International Journal of Engineering & Technology, 7 (1.9) (2018) 28-33

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Analysis and assessment of various cryptographic techniques based on a variety of features

R. Rajan [1] *, Dr. G. Murugaboopathi [2], Dr. C. Parthasarathy [3]

[1] Ph D. Research Scholar Department of Information Technology SCSVMV University
[2] AP/CSE Kalasalingam University
[3] AP/IT SCSVMV University
**Corresponding author E-mail: rajanrajavelu@gmail.com*

Abstract

Cloud computing process is an IT service invented for providing efficient network, software, hardware, storage, software systems and resource services. Cloud computing delivers service to the customers through a network. The IT and the management services involved in it is taken care by third parties that owns the physical infrastructure involved in the service. Cloud service provides us the ease to access information at any place, any time with minimum cost involved and high reliability, scalability and resilience. Because of these advantages many organizations are converting themselves to cloud. With growing demand it is necessary to consider the confidentiality of information and also secure it from unauthorized users, denial of services, modification, etc. Securing the storage and computation process in cloud is essential to avoid the above threats. Security protocol in cloud is enhanced through cryptographic algorithms to eliminate the various security threats in our work.

Keywords: *Cloud Computing; Security Issues; Cryptography System; Security Solution.*

1. Introduction

Outsourcing is considered to be the most sought after technology by many organizations due to its flexibility and computing resources [13]. In cloud computing resources are used as service over the internet without actually possessing the resource or maintaining it [15], [12].

There are several structures being provided as service namely: Platform as a Service (PaaS), infrastructure as a service (IaaS) and Software as Service (SaaS).IaaS means the customer use the service providers computing, storage, network or infrastructure over the internet, PaaS means the customer use the provider's resources for running custom applications and SaaS means the application is provided by the provider and the customer uses it. [5], [6], [7].

According to the researchers in [14], [6] it's crucial to handle security concerns involved in the process of cloud computing along with the legal concern. The major security issues in cloud computing are backup, network traffic, data security, security of host and file system [10].

Cryptography is the technique of converting readable messages into non readable message. This process contains three algorithms namely Asymmetric-key algorithm, symmetric- key algorithm and Hashing [11]. Crypto Cloud computing came into existence due to the very presence of cloud computing.

The main aspect that bought this technique to existence is to secure data in cyber resource. It helps in protecting privacy and data security.

Crypto cloud service ensures information integrity along with security in the entire process of data sharing.

As discussed earlier there is no privacy over cloud network [9], [16] the current proposed approach ensures security of data sharing and privacy over cloud network. This can cause many scopes for information sharing over cloud [5].

2. Security problems in cloud computing

Though there is several security concerns involved in cloud, these issues can be grouped under two main subjects: Security issues involved in client end and service provider. In brief the service provider needs to control and take care of the infrastructure safety and also to ensure that client's data are safe and secured. The client must ensure that the service provider has taken complete care on customer's data and information. Hence security of data is an important concern for both client device and the service provider in the cloud network [1, 2 and 3].

a) Data Protection

Cloud providers must have proper systems to ensure there is no data leakage and third party access. Assigning appropriate duties for timely checks and auditions is necessary. Every identity involved in the network will have an identity in unique manner management system performs control operation and access operation on information and resources in cloud network.

b) Data Locality

It means the cloud providers must be able to manage the position of data to adhere customer preferences and rules. Data locality differs from countries and organizations and at times has their autonomous set of rules and regulations to be followed in order to guarantee information privacy and data locality.

c) Data Integrity

It means that the data must be reliable throughout its life cycle. Data integrity which provides assurance of that data is updated across all cloud data centers in case of any replication of data. Any changes to data have to be updated thoroughly in all places of

Copyright © 2018 R. Rajan 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.

replication for maintaining consistency, validity and regularity of data.

d) Data Segregation

It involves segregating the data in cloud storage since there are chances of intrusion in case of several users' data in the same location. Intrusion can happen either by client code injection or by hacking the application.

e) Data Access

Data accessibility is another interesting topic in cloud. Each client has his/her own data access rules and regulations. These rules have to be implemented on that particular users own data. Cloud provides the facility to handle this task through cloud access control model.

An efficient access control mechanism is required to secure customer data from unwanted users and must state the parts of data that is accessible for a particular user.

f) Data Confidentiality

Confidentiality refers to rules that provides access and restricts access to certain types to data. In terms of customer and service provider, confidentiality means that data and the computation process must be saved confidentially. It must be ensured that private data must never be available to any unauthorized user or for that case it must not be accessible to CPU, application, platform and physical memory.

In certain scenarios the confidential data is shared with the service providers depending on the below mentioned situations. The first scenario is when the service provider knows about the location where user's confidential information is stored in the system. Second scenario is when the service provider will have the right authority for the users to access private information and also gather it in the cloud system. The final situation is when service provider understands the meaning of user's private information in cloud system.

g) Data Availability

It so happens that at times the information stored in cloud server may not be available to the client under certain situations. In case of cloud system storing of data is in remote locations that belong to others. When cloud stops responding in certain scenarios then data may not be accessible since data depends on single service provider. Some other scenarios are like flood that results in deny of service and causes Direct/Indirect (DOS) attack. In such cases when there is no service the quality of the service is not up to the standard of Service Level Agreement (SLA) then customer can lose trust in the system.

h) Data Breaches

Data breaches are an imperative aspect of threat that needs attention and caution in cloud system. Since client's data are stored in cloud it is open to any type of breach and hence creates a fear in consumers mind. It is risky from both insider and outsider attackers who can advance access to customer's confidential information.

3. Cryptography

a) Plain Text

A novel content which the sender sends it to the receiver. This original text is considered as input to algorithm.

b) Cipher text

It is the unknown form of the novel text. Cipher text is the output that comes from the encryption algorithm and it is also the input for the decryption process. Two different cipher texts will be produced if pair of keys sis utilized.

c) Encryption Algorithm

It implements various techniques to convert the plain text into the cipher text.

d) Decryption Algorithm

This does the exact opposite of the encryption algorithm. It converts cipher texts into plain texts using secret key.

e) Secret Key

Secret key is given as input to encryption process. The key value is independent of algorithm and plaintext. Its output depends on this key being used. The operation is performed in the algorithm which is completely dependent on this key. From the above points it is noticeable that all the standard security processes that include integrity of data, privacy, confidentiality, robustness and access control is necessary. Hence it becomes complicated to handle the security process in cloud technology. There are various cryptographic methods that is being proposed in many researcher papers. Based on the key that is being used in the algorithm cryptography is categorized as follows:

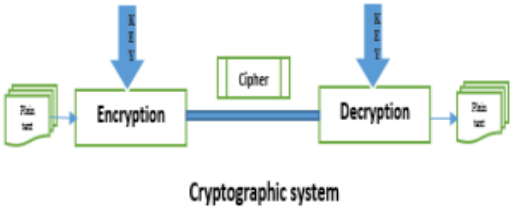

Fig. 1: Shows Cryptographic System.

Symmetric key Cryptography

In this type, the encryption and the decryption process uses the key of same type. It's a common key which is shared to the sender device and the receiver device.

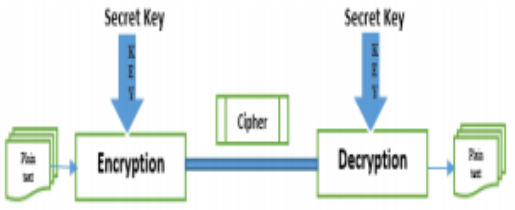

Fig. 2: Shows Symmetric Key Cryptography.

Asymmetric key Cryptography

In asymmetric type, a private key parameter and public key parameter is used for decryption and encryption of the data. During encryption, private key is used and during decryption public key is used.

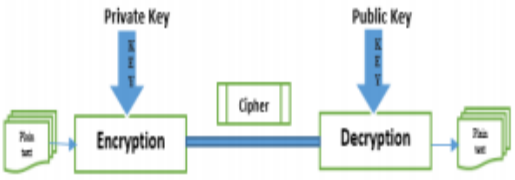

Fig. 3: Shows Asymmetric Key Cryptography.

4. Need of cryptography

a) Confidentiality

The concept behind confidentiality is to allow content access only to the receiver and sender. Illegal access can happen if there is fault in confidentiality.

b) Authentication

Authentication is to verify the authenticity of a user. This process guarantees you that the sender is sending the message to the verified receiver.

c) .Integrity

This process makes sure the message sent by sender is not altered during the process and the exact data is received by the receiver. If integrity of data is lost then it means an unauthorized modification is done to the original message.

d) Non-repudiation

This process provides the security against denial of one party that is required in a communication.

e) Access Control

Access control helps in preventing illegal or unauthorized use of data or resources.

f) Availability

This takes care of the system availability with good status and the service is provided to only authorize users.

5. Cryptography algorithms

a) Data Encryption Standard (DES)

This method encrypts data with 56-bit symmetric key that is randomly generated.DES (Data Encryption Standard) was developed by the US Government along with IBM as a block encryption algorithm. This method was not so secure and cracked several times.

b) Data Encryption Standard XORed (DESX)

DESX is the successor of DES. The algorithm was highly enhanced to make it less crack able by hackers. The plaintext is a bitwise XORed that has 64 bitskey with additional parameter prior to it is encrypted with DES. It also yields bitwise XORed operation with another 64-bit key.

c) Triple DES (3DES)

The Triple DES is an advanced approach of DES that uses 8 parity bits and 56 effective key bits that includes 64-bit key. In this approach DES is applied on the plaintext three times. Now plaintext is performed encryption operation with key A, decryption operation is performed with key B and encrypted again using key C.3DES is called as a encryption algorithm performed on blocks.

d) RC2 and RC5

These are block oriented encryption algorithms which was originally invented by Ronald Rivest (RSA Labs) using key sizes and variable block. If the original size is unknown by the attacker for decryption then it becomes complicated to break this algorithm.

e) RC4

This algorithm is built on a random permutation with the variable key size stream cipher along with the byte- oriented operations.

f) Advanced Encryption Standard (AES)

It uses the Rijindael algorithm. It is the encryption method with strongest manner developed by Vincent Rijmen and Joan Daemen AES is capable of replacing 3DES and DESX. AES can use keys of 256-bit, 192-bit and 128-bit.

g) International Data Encryption Algorithm (IDEA)

It's a block cipher algorithm proposed by Professor J.Massey and Dr. X.Lai. It utilizes 128-bit key on a 64-bit plaintext. It is made up of 8 rounds in which XOR performs addition and multiplication for each rounds. It comprises of four sub-blocks and key material contains six 16-bit sub-blocks.

h) Blowfish

It was from Bruce Schneier and is a block cipher for symmetric operation utilizing 64 bits blocks size and variable key length of 32 to 448 bits.

i) CAST

CAST was originally designed by Carlisle Adams and Stafford Tavares. It uses 40-bit to 128-bit key.It is used in products like IBM and Microsoft and it is fast and efficient.

6. Overview on various cryptographic systems

a) RSA (Rivest-Shamir-Adleman Algorithm)

In terms of public key cryptosystem the RSA- Rivest-Shamir Adleman algorithm is very ideal. It is the most commonly used scheme in public key cryptography for modern computers and technology. It is asymmetric and uses integers in the range of 1,024 bits in size. The main utilization of RSA can be to encrypt and decrypt. It uses two different keys and hence termed as asymmetric.

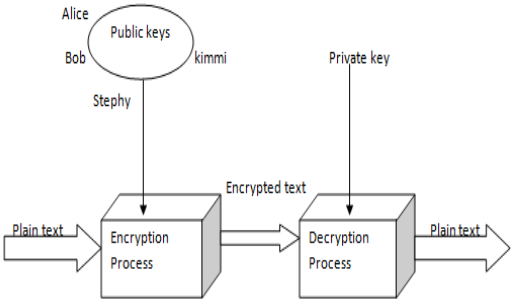

Fig. 4: RSA Algorithm (Asymmetric Key Cryptography).

In this algorithm one key can be shared to all and another is kept private. RSA exists since 1978 by Ron Rivest, Adi Shamir and Leonard Adleman.

It gives a return product as two prime numbers (P*Q) and (I) as the public key. The value (P*Q) is kept as the secret key. It is possible that they (with public key) can encrypt the data but only if the prime factor of that large number can be found the user will be able to decode the message.

RSA is used for public key encryption and digital signatures as well. The complexity of the algorithm depends on the complexity in factoring large integers. Following algorithm is used in RSA.

The below algorithm is used in RSA,

1) Choose p and q
2) Calculate n = p * q
3) Find φ (n) = (p - 1) * (q - 1)
4) Select e such that 1 < e < φ (n) and e and n are co-prime.
5) Compute a value for d such that (d * e) % φ (n) = 1.
6) Public key is (e, n)
7) Private Key is (d, n)
8) For encryption C=me (mod n) and decryption m =cd (mod n)

Using the above algorithm a plain text can be encrypted and then the cipher text can be decrypted into plain text. The amount of time consumed in encrypting data is the major drawbacks. RSA also uses the concept of asymmetric where the keys used are different. This again is time consuming. The level of security delivered in RSA is high but the only disadvantage is the time involved in the process of cryptography. Another possible loop hole in this algorithm is the usage of fake keys to decrypt data. So it is highly important to keep the secret key confidential and prevent hackers from using the same.

a) AES (Advanced Encryption Standard)

AES is advanced edition of DES. It was the aspiration of National Institute of Standards and Technology (NIST) to have a modified version of DES. Among the several proposals, Advanced Encryption Standard was chosen and replaced DES and 3DES. AES was originally developed by Joan Daeman and Vincent

Rijmen in 2001. AES uses symmetric block cipher structure with three block ciphers and with several rounds of encryption. AES uses AES-128, AES-256 and AES 192 block ciphers. All the block ciphers encrypt function and decrypt function for data in blocks of 128 bits through cryptographic keys incorporated as 128 bits, 192 bits and 256 bits. AES contains 10 rounds of encryption for 128 bit keys with 12 rounds can be used for 192 bit keys and finally 14 rounds can be used for 256 bit keys.

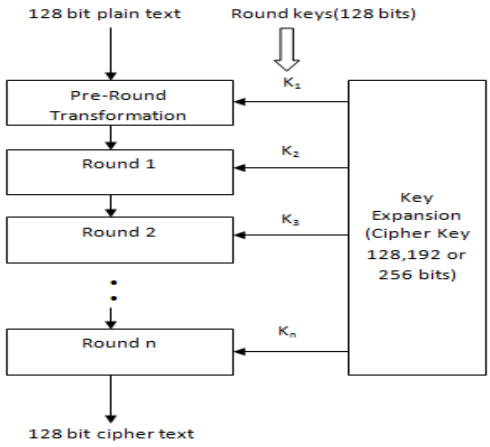

Fig. 5: AES.

The similar process is followed in all the rounds and the encryption process can be further listed as follows:
1) Substitute byte, 2) Shift rows, 3) Mix column and 4) Add round key.
Substitution round:
Here the sub-bytes are substituted byte-by-byte in forward encryption process.
Shift Rows: The rows in state array are shifted in this step during forward process (S-Box process)
Mix Column: The bytes in all columns are mixed up in the forward process.
Add Round key: It is added to the output that is received from the earlier step depending on the key size.
AES encryption process contains different round keys and is applied on data array using mathematical operations. After which the data is represented in an array form called the state array.
The encryption process is detailed below:

1) Basically Round keys are completely derived from cipher key.
2) State array is formed using block data or plain text.
3) Round key is added with initial state array with other keys.
4) The manipulations are continued till 9th round.
5) After the 10th round we derive to the final output with a cipher text. Through above process we derive the final cipher text or encrypted text as the output.

b) Blowfish

Bruce Schneier introduced Blowfish algorithm in the year 1993. It uses variable length key of 32 bits up to 448 bits. The block size is fixed to 64 bits. The S-box constitutes 32 bits of data.

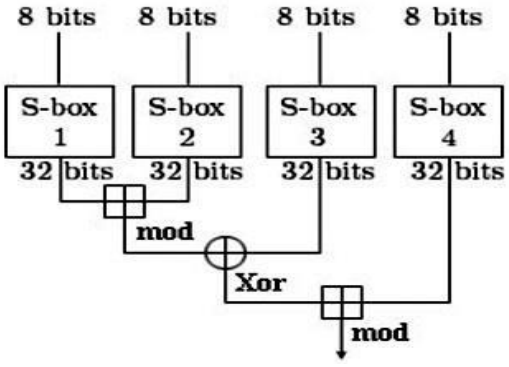

Fig. 6: BlowFish.

The above figure demonstrates Blowfish's F-function. Input data of 32 bit segmented into four 8-bit quarters and then used as input to the S-boxes. The outputs (Mod) modulo232 and the XORed are added in order to derive the 32-bit output (final) which is the encrypted data. The same procedure in reverse order is conduct decryption process.

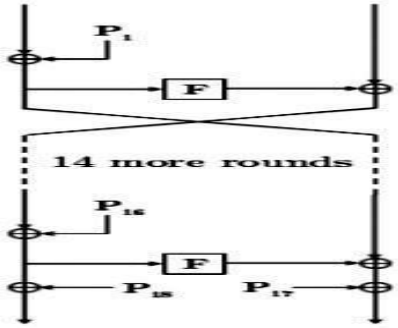

Fig. 7: BlowFish Structure.

There are no attacks and loop holes found in Blowfish algorithm. There are two parts in this algorithm namely data encryption and key expansion. Data encryption holds 16 rounds of feistel network. The rounds in the algorithm have key dependent permutation in P-Box and key/data dependent substitution in S-Box.
Blowfish algorithm comprises of P-Box and S-Box. Let's consider the P-array first. It comprises 18 keys of 32 bit and named as P1, P2, P3... P18. 4 S-boxes with 32 bit and 256 entries each.S1[0], S1[20],..., S1[255]; S2[0], S2[20],..., S2[255]; S3[0], S3[20],..., S3[255]; S4[0], S4[20],..., S4[255].
Encryption is done using the below steps.
Divide x into two 32-bit halves:

(xL) and (xR)
For i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
Next i
Swap xL and xR (or Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR.
Divide xL into four eight-bit quarters: a, b, c, and d
F (xL) = ((S1, a + S2, b mod 232) XOR S3, c) + S4, d mod 232

Decryption is similar to encryption but with a reverse process. Encryption rate is enhanced and is much faster than the IDEA and the DES. In several simulations it is proven that the Blowfish algorithm yields better results compared to others.

c) Two fish

Two fish follows the feistel structure with symmetric block cipher. Bruce Schneier was the founder of this algorithm in 1998. Two fish is proven to be competent in softwares that run on smaller processors like the smart cards embedded in hardware.
The implementers have the leverage to customize the encryption speed, code size and key setup time in order to optimize the performance.
This algorithm is un-patented, free of cost and license free. It utilizes key sizes of 256, 192 and 128 bits. The 128 bit block size is used with 16 rounds of encryption.

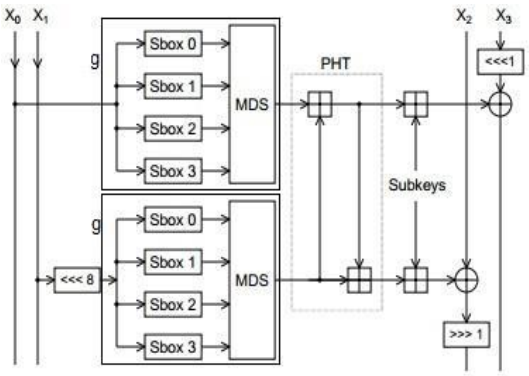

Fig. 8: TwoFish.

Fig.8 clearly shows a round function that is involved in two fish algorithm.

The round function occurs 16 times and derives to a final result of cipher text after the 16th round. The process visualized in the figure is explained as follows:

1) X0 and X1 is the input for function g after the rotation is done by 8 bits.
2) 2. The function g comprises of 4 bytes key-dependent S-boxes that is followed by linear mixing step (MDS matrix).
3) With PHT (Pseudo-Hadamard Transform), the results of two g functions is combined.
4) There are two keywords supplemented and then one keyword is rotated by 1 bit and it is XORed to the result on its left.
5) In the subsequent round of the process the right and the left halves are swapped.
6) Reversal is done for the last swap after the 16th round. And the four keywords are XORed with other set of four keywords to get the end encrypted text or the cipher text.

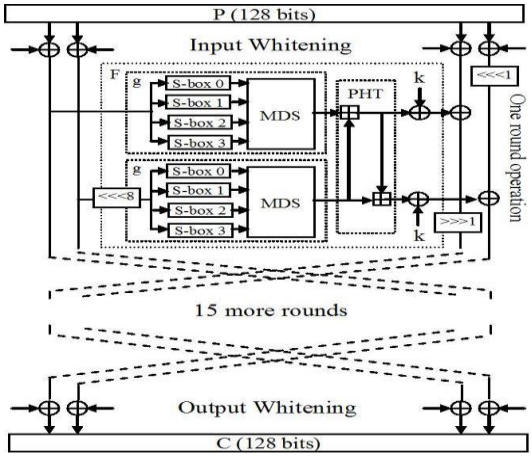

Fig. 9: TwoFish Structure.

The above diagram depicts the Twofish algorithm. It contains 16 rounds of data encryption and derives a 128 bit cipher text as the final output. Two fish algorithm results in good security level but its encryption speed is slowwhen compared to Blowfish algorithm.

d) IDEA (International Data Encryption Algorithm)

James L and Xuejia Lai designed an International Data Encryption Algorithm (IDEA) in 1991 as a block encryption algorithm. There were several modification conducted on the original algorithm to derive the final IDAE algorithm. IDEA works on a 64 bit plain text or cipher text blocks with the key size 128 bit. They are then transformed into four 16 bits sub-blocks. These four blocks are represented as P1 (16 bits), P2 (16 bits), P3 (16 bits), and P4 (16 bits).

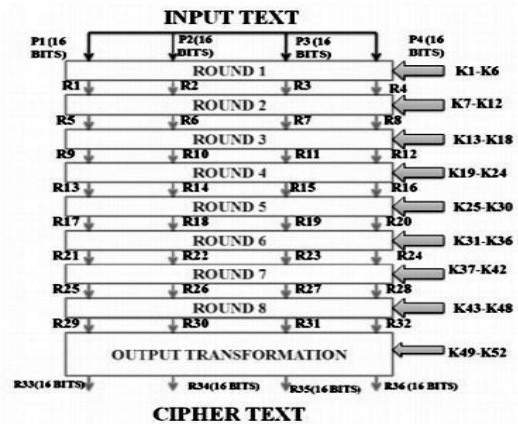

Fig. 10: International Data Encryption Algorithm.

All the blocks undergo 8 rounds with one output of the transformation phase. Each round is dealt with some arithmetic and logical calculations. The operation is in the range of eight rounds and similar sequence of steps performed.

The output transformation phase in the output is performed with arithmetic operations during the culmination of the 8th round. As encryption process commences 64 bit plain text is fragmented into four blocks and is the input for round 1.

The result of round 1 is considered as input for round2 and in similar way output of round 2 is input for round3 and it continues. The round 8 generates final output that is the input for the output transformation whose end product is 64 bit cipher text (considered as C1 (16 bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)). Encryption and decryption uses one key since it follows concept of symmetric key algorithm.

Table 1: Shows Comparisons of Various Cryptographic Systems

Algorithm	Created By	Year	Key Size	Block	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64 bits	16	Festial	No	It is not Strong Enough
3DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Sufficient Security
AES	Joan Daemen & incent Rijmen	1998	128, 192, 256 bits	128 bits	10,12, 14	Substitution Permutation	Yes	It is a replacement for DES with Excellent Security
Blowfish	Bruce Schneier	1993	32-448	64 bits	16	Festial	Yes	It provides excellent Security
RC4	Ron Rivest	1987	Variable	40-2048	256	Festial Stream	Yes	It is a fast Cipher in SSL
RC2	Ron Rivest	1987	8-128 64 by default	64 bits	16	Festial	-	It is a stream Cipher
Twofish	Bruce Schneier	1993	128- 256	128 bits	16	Festial	Yes	It gives good Security
Serpent	Anderson,, Lars Knudsen	1998	128- 256	128 bits	32	Substitution permutation	Yes	It gives good Security
IDEA	James Massey	1991	128 bits	64 bits	8.5	Substitution Permutation	No	It is not Strong Enough
RC6	Ron Rivest, Matt Robshaw	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	It gives good Security
RSA	Rivest,, Shamir, Adleman	1977	1,024 to 4,096	128 bits	1	Public Key algorithm	No	Excellent Security with low speed
Diffie Hellman	Whitfield Diffie , Hellman	1976	1024 to 4096 bits	512	-	Asymmetric algorithm	Yes	Many attacks

The only difference is the encryption algorithm and decryption algorithm process is the sub keys that are comprehensively derived through different algorithms [4]. The size of the symmetric key is 128 bits. Total of 52 keys is involved in the process of encryption transformation phase).). In every round 6 sub keys are used and these 52 keys are derived from 128 bit cipher key. The output transformation process uses 4 sub keys which includes 8 rounds with output transformation phase). In every round 6 sub keys are used and these 52 keys are derived from 128 bit cipher key. The output transformation process uses 4 sub keys.

7. Conclusion

Dissemination of information through internet has become a common feature among individuals, organizations and government. The biggest challenge is to secure this information shared over internet from external users and hackers. For protecting the information we use the concept of decryption and encryption using cryptographic algorithms. The existing cryptographic method is analyzed in the paper and also surveyed with the existing works for the encryption techniques. It is analyzed in detail so as to promote the security system in these techniques. In general all these techniques are applicable in real time scenarios and are useful in its own ways and are applicable for different applications. With unprecedented demand for security in cloud system, new and powerful techniques are also evolving according to the variations in the requirement.

References

[1] J. Feng, Y. Chen, D. Summerville,Z. Su and W. Ku"Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol" on 2011 in Consumer Communications and Networking Conference (CCNC).

[2] Lori M. Kaufman, "Data security in the world of cloud_ computing", July. Aug. 2009. IEEE Security and Privacy Journal, Vol. 7.

[3] Giuseppe Ateniese, Kevin Fu, Susan Hohenberger and Matthew Greenon February 2005 "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage", In Proceedings of the 12th Annual Network and Distributed System Security Symposium

[4] Sunia Rani, Ambrish Gangal "Cloud Security with Encryption using Hybrid Algorithm" International Journal of Computer Science and Information Technologies, vol. 3(3), ISSN: 0975-9646, 2012.

[5] G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, [online] http://www.theregister.co.uk/.

[6] Hassan Takabi , James B.D. Joshi, Gail Joon Ahn, "Cloud Computing Security and Privacy Challenges in Cloud Computing Environments ", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES,1540-7993/10/$26.00 © 2010 IEEE.

[7] Australian government department of defense, "Cloud Computing Security Considerations", CYBER SECURITY OPERATIONS CENTRE APRIL 2011, UPDATED SEPTEMBER 2012.

[8] Akansha Deshmukh, Harneet Kaur Janda, Sayalee Bhusari, "Security on Cloud Using Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015 ISSN: 2277 128X Available online at: www.ijarcsse.com

[9] James Mark Kelly,Columbus state University CPSC 6128 Spring 2010- Cloud computing and cryptography

[10] Neha Jain and Gurpreet Kaur ,,Implementing DES lgorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.

[11] Rashmi Nigoti1, Manoj Jhuria2 Dr.Shailendra Singh3, " A Survey of Cryptographic Algorithms for Cloud Computing ", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) Available online at: www.iasir.net.

[12] G. Murugaboopathi, C.Chandravathy, P. Vinoth Kumar, " Study on Cloud Computing and Security Approaches", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[13] Seny Kamara, Kristin Lauter, "Cryptographic Cloud Storage", Financial Cryptography and Data Security Volume 6054, 2010, pp 136-149. https://doi.org/10.1007/978-3-642-14992-4_13.

[14] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Jesus MolinaRyusuke Masuoka"Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control", In Proceedings of the 2009 ACM workshop on Cloud computing security, CCSW ˝09, pages 85–90.

[15] SADIKIN RIFKI, YOUNGHO PARK, SANGJAE MOON, "A Fully Secure Cipher text-Policy Attribute-Based Encryption with A Tree-Based Access Structure".

[16] Niranjanamurthy M , Charan Raj U , Raghavendra E , Sowmya R , Suhas Jadhav J, "Comparative Study on Cloud Computing (CC) and Mobile Cloud Computing (MCC)", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.10, October- 2014, pg. 280-290.