ISSN: 0974-5823 Vol. 7 (Special Issue 5, April-May 2022)

International Journal of Mechanical Engineering

SECURITY IN CLOUD COMPUTING USING BLOWFISH ALGORITHM

[1]**Vinod D. Rajput** Asst. Professor, In-Charge Dept of Computer Science, B. K. Birla College (Autonomous), Kalyan, Maharashtra State, India

[2]**Kajal D. Jaisinghani** Asst. Professor, Dept of Computer Science, B. K. Birla College (Autonomous), Kalyan, Maharashtra State, India

ABSTRACT

Cloud computing is a resource pool with a huge number of machines that stores massive amounts of data. Encryption techniques can be used to secure massive amounts of data in the cloud. Encryption is a technique used for converting data into encrypted data and securely transmitting data over public networks. As each type of data has its own characteristics, multiple strategies are used for protecting confidential information from illegal access.In this paper we discussed about block-based transformation approach that combines data with the Blowfish encryption algorithm. We also examined cloud computing security difficulties, applications that use this algorithm for secured data transmission, and as well as a metaphoric analysis of the blowfish security algorithm.

Keywords: Security Algorithm,Blowfish,Encryption,Decryption,Block based transformation.

1.INTRODUCTION

Cloud computing refers to data that is stored in the cloud and accessed by clients via virtual servers and mobile devices. With the availability of an internet connection, cloud computing infrastructures have created a mechanism for users to conveniently store and access data. Cloud computing maintenance and technical services are given by cloud providers, who are responsible for ensuring that the services are of high quality. Schools, businesses, financial institutions, dealers, and government offices have benefited from cloud computing's improved storage capabilities.

Cloud computing is a model for big data that allows access to a network of heterogeneous virtual services that can be supplied and delivered quickly with little effort or with the interaction of a service provider. The information technology industry has seen potentially significant changes and significant enhancement as a result of cloud computing. It comes in handy in the majority of networked operations. Data security, privacy, confidentiality, validity, integrity, and durability are the most typical issues with cloud computing.It is a concept for offering access controls to a common collection resource pool that is both accessible and available on demand.

Service Models In Cloud

i)Software service (SaaS): This service allows any user to download oruse the Networking application over the internet. For example, Google Documents, Youtube, and Google Spreadsheet.

ii) Platform as a service (PaaS): The service gives the platform to the user to build their own software through this interface and by providing virtual back end and front end tools, sell it to others, and utilize it themselves.

iii)Infrastructure as a Service (IaaS): The bottom of the hierarchy. It is made up of storage hardware, network capacity and power, as well as other computational resources. This is a pay-per-use service that is available on demand. Consider Amazon Web Services.

Deployment Models In Cloud

i)Private Cloud: Due to security concerns, a corporation has a private cloud for its own use and does not share information with other clients. It could be a local in-house/provider option. Only one entrepreneur has access to the side server storage.

ii) Community cloud: Share resources for a single community, such as banking or pharmaceuticals, to meet a common demand for security and consistency. For example, all pharmaceuticals pay or purchase cloud.

iii) Public cloud: This service marketed to large groups of people. It is free of charge at all times. It is accessible to a wide range of users, and because all users can exchange data by default, security is minimized.

iv) Hybrid cloud: Hybrid cloud gives a platform to connect both public and private cloud.

When a user keeps critical information on a cloud server, they do not have direct control and maintenance of the information security; this becomes a major concern in cloud environments.It is necessary to keep the data secure at all times. If three conditions below are met then it means information is secure.

Confidentiality is defined as the safeguarding of data by not revealing it to others in order to prevent any illegal access to confidential information.Integrity implies that the data received should be similar to what the sender transmits; this prohibits unauthorized users from altering the data. The term "availability" refers to the guarantee that a user can access information at any time and over any connection.

Cryptography is used in cloud computing to protect confidentiality. Cryptography is the science of maintaining information safe, and it plays a critical role in data security versus common threats and minimizing the danger of data theft. The extraordinary usage of digital communications, online economic transactions, and online payments has released tremendous potential in terms of security challenges and cryptographic assaults; hackers are certainly becoming more skilled year in year out.

Algorithms of Cryptography

a) Symmetric key Algorithm

In this type of algorithm only one secret key is used for both encrypting the data and decrypting the data.Here both sender and receiver should agree the key before starting the communication and they should maintain the secrecy of the key .Blowfish and DES Algorithm are example for Symmetric key algorithm.

P=D (K, EP ()).

Where P=Plain text,

EP()=Encryption of plain text,

D= Decryption, K=Key.

b) Asymmetric key Algorithm: A Conventional cryptography in which two keys are used one for encrypting the data and other for decrypting the data. Asymmetric key cryptography is mainly used in Hellman Algorithm..

P=D(Kd,E(Ke,P))

where P=Plaintext,

E(P)=Encryption of Plain text,

D=Decryption

Ke and Kd=Encryption key and Decryption key.

2.THE BLOWFISH ALGORITHM

The Blowfish algorithm is the Symmetric Key Cryptographic algorithm,which is noting but only one security key is used for both encrypting data and decrypting data..This algorithm was developed by Bruce Schneier in 1993.This algorithm is otherwise called as Blowfish Cipher or Blowfish Encryption.This algorithm is initially developed and placed in the open public domain,,this means no one needs his permission to use this algorithm.he did not patient the algorithm and he did not received single bug for this algorithm.

With the advancement of the networking,people began using the internet for a variety of private purposes.It means that there should be some sort of data protection while transmitting data through the internet.Encrypting the data before transmitting through internet is prefered by most internet users to secure their confidential data.Bruce Schneier was the first person to develop the Symmetric Key Cryptography algorithm.Symmetric encryption is a technique in which data is encrypted and decrypted before transmitted through the internet by using a single security keysThe encryption key is in charge of encrypting the data; whatever encryption algorithm you use, it's worth remembering that the encryption key must be complex and dependable.By using this Blowfish algorithm ,only a one key is used for both encrypting and decrypting the of informatiom.As the result key generated for encryption is used for decryption of data.This algorithm helps in encrypt a huge amount of data in short time.Once you create encryption structure in this same structure of algorithm is used for decrypting the data.Feistel structure cipher is used in this algorithm,which is nothing but function F is involved which is a constant function.

3.ADVANTAGES OF USING BLOWFISH ALGORITHM IN CLOUD

License-Free

Blowfish encryption is freely available in the public domain.is the first consideration. It is currently the fastest block cipher accessible for free. As a result, it's a great fit for a variety of computer and mobile data transmission. Every second, this algorithm encrypts vast amounts of data in order to give us information on a daily basis.

Feistel Structure

Feistel is a technique for quickly converting any function into linear order. It is still one of the finest linear ordering strategies in block cipher-based encryptions in 2021.

4.ALGORITHM SPECIFICATION

The Blowfish Symmetric Key Algorithm encrypts 64-bit blocks at a time. The Feistel network is used by the algorithm. Blowfish uses a 32-bit microcontroller to encrypt data. This Algorithm can run on a low-memory system. Simple addition, XOR, and lookup technique are employed. The key length is flexible, which makes it more secure, depending on the complexity of the input.

- **KeySize: 32-bits to 448-bits variable size**
- **Number of subkeys: 18 [P-array]**
- **Number of rounds: 16**
- **Number of substitution boxes: 4 [each having 512 entries of 32-bits each]**

5.DATA ENCRYPTION

The BLowfish Algorithm constructs a function that iterates the network 16 times. Each round includes a key and data-dependent rearrangement as well as a key and data-dependent substitution. On 32-bit words, all operations are XORs and additions.

Step1:Initial step of this algorithm is to fix a key array with the size of 18 and 4 subsitional boxes with a maximum of 256 entries and in size of 32 bit are initialized for each p-array. Each Key string should be in the form of hexadecimal digits .

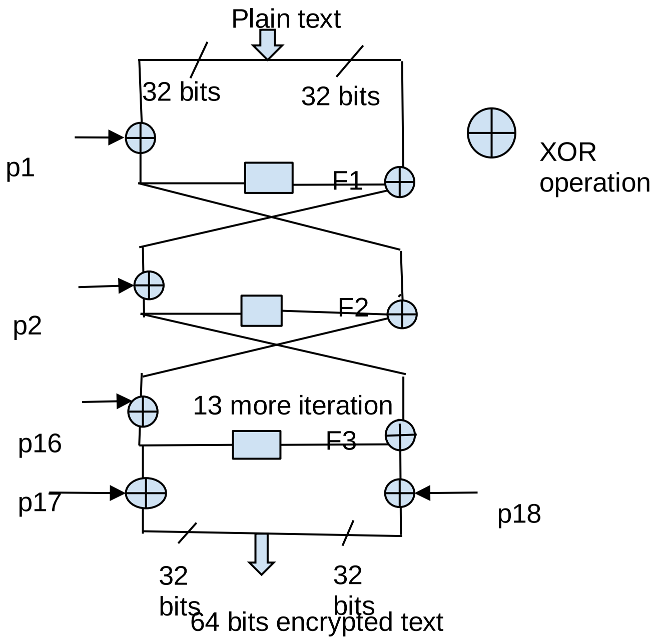
Step2: For the first iteration ,input data of size 64 bits is divided into two 32 bit data asLX andRX.Then LX is XOR with P1 key and then the output LX1 is given as input to the F function.

Step3:Inside F function we have four s boxes of size of 32 bit each,8 bit input is given to each four s box and 32 bit output generated by each sbox,output of s1 box is added with s2 box and then s3 and s4 boxes are also added finally these two added outputs are XOR to get final encrypted dat

Step4:Output of F function is XOR with another 32 bit input R X to get out put RX1.

Step5: The Output LX1 and RX1 is swapped and given as the input for next iteration

Step6:This process is iterated by replacing all entries of the P array, and then all four S-boxes in order, with the frequently changing Blowfish algorithm. These steps are completed after 18 rounds of iteration and finally 64 bit ciphertext is received from the output XL17and XR17.



WORK FLOW DIAGRAM OF BLOWFISH ALGORITHM

Pseudo Code of Blowfish Algorithm

```
for i = 1 to 16:
LXi = LX  XOR  Pi
 RXi= F(LXi) XOR RX
 Swap LXi and RXi
After the sixteenth iteration,
Swap  LX and RX again to undo the last swap.
RX= RX XOR P17 and LX = LX  XOR P18.
Recombine LX and RX  to get ciphertext
```

Data Decryption

Decryption is identical to encryption, with the exception that the P array is used in reverse order. Blowfish implementations requiring that the quick speed of the algorithm should not damage the performance of the loop and verify that all subkeys are cached.

6.BLOWFISH ALGORITHM APPLICATIONS

Password Management: Usually we use password to login to cloud based applications and services.Such as social media websites like twitter,Facebook,Instagram,Tumblr,etc,.to commercial websites like Amazon,EBay,Flipkart,etc.All these cloud platforms use this techniques to maintain user's credentials.Another important aspect of using password management by this algorithm is that users need not find and use a new password every time when they log in to any application.The Blowfish algorithm used in password protection is completely reliable. If you want to make sure that your password and login information are safe, you can go through two step verification process.First is that corresponding web application will send you an OTPl if corresponding OTP send by the organization and received by you are same then your your information are quite safe.This two step verification is done by symmetric encryption algorithm.

Backup Tools: Software that backup organization’s data should be more secure in a cloud environment.The backup should be secured in that way that no attacker can easily trespass in to back up data to hack your data or delete it. Most of the backup software like Backup for Workgroup andSymantec NetBackup use Blowfish encryption algorithm to safeguard the data.

Miscellaneous: Before granting access to cloud computing services, the Blowfish technique is employed for user authentication.This algorithm provides high security to cloud data which is hosted from the remote area.In addition to this email encryption can also be done by this algorithm.

Operating System: The open source operating system like Linux use the Blowfish algorithm to produce their data and users from the cyber attack.Linux is one of the preferred OS options for white hat hackers.OpenBSD is the other OS which seek help from this algorithm.

File and Disk Encryption: As this algorithm is good enough to encrypt huge amounts of data in a short span of time ,files present in the organization's server can easily encrypt those data without any complexity.When companies try to encrypt or decrypt huge amounts of information in a short span they require better software with good algorithms to implement this. GnuPG, Bcrypt, and CryptoForge are examples of industry-leading disc encryption applications that use blowfish algorithms.

7.CONCLUSION:

In this paper , we explained about the use of an encryption algorithm while storing or retrieving information on the cloud. Blowfish encryption algorithm is one of the fastest encryption algorithms. Blowfish is a very efficient data encryption algorithm. It creates 64-bit keys, which are extremely efficient. Huffman coding is a technique used in the blowfish algorithm to compress data. By employing these encryption approaches, we can encrypt data safely and effectively while also lowering the device's battery consumption. We can improve decryption algorithms and non-repudiation in the future. It is possible to improve authentication by increasing the key size.

References

[1] B. Joshi, Karuna P, Theofanos, Mary, And Stanton, ―Framework for Cloud Usability NIST Special Publication 500-316 Framework for Cloud Usability,‖ pp. 1–18, 2015.

[2] H. Takabi, J. B. D. Joshi, and G. J. Ahn, ―Security and privacy challenges in cloud computing environments, IEEE Secur. Priv., vol. 8, no. 6, pp. 24–31, 2010.

[3] L. Ertaul, S. Singhal, and G. Saldamli, ―Security Challenges in Cloud Computing,‖ 2010.

[4] T. Ramaporkalai, ―Security Algorithms in Cloud Computing SECURITY ISSUES OF CLOUD,‖ vol. 5, no. 2, pp. 500– 503, 2017.

[5] R. Ahmed and M. L. Ali, ―Minimization of Security Issues in Cloud Computing,‖ 2017.

[6] C. Paper and K. P. Siemens, ―Cloud computing security issues and challenges,‖ no. June 2010.

[7] R. Kaur and R. P. Singh, ―Enhanced cloud computing security and integrity verification via novel encryption techniques,‖ Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014, pp. 1227–1233, 2014.

[8] M. Shashi, ―Cloud Computing Models : Background, Data security, & Security Issues,‖ vol. 2, no. 2, pp. 1–6, 2017.

[9] H. Kaur, ―A Novel Technique of Data Security in Cloud Computing based on Blowfish with the MD5 method,‖ vol. 3, no. 6, pp. 828–837, 2017.

[10] A. Pansotra and S. P. Singh, ―Cloud security algorithms,‖ Int. J. Secur. Its Appl., vol. 9, no. 10, pp. 353–360, 2015.