International Journal of Scientific and Technical Research in Engineering (IJSTRE)
www.ijstre.com Volume 5 Issue 5 ǁ Nov-Dec 2020.
ISSN: 2581-9941

Cloud Computing and Cloud Security Using Symmetric Encryption Algorithms

N Shivali
Department of Electronics and Computer Engineering Sreenidhi Institute of Science and Technology

Abstract: Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet).Cloud computing allows users can access files and use applications from any device that can access the Internet. Cloud computing facilitates the access of applications and data from any location worldwide and from any device with an internet connection. Cloud computing offers various types such as private cloud, public cloud and hybrid cloud solutions each with different features. Organizations can choose these options depending on what best serves their purpose. Cloud computing is helping the society to cope with future problems such as managing big data, cyber-security and quality control.

I. Introduction

The "cloud" is a set of different types of hardware and software that work collectively to deliver many aspects of computing to the end-user as a service over the internet. It can serve many facilities to the business such as resources, infrastructure, platform etc by paying amount on demand basis over network with the functionality of increase or decrease the requirements. This technology can meet any IT requirements at any time. It can serve most of the hardware and software facilities required for companies for storing, creating, managing, running consumer applications on cloud in lease or rent basis, it provides resources as a service to multiple consumers by virtualization. Cloud computing consists of three distinct types of computing services delivered remotely to clients via the internet. Clients typically pay a monthly or annual service fee to providers, to gain access to systems that deliver software as a service, platforms as a service and infrastructure as a service to subscribers. Cloud computing also offers the most efficient means for small, medium and even large enterprises to backup and restore their data and applications in a fast and reliable way. Various cloud service providers are Amazon, Google, IBM, Microsoft, and Salesforce.com, offer their cloud infrastructure for services.

II. Cloud security

The complexity of cloud computing create many issues related to security as well as all aspects of Cloud computing. Cloud security is the protection of data stored online from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, insecure application program interfaces (APIs), poor choice of cloud storage providers, and shared technology that can compromise cloud security. Cloud security consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.

III. Encryption algorithms

Encryption Algorithms have an important role in the data security of cloud computing. Examples of algorithms are AES, DES, RSA, Homomorphic etc. Two operations performed by these algorithms are encryption and decryption. Encryption is the process of converting data into scrambled form and Decryption is the process of converting data from scrambled form to human readable form. Symmetric algorithms use one key for encryption and decryption while Asymmetric algorithms use two keys for encryption and decryption. Symmetric uses single key, which works for both encryption and decryption. Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).In asymmetric-key algorithms different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme. Each receiver has a decryption key of its own, generally referred to as his private key. Receiver needs to generate an encryption key, known as his public key. Generally, this type of cryptosystem involves trusted third party which officially declares that a particular public key belongs to a specific person or entity only.

IV. Blowfish algorithm

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish requires about 5KB of memory. It uses the same key for encryption and decryption. Blowfish works with keys up to 448 bits in length. Here, plaintext is the message you're trying to transmit. The process of encryption converts that plain text message into cipher text. P is an array of eighteen 32-bit integers. S is a two-dimensional array of 32-bit integer of dimension 4x256. In this description, a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value P', run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value F'. F' then replaces the "left" half of the message and P' replaces the "right" half, and the process is repeated 15 more times with successive members of the P-array. The resulting P' and F' are then XORed with the last two entries in the P-array (entries 17 and 18), and recombined to produce the 64-bit cipher text. The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is ciphertext. The P-array and S-array values used by Blowfish are pre-computed based on the user's key.

In effect, the user's key is transformed into the P-array and S-array; the key itself may be discarded after the transformation. The P-array and S-array need not be recomputed (as long as the key doesn't change), but must remain secret.

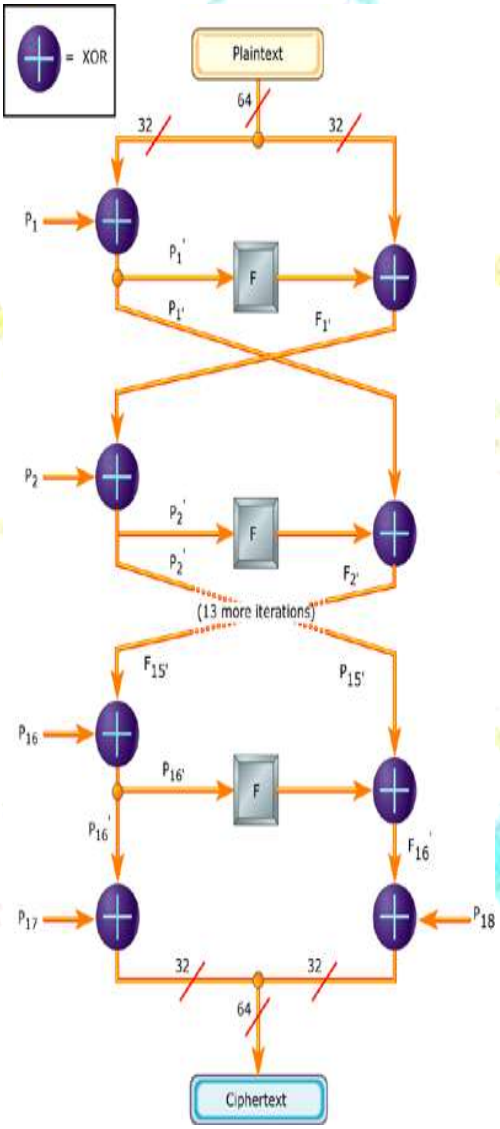

Fig 1: Blowfish algorithm

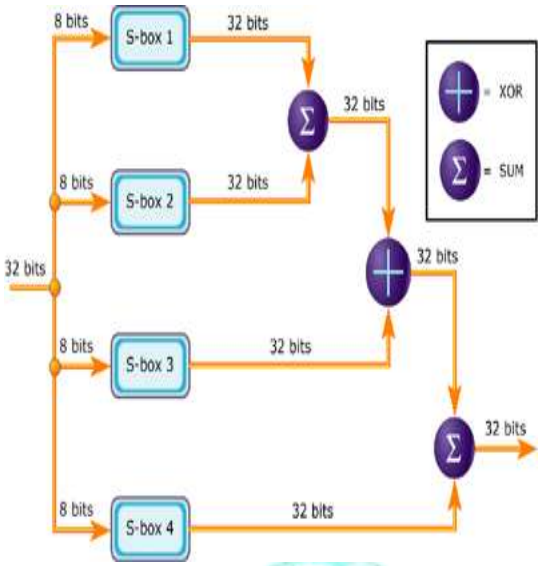

Fig 2: Graphic representation of F

V. Benefits of cloud computing

Reduced Cost

Due to large number of consumers the cost of services offered by the cloud is reduced. The services offered by the cloud are shared by multiple users.

Scalability and Flexibility

Cloud computing can assist companies to start with a small set up and grow to a large condition fairly rapidly, and then scale back if necessary. It provides the necessary flexibility required.

Backup and Recovery

Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Also it has many techniques to recover it from any type of disaster.

Broad network Access

Cloud services are delivered through open network (Internet), it can be accessible at any time anywhere in the world.

Multisharing

Cloud Computing offers services by sharing of architecture and other applications over Internet for single and multiple users by using virtualization and multi-tenancy.

VI. Challenges of cloud computing

Privacy of data

Many organizations feel that it is safe to put their valuable data in their site rather than cloud space so that privacy of their data is mainained.

Confidentiality of data

Confidentiality refers to data privacy; it ensures data is accessible only to authorised users.

Data integrity

Preservation of information from loss or modification by unauthorized users is referred as data integrity.

Data Remanence

Data should be deleted from cloud after it has completed its usage, or the memory should be reformatted or recycled.

Malicious Insiders

Malicious insiders are authorised users. These users appointed for managing and maintaining the information related to cloud.

VII. Conclusion

Cloud computing is the latest technology that promises many benefits however a lot of research is still required in this area. as many of the concerns related to security and privacy issues are not been answered by the experts and remains open. Cloud Computing is emerging widely in the field of information technology. However, there are lot of research and development in the area by the Information technology is being carried out by companies like Microsoft, Google, Cisco, IBM and soon the cloud will widespread adopted and all the security and privacy issues will be handled efficiently.

References

[1] Nasarul Islam.K.V et al, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 90-97
[2] International Journal Of Scientific & Engineering Research, Volume 7, Issue 7, July-2016 1072 ISSN 2229-5518
[3] Secure Cloud Using Cryptography Saharsh, Shubham Srivastava*, Lavanya M C Dept. of Information Science & Engineering, The National Institute of Engineering
[4] https://www.schneier.com/academic/blowfish/
[5] https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35
[6] https://www.investopedia.com/terms/c/cloud-security.asp