iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6123

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

A Survey on Data Security in Cloud Computing using Hybrid Encryption Algorithms

Jayana C. Kaneriya[1], Jalpa J. Khamar[2], Avani J. Dadhania[3]
[1, 2, 3]*Computer Engineering Department, KSV University*

Abstract: ***Cloud computing enables to share various resources from anywhere and anyone can access those resources. Resources can be information, storage, applications, platforms, infrastructures and many more. Cloud computing features like elasticity, Migration flexibility, Dynamic Provisioning, Workload resilience, Pay per use attracts many companies to expand business with minimal cost. Main challenge to cloud computing is security of data against unauthorized access. Encryption is a method to secure data from unauthorized access. To provide security of data various encryption algorithms are used. For all cloud computing applications performance and cost of implementation are also major challenges. So encryption algorithms are useful if it is secure and fast in performance. In this paper, we have discussed about security challenges of cloud computing and presented study of various encryption algorithms (AES, DES, RSA, Blowfish, Twofish, Hybrid algorithms).***
Keywords: Cloud computing, data security, encryption algorithm, AES, DES, RSA, Blowfish, Twofish, Hybrid algorithms

I. INTRODUCTION

Cloud Computing is the delivery of computing resources over the internet everything ranging from applications to data centers. It provides the on-demand services on a pay as you use basis. It provides high reliability & scalability. The resource of the cloud system provide transparent for the application and the user don't know where the resource come from. The user can access the data from anywhere through the application. The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service oriented architecture. The advantage of cloud computing over traditional computing include: agility, lower entry cost, device independency, location independency, and scalability [1].

Encryption is the way of converting a plaintext message into cipher text which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption. There are various types of data encryptions which form the basis of network security. Encryption schemes are dependent on block or stream ciphers. The length and type of the keys utilized depend on the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used .The data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by third party users. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are not same. The public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message [1].

II. SECURITY CHALLENGES

Security is taken into account collectively of the foremost important aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Challenges related to cloud computing are data security and privacy, lack of standards, ceaselessly evolving, trust, expectations and performance [2].

In cloud computing customers are not aware the place where data is stored. So data storage in internal organization and in cloud is different. With cloud physical security is lost so, in cloud security of data is a challenge. For this security mechanisms between organizations and cloud needs to be implemented. In cloud computing rate of change is too fast. So standards also need to be updated. For a fast evolving technology it is difficult to maintain and to update cloud standards. Cloud has documented interfaces but no standards are associated with this. Current IT market and user requirements are continuously evolving. Means cloud interfaces, networking and storage interfaces are also evolving.

There square measure numerous policies problems and threats in cloud computing that embody privacy, security, reliability and a lot of. In this paper various hybrid encryption algorithms are discussed to solve security issue in cloud computing [3].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

III. HYBRID ALGORITHMS

A. Enhanced Security Using Aes, Blowfish And Twofish Algorithm

This method uses AES, Twofish and Blowfish encryption algorithms. The Advanced Encryption Standard, or AES, Blowfish and Twofish are symmetric block cipher. Following section describes all three algorithms and also hybrid encryption algorithm.

AES is a symmetric key block cipher. It performs a series of operations. It uses 128 bits of data with 128/192/256 bits of keys. AES performs all its computations on bytes rather than bits. Number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. AES encryption process has four sub-processes. First sub process is called byte substitution. In this process data bytes are replaced by S-box table bytes. The result is in a matrix of four rows and four columns. Second sub process is called as shift rows. In this process first row is not shifted. Second row is shifted one position to the left. Third row is shifted two positions to the left and fourth row is shifted three positions to the left. Next process is called as mixcolumns. Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round. Next process is called as addroundkey. The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.AES decryption process is similar to encryption process in the reverse order. Each round consists of the all four processes conducted in the reverse order. [4].

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follow the feistel network and this algorithm is divided into two parts key-expansion and data Encryption. In key expansion, it will convert a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses large number of subkeys. The subkeys are calculated using following steps:

1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
2) XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3) Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4) Replace P1 and P2 with the output of step (3).
5) Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6) Replace P3 and P4 with the output of step (5).
7) Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.In total, 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.

To encrypt data, it is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round [5].

```
Divide x into two 32-bit halves: xL, xR
        For i = 1to 16:
            xL = XL XOR Pi
            xR = F(XL) XOR xR
            Swap XL and xR
            Swap XL and xR (Undo the last swap.)
            xR = xR XOR P17
        xL = xL XOR P18
        Recombine xL and xR
```

Twofish is a block cipher by Counterpane Labs, published in 1998. It was one of the five Advanced Encryption Standard (AES) finalists, and was not selected as AES. Twofish has a 128-bit block size, a key size ranging from 128 to 256 bits. This algorithm uses 16 round feistel network. IT also uses bijective function made up of four key dependent 8 by 8 bit s-boxes. Data is split into four 32 bit words. Then words are xored with four key words. In all 16 rounds first two words on the left are used as input to g functions. The g function consists of four byte wide key dependent s-boxes, followed by a linear mixing step based on MDS matrix. Each s-box takes 8 bits of input and produces 8 bit of output. The four results are interpreted as a vector of length 4 and multiplied by 4 by 4 MDS matrix. The results of the two g functions are combined using a PHT and two keywords are added. These two results are then xored into the words on the right. The left and right halves are then swapped for next round. After all the round, the swap of the last round is reversed and the four words are xored with four more key words to produce the cipher text [6].

In this method of hybrid encryption, cipher text is generated using AES, Blowfish and Twofish. All algorithms are used to provide security to data. This method follows following steps:

Storing procedure to cloud:

8) Register and login with correct information
9) Select data to upload
10) Apply ECDH for key generation
11) Apply AES with Twofish or AES with Blowfish on data that will generate encrypted data. Getting data from cloud
12) login with correct login information
13) Client selects desired data to download
14) Enter correct key to download data
15) Apply AES with Blowfish or AES with Twofish to decrypt data. The hybrid of AES and Twofish or Blowfish provides more security to data [7].

B. Enhanced Security Using Aes, Rsa And Sha-1 Algorithm

This method uses AES, RSA and SHA-1 algorithms. The Advanced Encryption Standard is a symmetric block cipher. RSA is a symmetric key algorithm and SHA-1 is a hash function used for digital signature. Following section describes RSA and SHA-1 algorithms and also hybrid encryption algorithm.

In RSA, Generate two large random prime numbers called p and q. compute n=p*q and $\Phi = (p-1)(q-1)$. Choose an integer, $1<e<\Phi$, such that $\gcd(e,\Phi) = 1$. Compute d, $1<d<\Phi$, such that $ed \cong 1 \pmod{\Phi}$. The public key is (n,e) and private key is (d,p,q). Encryption is done using receiver's public key(n,e). Data is represented as positive integer m, $1<m<n$. compute cipher text $c=m^e \bmod n$. To decrypt cither text receiver uses his private key (n,d) and computes $m=c^d \bmod m$ [5].

In SHA-1, Message is padded with a 1 and as many 0's as necessary to bring the message length to 64 bits less than an even multiple of 512. 64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.SHA1 requires 80 processing functions. SHA1 requires 80 processing constant. SHA1 requires 160 bits or 5 buffers of words (32 bits). Processing Message in 512-bit blocks .This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks [8].

1) Storing Procedure to Cloud

a) Information is converted to encrypted data using AES algorithm.
b) RSA algorithm produces key by RAS public key and AES key. RSA is used to increase key length.
c) AES encrypted message is delivered to generate signature.
d) Secure hash is produced by SHA-1 algorithm.
e) Using secure hash and RSA private key signature is generated.

2) Getting Data From Cloud

a) Using RSA private key and key AES decryption key is recovered.
b) Encrypted Data is decrypted using key and AES algorithm.
c) Secure hash is generated using encrypted message.
d) Digital signature is verified using secure hash and RSA public key [9].

C. Enhanced security using AES and PGP Algorithms

In this method of encryption, cipher text is generated using AES and PGP algorithms. The Advanced Encryption Standard, or AES, is a symmetric block cipher. PGP encryption uses a serial combination of hashing, data compression, symmetric key cryptography,

and finally public-key cryptography; Both algorithms are used to provide security to data. AES is used to provide data security and PGP is used to provide network security and authentication. Following section describes PGP algorithm and also hybrid encryption algorithm. PGP stands for Pretty Good Privacy. It uses asymmetric key encryption method. Encryption is done using public key and decryption is done using private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

1) Steps for Encryption

a) AES generates cipher text to plain text.
b) Sender generates a session key that is one time secret key for this message only.
c) This session key works with very secure, fast encryption algorithm like 3DES, IDEA, CAST-128.
d) Then session is encrypted with receiver's public key using RSA algorithm.
e) This double encrypted message is stored to cloud.

2) Steps for Decryption

a) Client downloads desired data.
b) Using Private Key, RSA decrypts session key.
c) Using session key and encryption algorithm receiver decrypts data
d) Using AES key again data is decrypted to get original data.

AES requires less memory than Blowfish algorithm. AES has a very high security level because of 128,192 or 256 bit keys. It shows resistance against a variety of attacks. AES algorithm has high performance without any weakness and limitations compared to other algorithms. PGP provides one more level of security to data [10].

D. Enhanced Security Using Blowfish And Md 5 Algorithms

This method uses Blowfish and MD5 algorithms. Blowfish is a symmetric block cipher. And MD5 is hash function used for digital signature. Following section describes MD5 algorithm and also hybrid encryption algorithm.

MD5 algorithm can be used as a digital signature mechanism. This algorithm takes as input a message of arbitrary length and produces as output a 128 bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest. Suppose a b-bit message as input, and that we need to find its message digest. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}. A four-word buffer (A,B,C,D) is used to compute the message digest. – Here each of A, B, C, D, is a 32 bit register. These are initialized to certain fixed constants. Four auxiliary functions that take as input three 32-bit words and produce as output one 32-bit word. The message digest produced as output is A, B, C, D. That is, output begins with the low-order byte of A, and end with the high-order byte of D [11].

In method of encryption uses Blowfish algorithm and MD5 algorithm. Blowfish algorithm is used to encrypt the data and MD5 is used to authenticate encrypted data. This method follows following steps:

1) Storing procedure to cloud:

a) Preprocessing of data for encryption.
b) Using key data is encrypted
c) Encrypted data is send to cloud
d) Cloud adds message digest to encrypted data

2) Getting data from cloud

a) Client downloads desired data
b) Using message digest check for originality of data and remove message digest from encrypted data
c) Using Blowfish key decrypt data.

Results prove that it is faster and occupies less memory than ECDH- AES algorithm [12].

IV. COMPARISION

Algorithms used	Advantages
Enhanced security using AES, Blowfish and Twofish Algorithm	With compared to Blowfish, Twofish gives better performance. And Twofish is also faster and requires less memory so suitable for smart cards. Twofish has no weak keys but Blowfish has weak keys. In hybrid encryption, AES and Twofish take less time to encrypt and decrypt files as compared to AES and Blowfish.
Enhanced security using AES, RSA and SHA-1 Algorithm	This method guarantees data protection and data integrity. The strong solution by integrating hybrid encryption and digital signature. AES algorithm has a very high security level.SHA-1 has the least computational cost among the similar algorithms. RSA digital signature scheme also guarantees the authenticity and integrity of data.
Enhanced security using AES and PGP Algorithm	AES is a good method for secure sensitive data stored in large database. PGP is a combination of symmetric key and asymmetric key encryption. The combination of these two encryption methods combines the convenience of public-key encryption with the speed of conventional encryption. In this hybrid solution, PGP adds one more level of security. This adds additional security to data at cloud side and network channel.
Enhanced security using Blowfish and MD 5 algorithms	This method is compared with and ECDH-AES (Elliptical Curve Diffie Hellman-Advanced Encryption Standard) encryption algorithm. In file size comparison, this method requires less memory to store encrypted file and encryption/decryption time is also less.

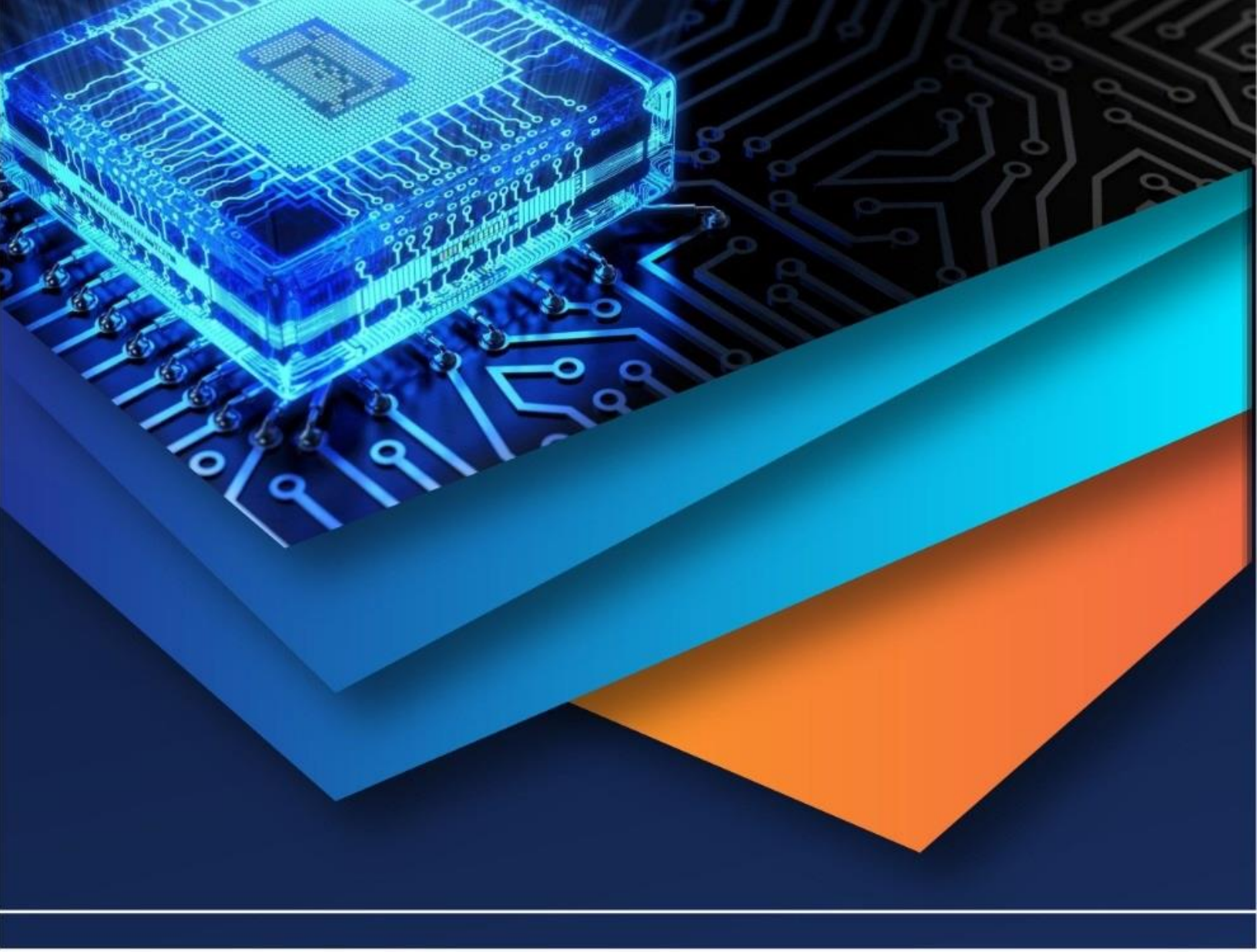
V. CONCLUSION

Security is a big challenge in cloud computing. There are number of existing techniques used to implement Security. In this paper various hybrid encryption decryption techniques are surveyed. First hybrid algorithm shows comparison on the basis of encryption/decryption time and hybrid of AES and Twofish takes less time to encrypt and decrypt the file as compared to AES and Blowfish. In second hybrid algorithm SHA-1 has the least computational cost among the similar algorithms. RSA digital signature scheme also guarantees the authenticity and integrity of data. In third hybrid algorithm, Combination of AES and PGP provides more security to the data at rest (cloud server) and in data in motion (network channel). So it provides more security to the confidential data. Fourth hybrid algorithm is compared with ECDH-AES. Results prove that this algorithm occupies less memory to store encrypted file and encryption/decryption time is also less.

REFERENCES

[1] Deyan Chen, Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing, IEEE International Conference on Computer Science and Electronics Engineering, 2012
[2] IR.Mathivanan, IIA.Christy Jeba Malar, Cloud Computing Security Provision Using Twofish Algorithm, International Journal of Advanced Research in Education & Technology (IJARET) Vol. 4, Issue 2 (April - June 2017)
[3] Rachna Arora, Anshu Parashar, Secure User Data in Cloud Computing Using Encryption Algorithms, International Journal of Engineering Research and Applications 2013
[4] Mitali, Vijay Kumar and Arvind Sharma , A Survey on Various Cryptography Techniques, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3, Issue 4, 2014.
[5] R.Gowthami Saranya, A.Kousalya, A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing International Journal of Computer Science and Information Technologies Vol. 8 (2) , 2017, 306-310
[6] John Kelsey Doug Whiting David Wagner Chris Hall Niels Ferguson k, Twofish: A 128-Bit Block Cipher Bruce Schneier, 15 June 1998
[7] Neha, Mandeep Kaur, Enhanced Security using Hybrid Encryption Algorithm International Journal of Innovative Research in Computer and Communication Engineering, 201
[8] Chaitya B. Shah, Darshti R. Panchal., Secured Hash algorithm-1 : review paper, International Journal for advance research in Engineering and Technology, volume 2, Issue X, Oct 2014 ISSN 2320-6802

[9] Aysan Shiliralizadeh, Abdulreza Hatamlou, Mohammad Masdari , Presenting a new data security solution in cloud computing Journal of Scientific Research and Development 2015
[10] K. Arul Jothy, K.Sivakumar, M UJ DelseyEfficient cloud computing with secure data storage using AES and PGP algorithm International Journal of computer science and information technologies vol 8(6) 201
[11] ZhaoYong-Xia and Zhen Ge ,"MD5 Research," Second International Conference on Multimedia and Information Technology, 201
[12] Data Security in Cloud Computing Based On Blowfish with Md5 Method Pooja Devi Amit Verma International Journal of Advance Research, Ideas and Innovations in Technology. 2017



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY