International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Implementation of Cryptographic Algorithm for Cloud Data Security

Prof.S.S Dhule[1], Durga Nehare[2], Komal Ballewar[3], Punam Bangade[4], Riddhi Raut[5], Mamta Sidam[6], Punam Pawar[7]

[1]M.E in Computer Science and Engineering
[2,3,4,5,6,7]Bachelor Of Engineering Scholar, Jagadambha College Of Engineering And Technology,Yavatmal,India, Department of Computer Engineering

Abstract- This paper proposes a simple, secure, and privacy-preserving architecture for inter-Cloud data sharing based on an encryption/decryption algorithm which aims to protect the data stored in the cloud from the unauthorized access.

Cloud computing is a new architecture that has released users from hardware requirements and complexity. The rapid transition toward clouds has advanced many concerns related to security issues which can hold back its widespread adoption. In fact, cloud computing special architecture has introduced many challenges especially in maintaining the security of outsourced data. Thus, to address this issue, we propose in this article, a new light weight encryption algorithm which consists of combining symmetric algorithm to encrypt data and asymmetric one to distribute keys. This combination helps to benefit from the efficient security of asymmetric encryption and the rapid performance of symmetric encryption while conserving the rights of users to access data by a secured and authorized way. Evaluation results prove that the processing time of our lightweight algorithm is faster than state-of-the-art cryptographic algorithms.

Keyword- Cloud computing, Cryptography, Encryption, Decryption, Security issue.

1. INTRODUCTION

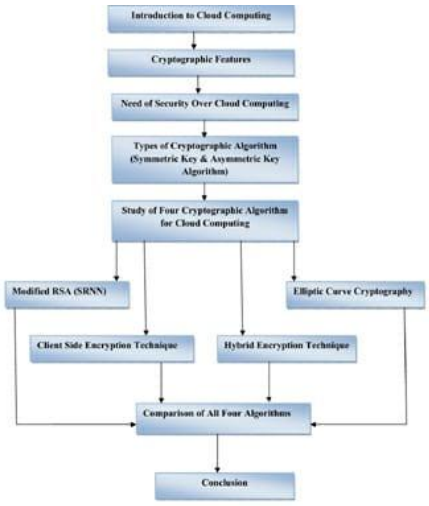
In recent years, there has been a huge proliferation of the distributed computing systems use and advancement. This increase has produced a large amount of network distributed paradigms, infrastructures and architectures such as Grid, Pervasive, Autonomic, Cloud, etc.

Cryptography is the science of securing the content of messages and communications. Cryptanalysis, the other subdiscipline, seeks to compromise or defeat the security achieved by cryptography. Mathematics is the foundation of cryptography and cryptanalysis. Cryptography is commonly associated with encryption, the transformation of data and information into a form that is unusable by a person who is not authorized to access that information. Historically, cryptography was used to protect the confidentiality of sensitive messages for military and diplomatic communications. Based on this traditional definition, cryptography can be seen as the science of encryption and decryption of messages, whose primary concern is to protect a message if it is disclosed to someone other than the intended recipient.

With the expansion of information economy where transmission of sensitive information across untrusted media has become prevalent, the use of cryptography has become common practice not only with organizations but also with individuals; the scope of data transmission

has exceeded the range of information sharing and entertainment to the core of industrial, scientific, and medical domain.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth tomake the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data fromencrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key andasymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large databaseasymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.



Comparative study of cryptography for cloud computing for data security.

Background Study

Cloud computing is an emerging technique by which anyone can access the applications as utilities over the internet. Cloud computing is the technology which comprises of all the characteristics of the technologies like distributed computing, grid computing, and ubiquitous computing. Cloud computing allows everyone to create, to configure as well as to customize the business applications online. So the cloud computing techniques need security of information communicated between the sending and receiving entities.

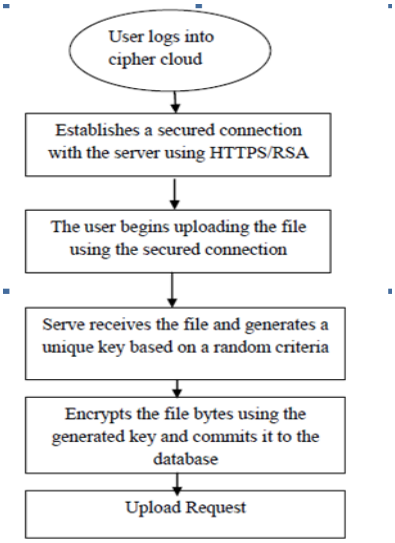
Objective of the Work

1. Protection of remote data.
2. Failure detection and prediction.
3. Availability, recovery and auditing.
4. Creating secure cloud architecture.
5. Storing and Accessing of the data from the cloud servers.

Proposed Work

The Proposed technique uses RSA and AES for the encryption and decryption. RSA uses two keys private key and public key through which a digital signature is also produced. On the other hand DES with the help of a key generation algorithm uses 256 bit keys and also apply a for loop it generates a 1024 bit private key. Now the private key of both RSA as well as DES together passes through XOR and we got output B.

To improve cloud computing protection with low processing, and high performance, a New Lightweight Cryptographic Algorithm (NLCA) for enhancing data security in cloud computing environment is pro- posed. The algorithm is simple and highly secure encryption/decryption. The proposed algorithm gives an easy structure effective for the cloud environment. There are Some well-known popular ciphers including "Camelia, SF, Blowfish and DES use the Feistel structure". The major benefit of applying Feistel architecture is that the encryption and decryption operations are almost similar.



Purpose of Algorithm

To improve cloud computing protection with low processing, and high performance, a New Lightweight Cryptographic Algorithm (NLCA) for enhancing data security in cloud computing environment is proposed. The algorithm is simple and highly secure encryption.

i. AES (Advanced Encryption Algorithms)

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information.

AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

```
Cipher(byte[] output, byte[] input)
{
byte[4,4] State;
copy input[] into State[] AddRndKey
for (rnd = 1; rnd < Nr-1; ++rnd)
{
SubBytes ShiftRows MixColumns AddRndKey
}
SubBytes ShiftRows AddRndKey
copy State[] to output[]
}
```

ii. DES (Data Encryption Security)

DES first came into use in 1976 in the United States and has since been used by a variety of parties globally. DES is a block cipher based on symmetric key cryptography and uses a 56-bit key. Although DES was considered to be very secure for some period of time, it is no longer considered to be so. In 1999, a distributed computing project was launched to break a DES key by testing every possible key in the entire keyspace, and the project succeeded in doing so in a little more than 22 h. This weakness brought about by the short key length was compensated for a period of time through the use of 3DES (pronounced triple DES), which is simply DES used to encrypt each block three times, each time with a different key.

Algorithm:

function DES_Encrypt (N, K) where N = (L, R)
N ←IP(N)
For round ←1 to 16 do
Ki ←SK (K, round)
L ←L xor F(R, Ki)
swap(L, R)
end
swap(L, R)
N ←IP-1(N)
return N
End

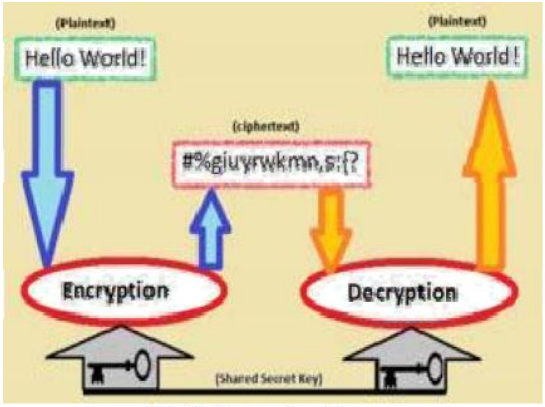


Fig 3: Encryption Process

Advantages & Disadvantages

- Advantages-

1. The two reverse operations makes algorithms more secured.
2. Simple algorithm in nature.
3. Receiving ends is easier as CRC checking present.
4. For less amount of data this algorithm works well.

- Disadvantages-

1. The network or the computer system can be attacked and rendered non-functional by an intruder.
2. Administrative controls and procedures are required to be exercised for the same.

2. CONCLUSION

With cloud computing progressing quickly, open and private associations are utilizing the cloud administrations, however protection and security issues is a major concern for them. The capacity to oversee issues is the quality of cloud computing. These previously mentioned algorithms can be executed in future to improve security over the system.

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or
denial of services etc.

3. REFERENCE

[1] A Platform Computing Whitepaper, 'Enterprise Cloud Computing:Transforming IT', *Platform*
[2] Computing, pp6, viewed 13 March 2010.
[3] K. Vijayakumar, Security Issues And Algorithms in Cloud Computing. Global journal of
[4] advanced research, Vol-2, Issue-3 PP. 569-574.
[5] Mahajan, Prerna and Abhishek Sachdeva. "A Study of Encryption Algorithms AES, DES and RSA for security." Global journal of computer science and technology 13 (2013).
[6] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. **(2011).**
[7] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
[8] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of
[9] Computer Science and Information Technology Journal, pp.179-183, 2012.
[10] J.R.N. Sighom, P. Zhang, L. You, Security enhancement for datamigration in the cloud, Futur. Internet (2017)
[11] Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthic, Hanumat Sastry, A.A
[12] (2016) Security Algorithms for Cloud Computing.
[13] Ashima Pansotra and Simar Preet Singh, A.A (2015). Cloud Security Algorithms.
[14] International Journal of Security and Its Applications, Vol.9, No.10, pp.353-360.
[15] Garima Saini, Gurgaon Naveen Sharma,"Triple Security of Data in Cloud Computing ", Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4) , 2014
[16] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii
[17] International Conference on System Sciences, pp.1-7, 2011.

[18] Kevin Curran, Sean Carlin and Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August
[19] 2011.

[20] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of
[21] Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.
[22] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, "Cloud Computing: A Perspective Study",
[23] New Generation Computing- Advances of Distributed Information Processing, Volume 28, pp.137-146, 2010.
[24] Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume
[25] 169, pp.103-112, 2011.
[26] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in
[27] Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.
[28] evin Curran, Sean Carlin and Mervyn Adams, “Security issues in cloud computing”, Elixir Network Engg.38 (2011), pp.4069-4072, August
[29] 2011.
[30] Wayne Jansen ,Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication,NIST SP - 800-
[31] 144 ,80 pp., 2011.
[32] B. Schneier, “Description of a new variable-length key, 64-bit block cipher (Blow-fish), ”1994, doi: 10.1007/3-540-58108-1_24.
[33] K. Aoki et al., “Camellia: a 128-Bit block cipher suitable for multiple platforms –design and analysis, ”2001, doi: 10.1007/3-540-44983-3_4.