption [3]. Various online threats exist that may compromise and steal your data, money, and even your entire identity. Any systems connected to the internet are exposed to many potential cyber-attacks from different outside adversaries who are targeting the systems and open communication channels, either to steal sensitive information or to disrupt the critical information system. Cloud computing is characterized by on-demand self-service, ubiquitous network accesses, resource pooling, elasticity, and measured services. The characteristics mentioned above of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. Security is one of the most crucial aspects prohibiting the widespread adoption of cloud computing [1]. Cloud computing is now a primary driver of the world's digital economy [2]. For a cloud to be secure, all participating entities must be secure, and the data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate). At the same time, the cloud offers lower costs, scalability, and flexibility and expands a company's risk profile exponentially. Attackers continually refine their techniques to take advantage of the millions of identical binary templates for virtual environments that power those cloud benefits [2]. This project proposes a division of data in the cloud for optimal performance and security. We divide a file into fragments, and security is provided to the fragmented data using RSA and Blowfish algorithms, and fragments are moved over the cloud nodes. Each node stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attackers.

II. EXISTING SYSTEM

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated, and managed by a cloud storage provider on a storage server built on virtualization techniques. This cloud is public; the user can store the file in the cloud storage and provide security by encrypting the file.

III. PROPOSED SYSTEM

Our primary objective is to provide security to the cloud data up to the limit. Security of data is the main concern in our day-to-day life. Everyone wants their data to be secure. But it is not possible to provide 100% security to data present in the cloud. Our proposed system provides security to the cloud data up to the limit by dividing the file into different fragments and providing security to each fragmented part, and uploading it into different buckets on the cloud. The division of a file into fragments is performed based on given user criteria such that the individual fragments do not contain any meaningful information. A successful attack on a single fragment must not reveal the locations of other fragments within the cloud. In this system, the RSA algorithm is used to encrypt the data, and the blowfish algorithm is used as a salt which provides extra security to the data. This scheme ensures that no meaningful information is revealed to the attacker, even in the case of a successful attack.

A. Fragmentation of file

Fragmentation of files ensures that no meaningful information is revealed to the attacker even in case of a successful attack. We fragment the file into different parts of different sizes according to the user. Users can fragment the file of the required size, and that fragmented part will be uploaded to different buckets into the cloud. If an attacker is uncertain about the locations of the fragments, the probability of finding fragments is very low [8].

B. RSA Algorithm

An algorithm is a procedure or formula. The idea was first discovered in 1973 by a member of the British government named Clifford Cocks. In cryptography, everything starts with data that can be read without extra effort, referred to as "plain text ."The method of converting plain text into unreadable gibberish called "cipher-text" is encryption. The process of reverting the gibberish into original plain text is called decryption. Cryptography is the science of using mathematics to scramble and descramble information. Cryptographic algorithms called "ciphers" and "deciphers" are used for encryption and decryption.

The steps of the RSA algorithm [4] are,

1. Key Generation

1. Choosing two very large prime numbers, p, and q.

2. Compute their system modulus, n= p*q and the 'totient' function ф (n) =(p—1) (q —1). Note that the factors p and q remain secret, and n is public.

3. Select the encryption key e at random, so that gcd(e,ф(n)) =1, where 1 < e <ф (n).

4. Solve the following equation to find the decryption key d:

e.d=1 mod ф (n), where 0 <=d<=n.

5. Publish the public encryption key:

PU = {e, n}, which is known to everyone.

6. Keep secret or private the decryption key:

PR = {d, n}, which is known only to the person who has to decrypt or sign the message.

2. Data Encryption

1. Input the plain text or message M, where 0<= M <=n.

2. Obtain the public key of the recipient, PU = {e, n}.

3. Compute the cipher C using the following equation: C= M^e mod n

3. Data Decryption

1. Input the cipher-text C.
2. Use their private key, PR= {d, n}.
3. Compute the message M using the following equation: M= C^d mod n

a. Blowfish Algorithm

Blowfish is a symmetric block cipher. It takes a variable-length key, from 32 to 448 bits, making it ideal for domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then, it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free and is available free for all uses. Blowfish is a block cipher that encrypts data in 8-byte blocks. The algorithm consists of a key-expansion part and a data-encryption part. Key expansion converts a variable-length key of at most 56 bytes (448 bits) into several subkey arrays totaling 4168 bytes. Blowfish has 16 rounds. Each round consists of a key-dependent permutation and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

IV. WORKING

Coming to the working of the proposed system, the project works with the help of cloud servers. In our proposed system, the user will select the file. Divide the file into different fragments according to the user requirements. Security is provided to these fragments using the RSA algorithm. Extra security is provided to each fragmented part by using the Blowfish algorithm. All these fragments of information will be stored in an xml document created by the user. Later all these fragments are uploaded to the cloud. Users can download the fragments from the cloud with the help of the previously created xml document, which will be present only with the user. All these fragments are merged with the help of the xml data.

Fig 1: Flow diagram of the proposed system

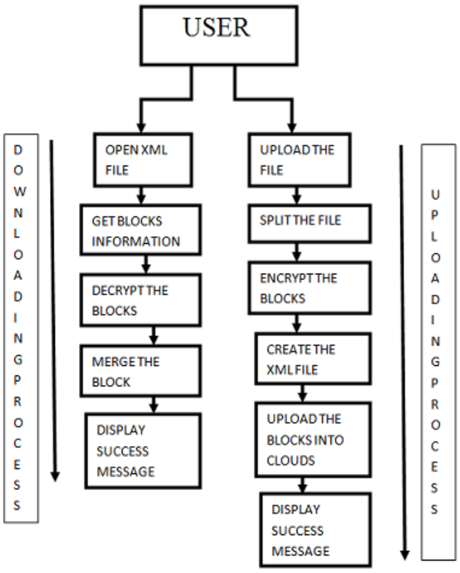
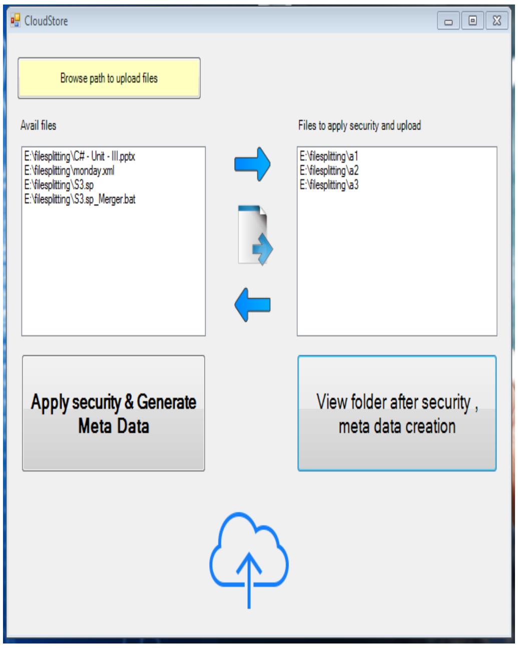


Fig 1 represents the flow diagram that explains the complete working of the proposed system. Here the work is divided into two parts. The first part is Uploading Process, and the second part is Downloading Process.

A. Uploading process


CloudStore
Browse path to upload files
Avail files
Files to apply security and upload
Apply security & Generate Meta Data
View folder after security , meta data creation

E:\filesplitting\C# - Unit - III.pptx
E:\filesplitting\monday.xml
E:\filesplitting\S3.sp
E:\filesplitting\S3.sp_Merger.bat

E:\filesplitting\a1
E:\filesplitting\a2
E:\filesplitting\a3

Fig 2: Uploading Process

Fig 2 represents the uploading process of the proposed system. In this process, the first user will browse the file in the system that they want to upload into the cloud to provide security. After browsing the file user will split that file into different blocks of different sizes. Then the user will encrypt each block's data by applying the RSA algorithm. After that, salt will be added using the blowfish algorithm to provide more security. After providing security to all blocks, we will create an xml file that will contain all information about the blocks. This means it will contain information like which block has how many bytes, starting byte and ending byte, etc., so we can get split information from metadata. After that, we will access the cloud server and upload the blocks into the cloud. After successfully uploading the file, the success message will be sent to the user.

B. Downloading process

In this process, the first user will open the xml file holding metadata and get the information about the file they want to download. Then corresponding data will be decrypted by a private key generated by the RSA algorithm. After that, blocks will be merged, and the user will get the required file. After successfully downloading the file, the success message will be sent to the user.

V. FUTURE WORK

This paper presents a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption. Hybrid encryption is a mode that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as the public and private keys are fully secure [7]. We propose ensuring data security and privacy by fragmenting the data and implementing different encryption techniques in this system. The system also uses a salting technique which even strengthens the entire encryption process. In the future, we wish to incorporate definite steps that would enhance the efficiency and generality of our system. This system can be enhanced by providing much more security with more investment. This could be in the form of extending our system to work for a multi-cloud environment and adding certain backup and recovery features to prevent data loss in case of an attack.

VI. CONCLUSION

In the Proposed system, a cloud storage security scheme collectively deals with the security and performance in terms of retrieval time. The fragmented data file and the fragments were secured using RSA and Blowfish algorithm. Then those fragments are dispersed over multiple buckets overcloud. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack.

REFERENCES

[1] DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, BharadwajVeeravalli, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE. IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 6, NO. 2, APRIL-JUNE 2018.

[2] https://www.cloudcomputingnews.net/categories/hacking/

[3] https://ieeexplore.ieee.org/document/7943164/

[4] https://simple.m.wikipedia.org/wiki/RSA_algorithm

[5] https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html

[6] https://www.schneier.com/academic/archives/1995/09/the_blowfish_encrypt.html

[7] https://www.techopedia.com/definition/1779/hybrid-encryption

[8] https://www.academia.edu/33494330/Optimal_Performance_and_Security_in_Cloud_Using_Division_and_Replication_of_Data