International Journal of Engineering & Technology, 7 (4) (2018) 4250-4252

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet. v7i4.15597
Research paper

Blowfish encryption on cloud data storage

DegalaDivyaPriya [1 *], BethalaShirisha [1], B. Pravallika [2]

[1] Assistant Professor, Department of CSE, CMR Institute of Technology, Hyderabad
[2] Assistant Professor, Department of IT, Institute of Aeronautical Engineering, Hyderabad
**Corresponding author E-mail:divya.degala@gmail.com*

Abstract

Cloud computing stores large amount of data and it acts as a resource pool with a network of large number of computers. To secure large volumes of data stored in cloud we can make use encryption techniques. Encryption is used to encrypt the data into cipher data andsecurely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential data from unauthorized access.We introduce a block-based transformation algorithm based on the combination of data and a well known encryption and decryption algorithm called Blowfish. In this paper we have discussed about cloud computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of blowfish security algorithm.

Keywords: *Blowfish; Cloud Computing; Cipher Text; Decryption; Encryption.*

1. Introduction

Cloud Computing is the ability to access a pool of virtual resources owned ,maintained and accessed by group of users along the network. The "cloud" is group of hardware, storage, networks, interfaces, and it provide services to the users on demand and it can also provide access to the applications which are on different locations.
It is a model for providing convenient and on demand network access to a shared pool of resources. There are three service models.

i) Software as a service (SaaS): It provides application LinkedIn over a network for any user to download or use it by network.

Ex: Google docs, Acrobat.com, Salesforce.com

ii) Platform as a service(PaaS):The user has to deploy his own application and sell it to others and make use it for their self

Ex: Microsoft azure, Google App Engine

iii) Infrastructure as a service (IaaS): It is the lowest part in a pyramid. It consists of hardware for storage, network capacity and power and other computing resources. This is a pay per use on demand.

Ex: Amazon Web Services

As a service in cloud, consumers can rent terminology as a service means that it on demand over the internet rather than purchase.

a) Advantages

- Apparent capital expenditure
- Efficiency. Enterprise users can get applications to market quickly, without worrying about underlying infrastructure costs or maintenance.
- Flexibility. Users can scale services to fit their needs, customize applications and access cloud services from anywhere with an internet connection.
- Strategic value.

b) Deployment models in cloud

i) Private Cloud: It individually owned by a company for its own use due to security reasons and didn't share information to other customers. It can be local in house/provider Side server storage reserved for only one entrepreneur.

ii) Community cloud: Share resources for one particular community such as banking / pharmaceutical toshare one particular similar need for security regularity concern
Ex: all pharmaceutical might rent/buy cloud.

iii) Public cloud: This is sold to mega scale public. It is free for all cost is free .It is open to all kinds of users, inherently all the users can share the data so the security ca least.

iv) Hybrid cloud: By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

c) Characteristics in cloud

They are explained as follows

- On demand self service: Here the provider will not have too much of command
- Broad network access: Access to the network will be broader
- Resource pooling: it provides resources many users access the data through network.
- Rapid elasticity: Scalable able to contract or expand over estimated or under estimated doesn't occur.
- Utility computing: It is the main characteristic of cloud.

d) Benefits of cloud

- Agility
- storage capacity
- performance
- High availability
- Protecting and securing data in cloud is not an easy task.

Copyright © 2018DegalaDivyaPriya et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

e) To secure data on cloud

- Encryption:-Data governance and regulatory compliance issues. Organization can maintain and high control of data through intelligent application of encryption across the cloud infrastructure.
- Better visibility:-Must have full knowledge and visibility in to how your data is protected
- Shared responsibility: Hypervisors, cloud providers, switching fabric, applications, physical servers understand each and every responsibility and secure the cloud data.

2. Security challenges in cloud computing

Set of challenges:

- Physical ownership
- access to servers
- Rely on cloud provider security.
- Many cloud providers data security is not their problem.

1) Cryptography

There are two types of cryptography

a) Symmetric key cryptography: Symmetric key cryptography is also known as private key or secret key cryptography. In this cryptography one key is used to encrypt or to decrypt the data.

It is denoted as P=D (K, EP ()).

Where P=Plain text, EP()=Encryption of plain text, D= Decryption, K=Key.

Here both sides must agree upon the secret key before the starting of the transmission and they should maintain it secretly. They have use the same key at the time of encryption and decryption.

This is usually known as Blowfish algorithm and Data Encryption Standard.

b) Asymmetric key cryptography: Asymmetric key cryptography is known as conventional cryptography system or public key cryptography.

In the public key cryptography two keys are used , one key is used to encrypt the data and the other to decrypt the data.

It is denoted as $P=D(K_d,E(K_e,P))$

where P=Plaintext, E(P)=Encryption of Plain text, D=Decryption K_e and K_d=Encryption key and Decryption key.

Here both sides will have 2 keys to decrypt and encrypt the data.

It is mainly used in Diffie Hellman Key exchange and Rivest Shamir Adlman algorithm.

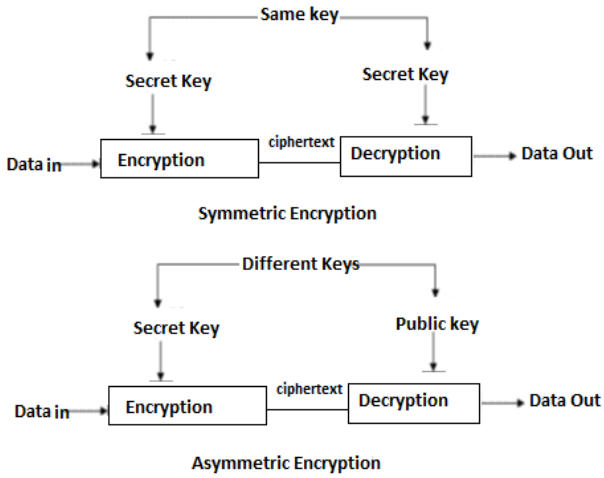


Fig. 1: Symmetric and Asymmetric Encryption.

3. Proposed algorithm

Blowfish algorithm for encryption and decryption: Bruce schneierin a symmetric block cipher 1993 encryption algorithm used in modern cryptographic software. It is as an alternative for AES,DES and 3 DES.it is a symmetric block encryptionalgorithm Plain text will be a input and 18 keys need to give for performing encryption.13 internal rounds will be done and plain text is a 64 bit data and this data is divided in to two 32 bits and performing a encryption process.

a) Design Implementation:

Blowfish encrypts data large 32-bit microprocessor.

- It can run in low memory
- It uses simple addition, XOR, lookup.
- It is more secure because the key length is variable.
- Blowfish encrypts 64-bit block data at a time depending on hefeistel network and it is divided into 2 parts:

b) Key expansion

Blowfish converts 448 bits into several sub key array

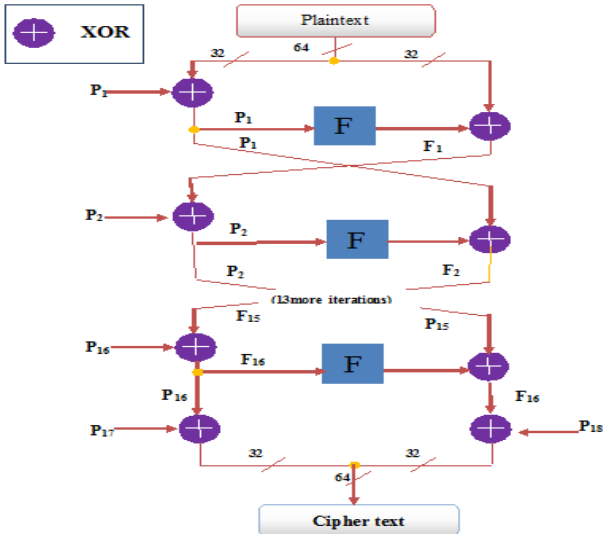
Step 1: Initialize the p-array that consists of 18-32bits and s-boxes consists of 255 bits.

Step 2: Perform x-or operation on p1.32 bits key to p2 32 bits .repeat this operation for all the p-array.

Step 3: Encrypt the data using blowfish algorithm, which makes use of sub keys.

P1& p2 are replaced.

Step 4: Encrypt the output of step44 by using blowfish sub keys.



Pseudo Code:

Step 1→Divide X in to two 32 bit.

Step 2 →X_L,X_R

Step 3 →For i=1 to 16;

Step 4 →X_L =X_L XOR Pi

Step 5 →X_R=F(X_L)XOR X_R

Step 6 →Swap X_L and X_R

Step 7 →X_R=X_R XOR P17

Step 8 →X_L =X_L XOR P18

Cipher text:-concatenation of X_L and X_R

Divide X_L in to four 8-bit parts

Step 9 →$F[X_L]=((s1[a]+s2[b] \bmod 2^{32})+ S3[c])s^4[d] \bmod 2^{32}$

c) Data Decryption

We use similar encryption techniques to decrypt the data. But the only change is that we use the sub-keys P1 to P18 in exactly the reverse order as that of encryption.

d) Generation of Sub-keys

The Blowfish algorithm uses more sub-keys. In Blowfish the key are pre computed before doing either encryption or decryption techniques, if it is not done then the speed will be slower. However, the encryption is still possible irrespective of computation.

Consider P is an array of 18, 32-bit integers. S is an array of 32 bit integers which has dimensions 4x256. We initialize the P-array and only after that, we will initialize the S-boxes in this order only, with a fixed string consisting of hexadecimal digits of pi.

1st step of P-array (P1) = 8k bits

2nd step of P-array (P2) = 8k bits

3rd step of P-array (P3) = 8k bits
Fourth step of P-array (P4) = 8k bits etc. one.
Here, we perform XOR P1 with the first 32 key bits, XOR P2 with the next 32 key bits and so on. We continue to do this until all elements of the P-array has been XOR'd by the key bits. 2. Then we encrypt the zero string using these sub-keys with the Blowfish algorithm.

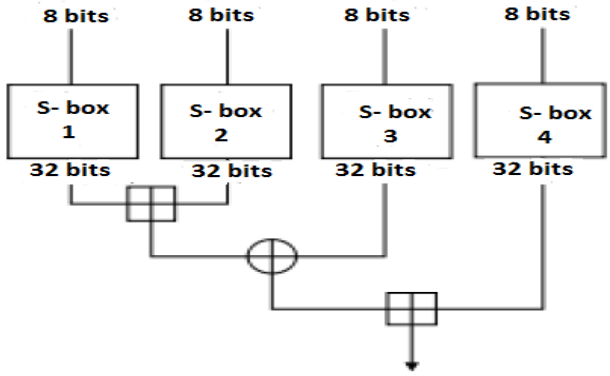


Fig. 2: Generation of F Function

4. Advantages

1) It is one of the strong encryption techniques.
2) Blowfish is patent as well as royalty free. Any user can use it.
3) It is the fastest encryption algorithm with the speed of 26 clock cycles per byte.
4) It is very compact with less than 5 KB of memory needed.
5) It is also secure due to variable length secret keys.

5. Disadvantages

1) It is easily attacked if we are using weaker keys.
2) It can be cracked only using brute-force attacks if 256 bit keys are not used.
3) This encryption is not possible for larger files because of small 64-bit block size.
4) In advance to blowfish we are having many techniques like Two fish, Three fish and AES etc. but not popular as blowfish

6. Conclusion

We discussed that the need of encryption algorithm to store or retrieve data on cloud. There are many encryption algorithms. In that one of the fastest encryption algorithm is blowfish encryption algorithm .Blowfish perform data encryption very efficiently.it generates 64 bit keys which are very efficient. In blowfish algorithm to compress code we can make use of Huffman coding.by using this encryption techniques we can encrypt data securely and efficiently and it also reduce consumption of battery power device.in future we can enhance the decryption techniques and non-repudiation. If we can increase the key size it can provide better authentication.

References

[1] Armbrust, Fox, Griffith, Joseph, "*Above the clouds: A Berkeley view of cloud computing*"[2009].
[2] Buyya, Venugo, "*Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility*", [2008].
[3] Caceres, Lindner, Vaquero, "*A break in the clouds: towards a cloud definition*", [2008].
[4] Keahey, Fortes, Freeman, "*Science Clouds: Early Experiences in Cloud Computing for scientific applications*" [2008].
[5] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," *Pakistan Journal of* Information *and Technology*. Vol. 2, no. 2, 2003, pp. 191-200. http://www.ansinet.org/
[6] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. *Proceedings of Advanced Concepts for Intelligent Vision Systems*, 2002.
[7] Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", *International Journal of Computer Trends and Technology*, ISSN: 2231-280, July to Aug Issue 2011.
[8] Irfan Landge, Burhanuddin Contractor, Aamna Patel and RozinaChoudhary "Image encryption and decryption using Blowfish algorithm" Proceedings of the 2012 National Conference of Emerging Trends in Information Technology, Shirpur, Maharashtra, April 21 , 2012.
[9] http://www.embedded.com/ design/configurable-systems/ 4024599/ Encrypting-data-with-the-Blowfish-algorithm
[10] https://www.schneier.com/paper-blowfish-fse.html
[11] https://en.wikipedia.org/wiki/Blowfish_(cipher).