iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

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

Volume 5 Issue, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Achieving High Secure Data Storage in Cloud Computing

S. Meena[1], Dr. N. Kowsalya[2]
[1]M. Phil Full Time Research Scholar, PG and Research Department of Computer Science
[2]Asst. Professor, PG& Research Department of Computer Science & Applications, Vivekanandha College of Arts & Sciences for Women (Autonomous), Tiruchengode, Namakkal-637

Abstract: ***Nowadays, cloud computing has attained great prominence due to various reasons for instance, on demand resource sharing and online storage of data. It is a collection of shared pool of information, resources that makes up a cloud. In this paper, emphasis is to provide a various encryption techniques and effective security solution and also to reduce cloud storage to reduce its overhead. The various security techniques over cloud platform and show analysis of protection by using various cryptographic techniques which is most useful and helpful in the information security. This technique is a two way secured data encryption system, which focus on the matters related to user's privacy, authentication and accuracy. The security and performance of encryption algorithms must be balanced. This paper, encryption algorithms (AES, Blowfish, RSA) has been discussed to analyze the performance level of each algorithm.***
Keywords: Cloud Security, Symmetric & Asymmetric Encryption, Data Integrity, Cryptography

I. INTRODUCTION

Cloud computing is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g.,
networks, servers, storage, applications and services),[1]which can be rapidly provisioned and released with minimal management effort. Now a day's Security of data has become a big distress. Hence, to block these loop holes related to security, an integrated methodology is proposed in this paper. This involves utilization of two algorithms, asymmetric encryption-Rivest, Shamir and Adleman (RSA) and symmetric Key Standard-Advanced Encryption Standard (AES) to provide two way data encryption. As we know, in encryption a plain text is transformed into cipher (secret)text using a special key before transmission [2]. This key can be either public or private. However at receiver side,
in decryption, this cipher text is then decoded in order to obtain the original message using a key. Many algorithms have been given in literature for the encryption and decryption so far [3-5].
In this paper we will discuss about various security techniques over cloud platform and show analysis of protection by using various cryptographic techniques which is most useful and helpful in the information security.

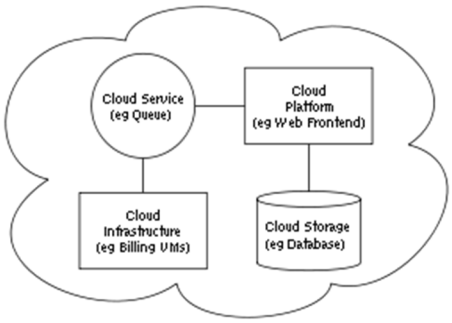


Fig 1: cloud computing

II. LITERATURE REVIEW

Cloud computing has some unavoidable flaws like security of data, files system, backups, network traffic, host security. They have suggested a concept of digital signature with RSA algorithm, to encrypt the data while drifting it over the network. Thus, by this,

©IJRASET: All Rights are Reserved

dual problem of authentication and security is solved. The potency of their work is the framework proposed to address security and privacy issue.

Priyanka Ora, P.R.Pal [6] has proposed a system to maintain data integrity and data confidentiality. To provide its finest level of security, combination of two cryptography scheme is implemented to generate a new encryption pattern before uploading it to the server. In addition to maintain its integrity and confidentiality, data backups are performed that also serves the purpose of security as well by making checks on this data backup.

In[7] authors discussed the various problems associated with cloud computing like data privacy, security, accessibility and reliability etc. But the most important between them is security and how cloud provider assures it. In this paper, the proposed work plan is to remove the issues regarding data privacy using encryption algorithms to enhance the security on cloud. He proposed various encryption algorithms such as AES, DES, RSA and Blowfish that will enhance the performance of cloud. He proposed the model through which we can compare these algorithms and can determine the best algorithm in terms of providing security to the cloud.

In [8] authors analyzed and found an efficient encryption algorithm which takes less space among these encryption algorithms such as DES, TDES, AES, Blowfish and Twofish.

After analyzing above result we found that TDES is better than all these algorithms. DES takes less space than TDES but DES is not a secure algorithm because after 2^56 imagination brute force attack can crack this algorithm. TDES is strong algorithm but it also takes almost two times more space than DES.

In [9] authors proposed a hybrid model which uses a combination of two symmetric algorithms enhanced AES and Blowfish for data confidentiality, Message Digest-5 for data integrity, Elliptic Curve Diffie Hellman algorithm-ECDHA for key exchange and Elliptic Curve Digital signature algorithm-ECDSA is used for digital signature. In this, AES is enhanced by modifying the S-boxes columns, and then the combination of enhanced AES and blowfish is used for data confidentiality.

Performance of this system is evaluated on the basis of encryption/decryption time, throughput and memory usage for different data formats like text file, image file, audio file and video file.

In [10] authors surveyed the various techniques of cryptography and compare them to determine the best technique for security. They have described particularly four algorithms i.e. AES, DES, TDES and Blowfish and compare them according to their encryption times. They concluded that Blowfish is better in terms of speed followed by AES. Other algorithm such as 3DES has least efficient performance as compared to other. In future, Encryption techniques can be used in such a way that it can consume less time and power.

III. SECURITY TECHNIQUES

To secure the cloud, various encryption/decryption algorithms are used to store the data on cloud in encrypted form and retrieve the data from cloud in decrypted form.

2.1 Algorithms used AES AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. 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.

A. AES performs following steps for encryption/decryption

1) First step is to generate round keys, round keys are generated using Rijndael's key schedule
2) The plaintext is converted to4 x 4 state matrix.
3) Each byte of the state is combined with the round key using bitwise xor.
4) This is followed by ten rounds. In each of the first nine rounds, it performs four steps.
5) Byte substitution in which each byte of state is replaced with the byte of S-Box in case of encryption and with the byte of Inverse S-Box in case of decryption depending upon its value
6) Shift rows in which first row of state matrix remains unchanged, second row shifts by 1 bit to the left, third row shifts by 2 bits to the left and fourth row shifts by 3 bits to the left. In case of decryption, shifting is to the right.
7) Mix Columns in which each byte is replaced by a value dependent on all 4 bytes in the column
8) Fourth step is Add Round Key in which each byte of the state is combined with the round key using bitwise xor.
9) In last round, it performs three steps only, the mix columns step is not performed in last step. The detailed descriptions of all stages are given as:
10) Substitute bytes or Sub bytes :It consists of a well-defined lookup table formed with a 16×16 matrix of byte values called an s-

©IJRASET: All Rights are Reserved

box. For a certain round, each byte is transformed into a new byte. Left nibble of a byte denotes a specific row of s-box and the right nibble indicates a column. The matrix that gets operated upon throughout the encryption is known as state.

11) Shift rows :In this state nth row is shifted to the left in circular manner by a factor n-1 as described below:
12) The first row of state remains same.
13) The second row is circularly shifted by one byte in the left.
14) The third row is circularly shifted by two bytes in the left.
15) The fourth row is circularly shifted by three bytes in the left. One byte circular shift is equivalent to a linear shift of four byte
16) s. his circular shift also confirms that the four bytes of one row are dispersed in four different columnsMix Columns: This stage is also a substitution stage but it exploits arithmetic of GF(28). Every column is operated individually. Every byte of a column is converted into a new value which is a function of all the four bytes of that column
17) Add Round Key In this stage, bits(128)of state are bitwise XOR with the bits(128)of the round key. The operation can be regarded as column wise operation among the 4 bytes of a \column of state and 1word of the round key. This transformation should be simple to improve efficiency and also effects every bit of state. Decryption is similar and done using inverse of all the encryption stages.

B. Advantage of AES

1) Fast in hardware and software implementations.
2) Big size data encryption can be done.
3) Provisions for larger key size
4) Less prone to attack.

C. Disadvantages of AES

1) Key exchange is major issue as the same shared key is used for both encryption and decryption.
2) Prone to interpolation attack.

D. Blowfish

Blowfish is a symmetric block cipher designed by Bruce Schneier in 1993. It is a variable length key, 64-bit block cipher. It uses a 32 to 448-bit key. It consists of two parts: The expansion of the key: break the original key into a set of sub keys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit sub keys, while each S-box contains 256 entries. The encryption of the data:64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).

1) The input is a 64-bit data element, x.
2) Divide x into two 32-bit halves: xL, xR.
3) Then, for i = 1 to 16.
4) xL = xL XOR Pi xR = F(xL) XOR xR
5) Swap xL and xR
6) After the sixteenth round, swap xL and xR again to undo the last swap.
7) Then, xR = xR XOR P17 and xL = xL XOR P18
8) Finally, recombine xL and xR to get the cipher text

E. Rivest, Shamir and Adleman(RSA)

RSA is the widely used encryption algorithm for securing the data[11]. In RSA, key used to encrypt the data is public key which is different from the key used in decryption. Thus, the decryption key is secretly preserved. This asymmetry is constructed using the method off actor the product of two large prime numbers. In this technique, both the plain text and cipher text are integers in between 0 and k-1 for some value k.The plain text is encrypted in blocks, with each block having a binary value less than k. The public key in this technique consists of the k(which is termed as modulus) and e(referred aspublic exponent).

The private key contains modulus k and d(known as private exponent)[12].The public-key and private-key can be produced using the following steps:

1) Generate two random large prime's p and q.

©IJRASET: All Rights are Reserved

2) Calculate modulus k as k= p*q.
3) Choose odd public exponent e in between 3 and k-1 which is relatively prime to p-1 and q-1.
4) Calculate private exponent d using e, p and q.
5) Output (k, d) as the private key and (k, e) as the public key.

The encryption in RSA is done as:

$c = \text{encrypt}(t) = t^e \bmod k$

where t is the input text or message; the output c is the cipher text . The decryption operation is described below:

$m = \text{DECRYPT}(c) = c^d \bmod k$.

The relationship between e and d is maintained in such a way that encryption and decryption are inverses. Hence, the original text or message t can be recovered easily from decryption operation. The private key (k, d) (or equivalently the prime factors p and q)is mandatory to recover t from c. Therefore, k and e can be easily made public without negotiating security.

G. Advantages of RSA

1) Due to asymmetric key pair (private key and public key pair)no key exchange problem occurs.
2) Increased security and convenience.
3) Provides digital signatures that cannot be repudiated.

H. Limitations of RSA

1) More memory is used
2) Large size data encryption cannot be done using RSA
3) Slow
4) Susceptible to impersonation attacks

IV. PROPOSED APPROACH

Bearing all security concerns in mind, we have a hybrid structure of ECC and MD5 as our solution to overcome the risk of data confidentiality, integrity and its security. It was created by taking the consideration of elliptical curve theory that uses the elliptic equation to generate keys. Data is more secure than other algorithms because here data slicing is performed as a part of encryption which will not only enhance its security but also reduces its storage capacity. In addition to that we collaborate MD5 that create a digest form which makes the security of data even more strong.

The keys created through ECC takes less memory space and provide better encryption results. It provides great level of security even on lower computing power resources. It generates a hash value for every data that is being uploaded and Use of ECC and MD5 in a distributed environment will provide better security results to our approach.

V. CONCLUSION

In this paper proposed scheme is used to provide for enhancing security on the cloud server. For this we use ECC and MD5 as a hybrid security mechanism. Encryption and decryption is done by ECC and MD5 is used for data digestion form which enhances the security.

REFERENCES

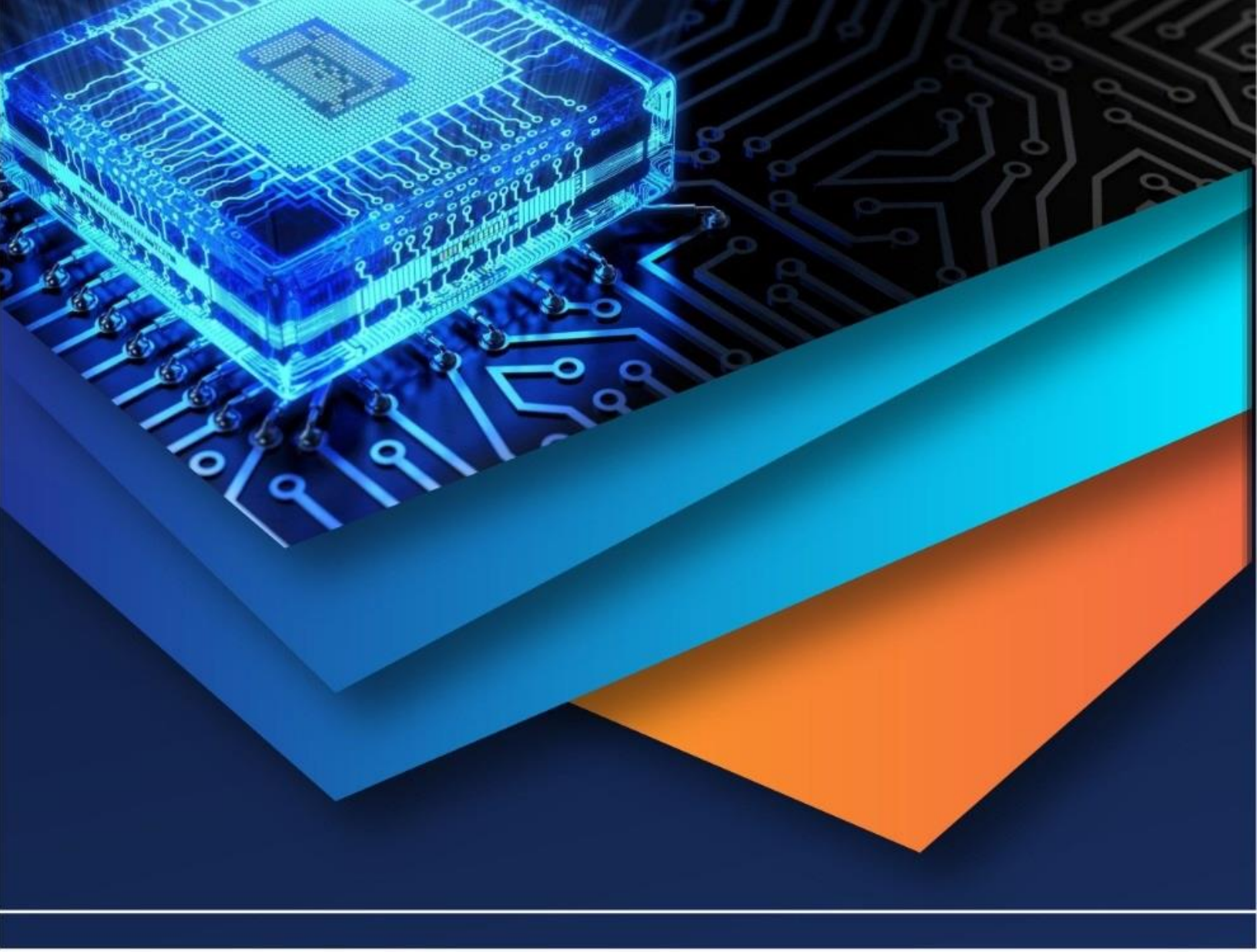
[1] Hassan, Qusay" Demystifying Cloud Computing". The Journal of Defense Software Engineering,December 2014.
[2] D.Delfs., and K. Helmut, " Introduction To Cryptography: Principles and applications", Second Edition, Springer Science & Business Media, (2007); Germany.
[3] K. Mehto, “A Secured and Searchable Encryption Algorithm for Cloud Storage,” vol. 120, no. 5, pp. 17–21, 2015.
[4] R. S and H. P. O H, “Biometric Based Approach for Data Sharing in Public Cloud,” Ijarcce, vol. 4, no. 2, pp. 95–97, 2015.
[5] A. I. Technology, H. Education, F. Women, H. Education, and F. Women, “ensuring security on mobile device data with two,” Vol. 80, no. 2, Pp. 221–226, 2015.
[6] Priyanka Ora, P.R.Pal, “Data Security and Integrity in Cloud Computting Base On RSA Partial Homomorphic and MD5 Cryp-tography,” In IEEE International Conference on Computer, Com-munication and Control, 2015.
[7] Mandeep kaur and Manish Mahajan , “Using encryption algorithms to enhance the data security in cloud computing”,International Journal of Communication and Computer Technologies, Vol. 1, No. 12, Pp. 56-59,2013.
[8] MD Asif Mushtaque Harsh Dhiman and Shahnawaz Hussain Shivangi Maheshwari, “Evaluation of DES, TDES, AES, Bowfish and Twofish encryption algorithm: based on space complexity”, International Journal of Engineering Research & Technology (IJERT), Vol. 3, No. 4, Pp. 1922-1933, 2014.
[9] A. P Shaikh and V. kaul, “Enhanced security algorithm using hybrid encryption and ECC”,IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 6, Issue 3, Pp. 80-85, 2014
[10] Mitali, Vijay Kumar and Arvind Sharma, “A Survey on Various Cryptography Techniques”, International Journal of Emerging Trends & Technology in

©IJRASET: All Rights are Reserved

Volume 5 Issue, May 2017
ISSN: 2321-9653

Computer Science (IJETTCS), Vol. 3, No.4, 2014.
[11] N.Y. Goshwe, Makurdi "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" IJCSNS International Journal of Computer Science and Network Security, Vol.13, no.7,(2013
[12] G. Singh, A. Singla, K.S. Sandha "Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 No.4, August.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)