iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 Issue: XI Month of publication: November 2016

DOI:

Volume 4 Issue XI, November 2016
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Review on Advanced Encryption Standard Algorithm in Cloud Computing

Rishith Polepally[1], T. Shanthan Reddy[2], Priya G[3]
[1,2,]Student ,School of Computer Science and Engineering, VIT University ,Vellore
[3]Assistant Professor, School of Computer Science and Engineering, VIT University, Vellore

Abstract— ***Cloud computing is a progressive figuring worldview, which engages adaptable, on-request, and minimal effort utilization of registering assets . Cloud computing is developing quick with time .But the information is outsourced to some cloud servers, and different security concerns rise up out of it. Thusly, Security is a fundamental segment in cloud computing for ensuring clients data is determined to the secured mode in the cloud .The development of the cloud clients has lamentably been went with a development in pernicious movement in the cloud. Security is a tidy worry in the utilization of cloud computing. In this paper we have reviewed an outline of security issues besides analyse the common sense of applying encryption calculations for data security and insurance in disseminated storage.***

Key Words—Cloud Compting, AES

I. INTRODUCTION

Cloud computing is a developing innovation which has increased noteworthy consideration as of late. It offers benefits through the web. Client can send the administrations of various programming by utilizing cloud computing without purchasing or introducing them all alone PCs. It is the coherent representation of the web in the graphs that is the reason is called cloud computing. As indicated by the meaning of NIST, "Cloud computing can be characterized as processing worldview for empowering on-request, valuable system access to the extensive pool of configurable registering civilities". Cloud computing is the expansion web based innovation of the dispersed processing, which utilizes the web and the remote servers to bolster applications and information. Today Numerous associations are feeling weight to lessen IT costs and advance IT operations[12],[13]. Cloud computing is quickly rising as a feasible intends to make dynamic, quickly provisioned assets for working stages, applications, advancement situations, stockpiling and reinforcement abilities, and numerous more IT capacities[1]. An amazing number of security contemplations exist that data security experts need to consider while assessing the dangers of cloud computing. "Large amounts of information repositioning have off-putting suggestions for information security and information shield and additionally information accessibility" [2]. Along these lines the principle stress with respect to security of information dwelling in the Cloud is: the manner by which to ensure the security of data or information which is at rest.

Cloud computing is a sort of information advancement which is being used where lesser interest in effective programming is required. Cloud computing includes Access to applications and organizations is enabled over the framework and it in like manner require simply access to web association. Maybe one can get access of the cloud with the usage of an ordinary client basically wherever and at whatever time and one needs a particular information office, with no external software. "Cloud computing in like manner empowers the clients for speedy access to pre-set ordinary however gainful information resources (as access to the framework, hardware, stockpiling limits, programming, and extraordinary data benefits) that are vivaciously available without a wide comprehension making process".

Most of the generous associations have propelled their own specific "cloud computing" stages and establishments for customers to pass on their web applications on these stages. Inside the cloud computing world, the environment which is virtual allows customer to get to figuring power that outperforms that contained inside their own specific physical universes. To enter this virtual environment obliges them to trade data on the cloud. Hence, a couple data stockpiling concerns can develop. Regularly, clients will know neither the correct area of their information nor alternate wellsprings of the information altogether put away with theirs. To ensure data grouping (neutralizing activity of unapproved presentation of information), uprightness (change in data), openness (arrangement of right organization at all times), constancy (congruity of right organization), and the organization supplier must offer limits that, at any rate, consolidate an attempted encryption development.

II. SECURITY ISSUES

Digital wrongdoing's belongings are felt all through the web, and cloud computing is a luring focus for some reasons. Suppliers, for example, Amazon, Google, and Microsoft have the current framework to redirect and survive digital assaults, however not each cloud has such ability. In the event that a digital criminal can distinguish the supplier whose vulnerabilities are the least demanding to adventure, then this substance turns into a profoundly noticeable target. If not all cloud suppliers supply satisfactory efforts to establish safety, then these mists will turn out to be high-need focuses for digital lawbreakers. By their design's inalienable nature, mists offer the open door for synchronous assaults to various sites, and without legitimate security, many sites could be bargained through a solitary malignant movement.

Security in Cloud computing is exceptionally vital with the goal that it would be more viable and valuable. The clients don't have any idea where their information is put. Since client's information is put some place on the cloud so there may be probability that an outsider who is taking care of that put away information. Some unlawful activities can hurt the data and which called as “Cyber Crime”[13]. The following security issue in cloud is that it has a solitary purpose of disappointment. Since cloud is a name given to a gathering and this is for single customer and additionally it is for the various customers so one mix-up or failure can influence the entire group. Another issue related to its security is that the programmer hack's the cloud data and also the customer account.

Cloud computing security incorporates various issues like multi tenure, information misfortune and spillage, simple openness of cloud, personality administration, dangerous API's, administration level understanding irregularities, patch administration, inner dangers and so on. It is difficult to authorize all the efforts to establish safety that meet the security needs of the considerable number of clients, on the grounds that distinctive clients may have diverse security requests depends upon their goal of utilizing the cloud administrations.

III. EXISTING ALGORITHMS FOR SECURITY

In [1], it is expressed that to give secure correspondence over the framework, encryption estimation accept a key part. It is an essential device for guaranteeing the data. Encryption figuring changes over the data into blended structure by using "the key" and just customer have the best approach to decipher the data. In “Symmetric key encryption”, one and just key is used to scramble and unscramble the information. Another strategy involves “asymmetric key encryption” where two types of keys which are private and open keys are utilized. “Open key is utilized for encryption of data and private key is used for decrypting” [1].

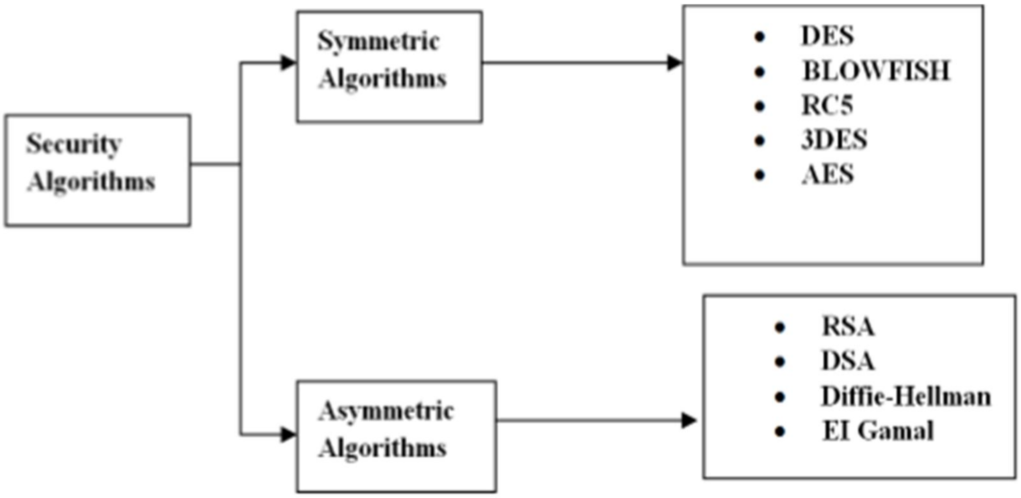

Fig.1 Security Algorithms

IV. LITERATURE REVIEW

In [4] it is stated that Advanced Encryption based security calculations AES is helpful to wipe out the worries in regards to data loss, isolation and protection while accessing web application on cloud. Algorithms like: AES, DES, RSA have been used and relative study among them have likewise been exhibited to guarantee the security of information on cloud [1]. “DES, AES, Blowfish are symmetric key calculations, in which a solitary key is utilized for both encryption/decryption of messages. AES (Advanced Encryption Standard) was planned by NIST in 2001” [2]. The DES (Data Encryption Standard) was made in around mid 1970s by IBM [2]. “RSA is an open key calculation concocted by Rivest, Shamir and Adleman in 1978 furthermore called as Asymmetric key calculation, the calculation that utilizations distinctive keys for encryption and decryption purposes”. “The key sizes of the considerable number of calculations are not quite the same as each other. The key length of DES calculation is 56 bits. The key size of AES calculation is 128, 192, 256 bits [11]. The key size of RSA calculation is 1024 bits” [1],[6].

V. SECURITY ALGORITHMS

A. AES Algorithm

In [7], it is suggested that Advanced Encryption Standard (AES), generally called Rijindael is used for securing information. AES is a symmetric piece figure that has been investigated broadly and is used for the most of the applications in today’s time. “The main question is how AES works in cloud environment?” The AES, “symmetric key encryption” estimation uses 128-bits key length [3]. As AES is used extensively in recent times for security of cloud. Execution recommendation communicates that First, User uses cloud benefits and will move his data on cloud [2]. By then User gives his organizations necessities “Cloud Service Provider” (CSP) and picks best demonstrated organizations offered by supplier. Right when movement of data to the picked CSP happens and in future at whatever point an application exchanges any data on cloud, the data will at first encoded using AES algorithm and after that sent to supplier. Once encoded information is exchanged on the cloud, any requesting to scrutinize the data will happen after it is decoded on the customers end and a while later plain content information can be perused by customer [2]. The plain content information is never composed anyplace on cloud. This incorporates a wide range of data. This fuses an extensive variety of data. This encryption game plan is clear to the application and can be composed quickly and viably with no change to application. The key is never put away close to the scrambled data, since it may trade off the key also. In order to store the keys, a physical key organization server can be presented in the customer's premises. This encryption secures data and keys and guarantees that they stay under customer's control and will never be revealed away or in travel [16].

B. Implementing AES Algorithm

AES is a type of block encrypter with a square length of 128 bits. "It grants three unique key lengths: 128, 192, or 256 bits". In [8] it is proposed AES which has 128 piece key length. The encryption technique involves 10 rounds of handling for 128-piece keys. Beside the last round for each circumstance, each and every other round are vague. "16 byte encryption key, as 4-byte words is wandered into a key timetable containing 44 4-byte words"[8]. The 4 x 4 structure of bytes created utilizing 128-piece input square is implied as the state display. Before any round-based get ready for encryption can begin, input state is XORed with the underlying four articulations of the schedule [11].

C. Algorithm

```
“Cipher(byte[] input, byte[] output)
{
byte[4,4] State;
copy input[] into State[] AddRoundKey
 for (round = 1; round < Nr-1; ++round)
{

 SubBytes ShiftRows MixColumns AddRoundKey

}
SubBytes ShiftRows MixColumns AddroundKey
 copy State[] to output[]
}”
```

1) “Key Expansion: First from the cipher key the round keys are derived using the key schedule of Advanced Encryption Standard.
2) “Initial Round - AddRoundKey: Then each byte of the state is combined with the round key using bitwise XOR
3) Rounds
   a) *SubBytes: This is a non-linear substitution step where each byte is swapped with another according to a lookup table[9].*
   b) *ShiftRows: In this transposition step each row of the state is shifted cyclically in a certain number of steps.*
   c) *MixColumns: A mixing operation operates on the columns of the state, combining the four bytes in each column.*

d) *AddRoundKey[9].*

4) *Final Round (no Mix Columns)*

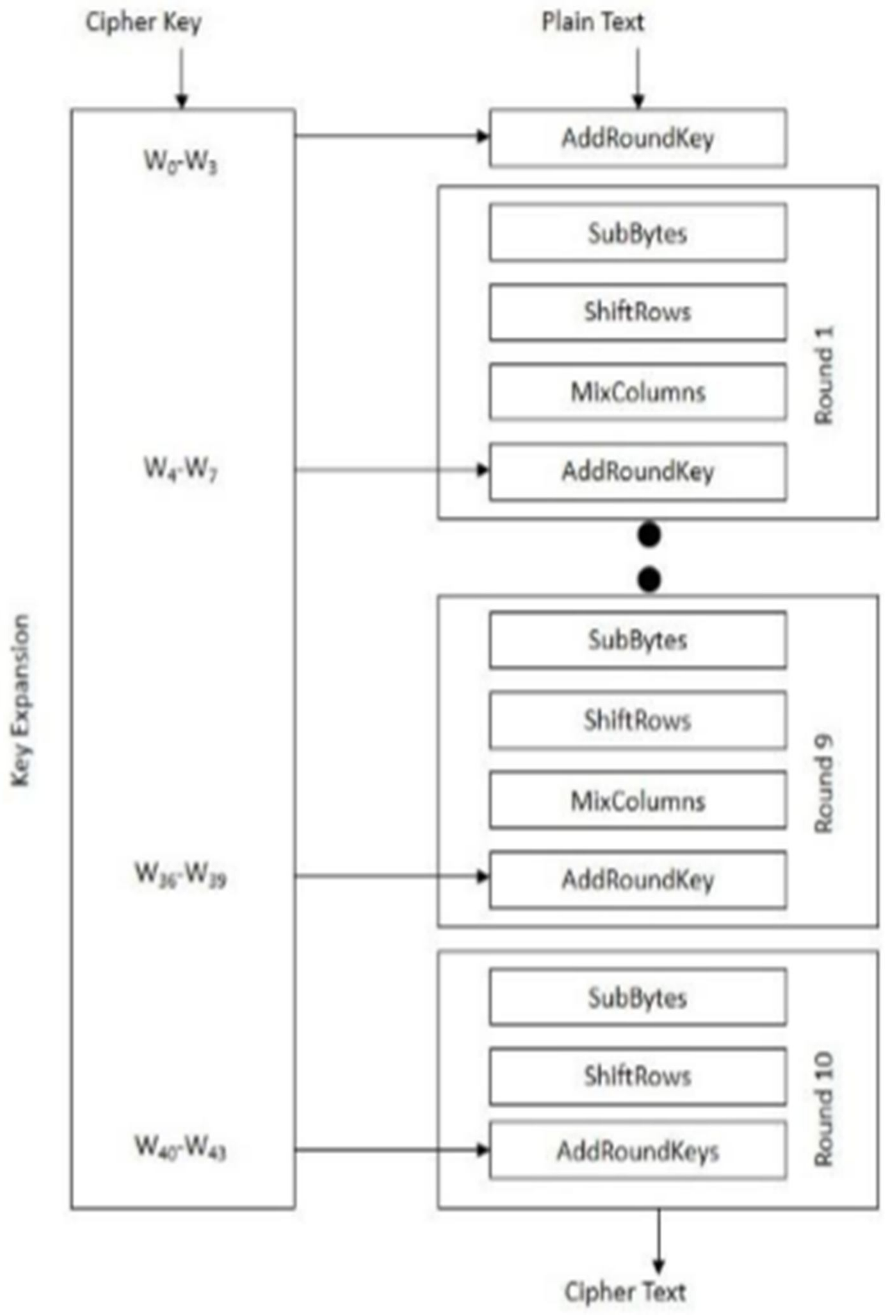

Fig. 2 AES Encryption

a) *SubBytes*: "The purpose of this step is to give ample resistance from differential and linear cryptanalysis attacks." This is byte-by-byte substitution where each byte is substituted self-sufficiently using Substitution table (S-box). Each info byte is isolated into 24-bit plans, speaking to a whole number esteem somewhere around 0 and 15 which can then be deciphered as hexadecimal qualities. "Left digit describes the line rundown and right digit portrays the area rundown of S-box. At the intersection purpose of line and area, regard given is substituted. There are sixteen specific byte-by-byte substitutions. S-box is worked by a mix of GF (28) number-crunching and bit damaging" [4], [9].

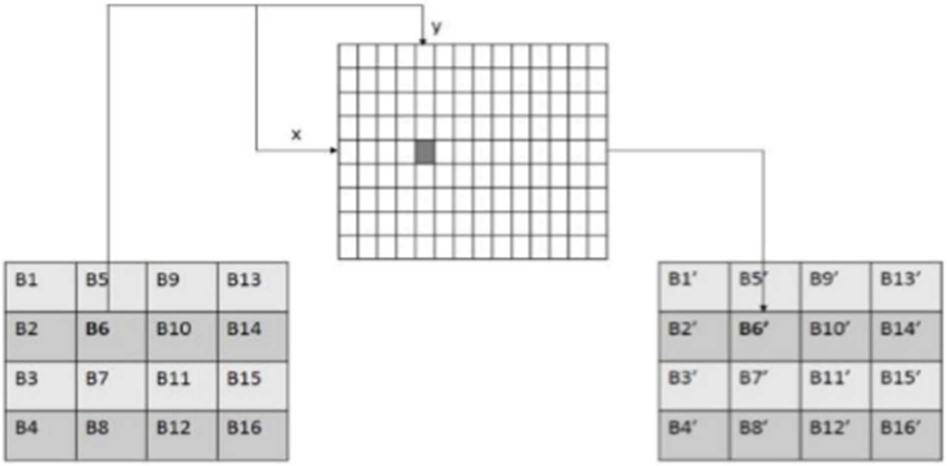

Fig.3 Sub Bytes Transformation Step

b) *ShiftRows*: The utilization of this methodology is to give dispersion of the bits over different rounds. The line 0 in the lattice is not moved, push 1 is roundabout left moved by 1 byte, push 2 is roundabout left moved by 2 bytes, and column 3 is roundabout left moved by 3 bytes[9], [19].

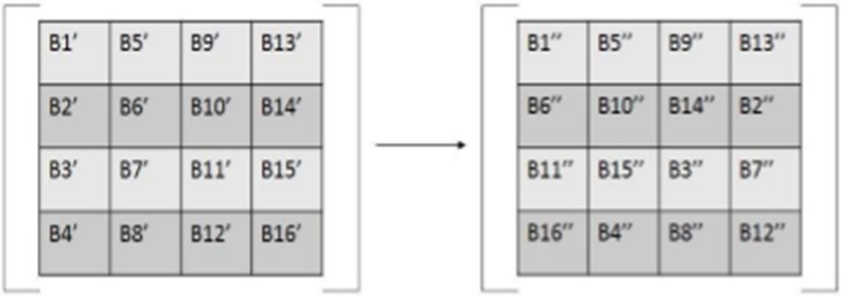

Fig. 3 Shift Rows Transformation Step

c) *MixColumns*: Like past method, the inspiration driving this movement is to give scattering of the bits over various rounds. This is refined by performing increase one section without a moment's delay. Each esteem in the segment is increased against every line estimation of a standard lattice. The outcomes of these duplication are XORed together. For clear understanding we take an example: estimation of first byte B1" is increased with 02, 03, 01 and 01 and XORed to convey new B1'"[19] of coming to fruition cross section. The incrementation proceeds against one framework push at once against every estimation of a state section [19], [21].

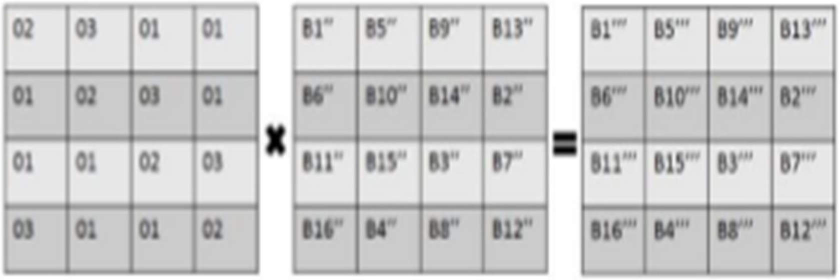

Fig. 5 Mix Columns Transformation Step

d) *AddRoundKey*: In AddRoundKey transformation, a roundkey is added to the State by bitwise Exclusive-OR (XOR) operation[21].

D. Decryption

Decryption is the way toward removing the plaintext from cipher content. The Decryption structure of proposed algorithm is acquired by modifying the encryption structure which is appeared previously. Comparing to the changes in the encryption, "InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey" are the changes utilized as a part of the decryption. The roundkeys are the same as those in encryption created by Key Expansion, yet are utilized in reverse order [21].

E. Why AES?

1) "AES performs dependably well in both equipment and programming stages under a broad assortment of environents. These consolidate 8-bit and 64-bit stages and DSP's".
2) Its trademark parallelism energizes profitable usage of processor assets achieving incredible programming execution.
3) This calculation has convenient key setup time and extraordinary key finesse.
4) This algorithm require very less memory for utilization, by making it sensible for constrained storage circumstances.
5) Its structure has incredible potential of benefitting from direction level parallelism.
6) Genuine Powerless keys aren't there in AES [6].
7) It also supports multiple block sizes and key sizes which are products of 32 (i.e. greater than 128-bits) [7].
8) "Statistical analysis of the cipher content has not been conceivable even in the wake of utilizing tremendous number of experiments".
9) "No differential and direct cryptanalysis assaults have been yet demonstrated on AES".

VI. COMPARING AES WITH OTHER ALGORITHMS

The way that the figure and its reverse utilize unmistakable fragments basically discards the probability for week and semi-weak keys in AES, which is a present drawback. Also, nonlinearity of the key improvement in every way that really matters wipes out the probability of proportionate keys in AES. An execution relationship among AES, DES and Triple DES for various microcontroller's show that AES has a PC cost of an indistinguishable request from required for Triple DES [8]. Another evaluation reveals that AES has influence over calculations 3DES, DES and RC2 to the extent execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption and decoding. In like manner by virtue of changing information sort, for instance, picture rather than content and also AES has an advantage over RC2, RC6 and Blowfish to the extent time utilize. [6][7]

VII. CONCLUSION

In [17], it is stated that General spending on cloud organizations is set to take off. As showed by a report, "Worldwide and Regional Public IT Cloud Services 2014-2017 Forecast" released by IDC, cloud administrations undergo as much as 41% advancement from 2014 to 2017[16]. "Spending on IT cloud organizations worldwide will edge toward $100 billion by 2016". Moreover, in this cloud advancement, security will expect a key part. Customers will be set up to benefit cloud organizations, and cloud suppliers need to legitimize security, privacy issues and satisfy customers. Each of the cloud suppliers has their own specific arrangement of principles, evaluating, versatility, bolster and other basic parameters. The key thought managed in this proposition is the encryption pattern to secure information by making it confused for all. "Executing AES for security over data gives favourable circumstances of less memory use and less calculation time when diverged from various calculations". Notwithstanding the way that each cloud framework has its own particular security qualities; the customer can pick base as showed by his security necessities. AES offers security to cloud customers as scrambled information in the cloud is protected from various assaults [14],[16],[17].

REFERENCES

[1] Randeep Kaur ,Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing".Available: www.ijaiem.org
[2] K.S.Suresh, Prof K.V.Prasad , "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering.
[3] Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications.
[4] Zhiyi Fang, Yao Sun, Yujing Sun, Jianming Yang, "The Reseach of AES algorithm and application in cloud storage system", 2nd International Conference on

Science and Social Research (ICSSR 2013) .

[5] K. Vijayakumar, “Security issues and Algorithms in Cloud Computing”, Global Journal of Advanced Research, 2010.

[6] Navrang Pal Kaur, “Comparison between RSA and Triple DES in Cloud Environment”, International Journal on Recent and Innovation Trends in Computing and Communication.

[7] Mrunalini Motilal Shete, Pragati Damodar Hipparkar, “Data Secure in Cloud Computing Using Encryption Algorithms by Mrunalini Motilal”, International Journal of Science and Research (IJSR).

[8] Khushboo Gupta, Neha Goyal, Puneet Rani, “Study of Security Algorithm to Provide Triple Security in Cloud Computing” , International Journal of Scientific and Research Publications, Volume 4, Issue 6, June 2014

[9] Vishal R. Pancholi, Dr. Bhadresh P. Patel - Enhancement of Cloud Computing Security with Secure Data Storage using AES, IJIRST –International Journal for Innovative Research in Science & Technology ,Volume 2 ,Issue 09 , February 2016

[10] Asfiya Shireen Shaikh Mukhtar, Ghousiya Farheen Shaikh Mukhtar - An Introduction of Advanced Encryption Algorithm: A Preview .

[11] Ellen Messmer (2012). Gartner: Growth in Cloud Computing to shape 2013 security trends,Network World[Online].Available: http://www.networkworld.com/news/2012/120612gartner-cloud-security-264873.html

[12] Sachdev Abha Thakral, and Mohit Bhansali. "Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.

[13] Talbot, David (2009). “How Secure Is Cloud Computing?” Technology Review [Online]. Available: http://www.technologyreview.com/computing/23951/

[14] Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance Evaluation of Symmetric Encryption Algorithms." IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.

[15] Gurpreet Kaur, Nishi Madaan , “A Comparative Study of AES Encryption Decryption”, International Journal of Science and Research (IJSR).

[16] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit.com/news/technology/1112692915/c loud-computing-growth-paas-saas-091212/

[17] Worldwide and Regional Public IT Cloud Services 20122016 Forecast [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=236552

[18] Ritu Pahal , Vikas kumar -Efficient Implementation of AES Online: www.ijarcsse.com

[19] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “Cloud security issues” In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[20] Xinmiao Zhang and Keshab K. Parhi,”Implementation approaches for the advanced encryption standard algorithm”, IEEE Transactions 1531-636X/12©2002IEEE