REVIEW OF RESEARCH
IMPACT FACTOR : 5.7631(UIF) UGC APPROVED JOURNAL NO. 48514 ISSN: 2249-894X
VOLUME - 8 | ISSUE - 1 | OCTOBER - 2018

ANALYSIS OF SYMETRIC ALGORITHMSDES AND AES IN CLOUD SECURITY

Dr. Girish Katkar[1] and Ms. Punam R. Naphade[2]
[1]MSc., Ph.D , Asstt. Prof. , Taywade College,Koradi.
[2]M.Sc.(C/S) , Asstt. Prof. RAICSIT, Wardha.

ABSTRACT

Cloud computing supports distributed service oriented architecture, multi – users and multi – domain administrative infrastructure.Cryptography is the science of making data and messages secure by converting the end user data to be sent into cryptic non – readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text and then performing decryption which is reverting back to the original plain text.Depending upon the number of keys used, modern crypto graphic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). The key length of this calculation is 56 bits; anyway a 64 bits key is really input. DES is consequently a symmetric key algorithm.Advanced Encryption Standard (AES), otherwise called Rijindael is utilized for anchoring data. AES is a symmetric square figure that has been examined broadly and is utilized generally now-a-days.

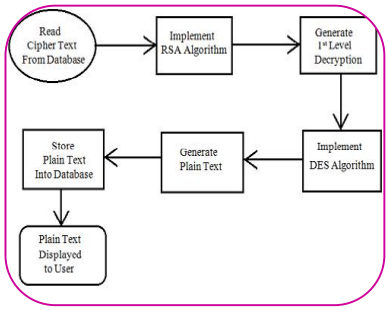
KEYWORDS: *Cryptography, Encryption, Decryption, AES, DES.*

INTRODUCTION

Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the internet. Cloud computing supports distributed service oriented architecture, multi – users and multi – domain administrative infrastructure. It is more prone to security threats and vulnerabilities. At present a major concern in cloud adoption is its security and privacy. Intrusion prospects within cloud environment are many and with high gains. Security and privacy issues are of more concern to cloud service provides.

SEQUIRITY THROUGH CRIPTOGRAPHY

It simple terms, Cryptography [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communication information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non – readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text [2] and then performing decryption which is reverting back to the original plain text.



With the speedy development of computer technology and advancement of internet, the importance and value of exchanged data are increasing. The widen usage of digital media for information transmission through secure and unsecured channels exposes messages sent via networks to intruders or third parties. Therefore to counterpart this weakness, many researches have come up with efficient algorithms

to encrypt information from plain text (or clear text) into cipher text (or encrypted data)[3]

Cryptography is a key technology for achieving information security in various fields such as computer science, e-commerce, and in the emerging information society. Cryptography is the art of combining some input data, called the plaintext, with a user – specified password (or key) to generate an encrypted output, called cipher text, in such a way that, given the cipher text, it is extremely difficult to recover the original plaintext without the key. A key is a succession of images that controls the cryptographic activities, for example, encryption, unscrambling, signature age or mark check [4], [5]. The simplicity or complexity of encryption process depends on encryption algorithm and the key which is used in algorithm to encrypt or decrypt the data. According to the Kirchhoff, the security of the encryption system should depend on the secrecy of the key rather than encryption algorithm. The security level of the encryption calculation ought to rely upon the extent of the key space, mystery of the key, length of the key, instatement vector and how they all cooperate.

Depending upon the number of keys used, modern crypto graphic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). In symmetric algorithms, both parties (I,e, sender and receiver) share the same key for encryption and decryption whereas in asymmetric algorithms two keys are used. One key is used for encryption , called “public key” and the other key is used for decryption, called “private key” Many schemes used for encryption constitute the area of study known as cryptography as shown in Fig. 1

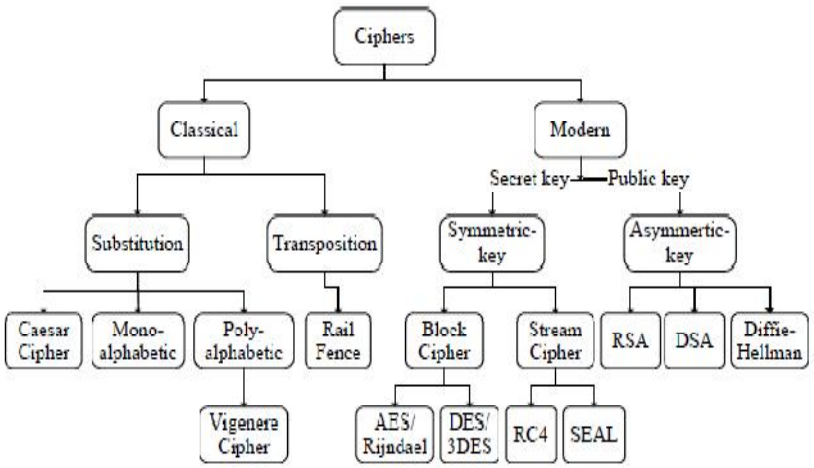


Fig. 1 : Typical Cryptography

With this ability, Cryptography is used for providing the following security:

a) Data Integrity: information has value only if it is correct. This is refers to maintaining and assuring the accuracy and consistence of data, its implementation for computer systems that store use data, processes, or retrieve that data.

b) Authentication for determining whether someone or something is, in fact, who or what it is declared to be.

c) Non Repudiation:Is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.

d) Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

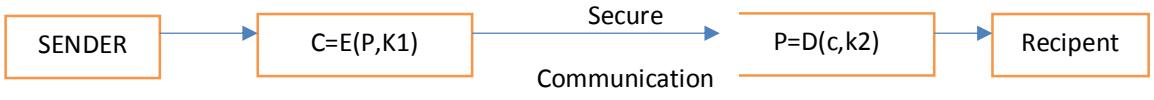


Fig. 2 :Encription And Decription Process

In pure science terms [6], Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverse and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, key}

Defining some terms used in Cryptography:

a) Plaintext is the original intelligible source information or data that is input to algorithms
b) Cipher text is the scrambled message output as random stream of unintelligible data
c) Encryption Algorithm substitutes and performs permutations on plain text to cipher text
d) Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
e) Keys are used as input for encryption or decryption and determines the transformation
f) Sender and Recipients are persons who are communication and sharing the plain text.

With respect to Cloud computing, the security concerns [7] are end user data security, network traffic, file system, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud.

a) Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
b) Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
c) Have Separation of data: Privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
d) Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service Provider.
e) User Access Control: for web based transactions (PCI DSS). Web data logs need to be provided to compliance auditors and security managers.

Security Algorithms are classified broadly as:

a) Private Key/Symmetric Algorithms: Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.
b) Public Key/Asymmetric Algorithms: Use a key pair for cryptographic process. With public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Difie- Hellman are some types of public key algorithms.

SYMMETRIC ALGORITHMS

Symmetric Algorithms involve a single shared secret key [8] to encrypt as well as decrypt data and are capable of processing large amount of data and from computing standpoint are not very power intensive, so has lower overhead on the system and have high speed for performing encryption and decryption. Symmetric algorithms encrypt plaintexts as Stream ciphers bit by bit at a time [9] or as Block ciphers on fixed number of 64 bit units.

There are however few problems with symmetric Algorithms

a) Exchanging Shared Secret Key [10] over unsecure internet. Symmetric – key calculations share mystery keys required by the sender and collector amid encryption of unscrambling process. In case a third person gains access to the secure secret key, cipher text messages can easily be decrypted. The fact of having one single secret key algorithm is the most critical issue faced by Cloud service providers when dealing with end

users who communicate over unsecure internet. The only option is to have that secret key be changed often or kept as secure as possible during the distribution phase.

b) Problem confirming if the content is altered or actually sends by the claimed sender. If a hacker has the secret key, decrypting the cipher text, modifying the information being send with that key and send to the receiver. Since a single key is involved during the crypto process, either side of the transitions can get compromised. Such data integrity and non-repudiation issues however need to involve the use of Digital signatures or Hashing functions like MD5.

c) Tools for cracking Symmetric encryption By use of Brute force [11] by running hacking tools that have the ability crack the combinations and keys to determine the plaintext message and perform Cryptanalysis where the attacks are focused on the characteristics of the algorithm to deduce a specific plaintext or the secret key. Then hackers are able to figure out the plaintext for messages that would use this compromised setup.

PROPOSED WORK PLAN

We have proposed different security algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like; DES, AES have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM, Blowfish was designed by Bruce Schenier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001 The key sizes of all the algorithms is 128, 192, 256 bits. Using Net beans IDE 7.3, and Java Run Time Environment, we have implemented our idea in the form of encryption and decryption algorithms which have discussed above and also we have made comparison between them on the basis of their characteristics.

DATA ENCRYPTION STANDARD (DES) ALGORITHM

DES is one of the most widely accepted, publicly available cryptographic systems. It was produced by IBM in the 1970s yet was later embraced by the National Institute of Standards and Technology (NIST), as Federal Information Processing standard 46 (FIPS PUB 46). The information encryption standard (DES) is a square Cipher which is intended to scramble and decode squares of information comprising of 64 bits by utilizing a 64 bit key [12], [13]

In spite of the fact that the information key for DES is 64 bits in length, real key utilized by DES is just 56 bits long. The minimum noteworthy (right – most) piece in every byte is an equality bit, and ought to be set so that there are dependably an odd number of 1s in each byte. These equality bits are disregarded, so just the seven most huge bits of every byte are utilized bringing about a key length of 56 bits. The calculation experiences 16 emphasis that join squares of plaintext with qualities got from the key. The calculation changes 64 bit contribution to a progression of ventures into a 64 bit yield. Similar strides, with a similar key are utilized for decoding. There are numerous assaults and strategies recorded till now those adventure the shortcomings of DES, which made it an uncertain square figure. Regardless of the developing worries about its weakness, DES is still generally utilized by monetary administrations and different ventures worldwide to secure touchy on line application [14], [15]

The stream of DES Encryption, calculation is appeared in Fig, 3. The calculation forms with an underlying stage, sixteen rounds square figure and a last permutation(i.e, invert introductory change)

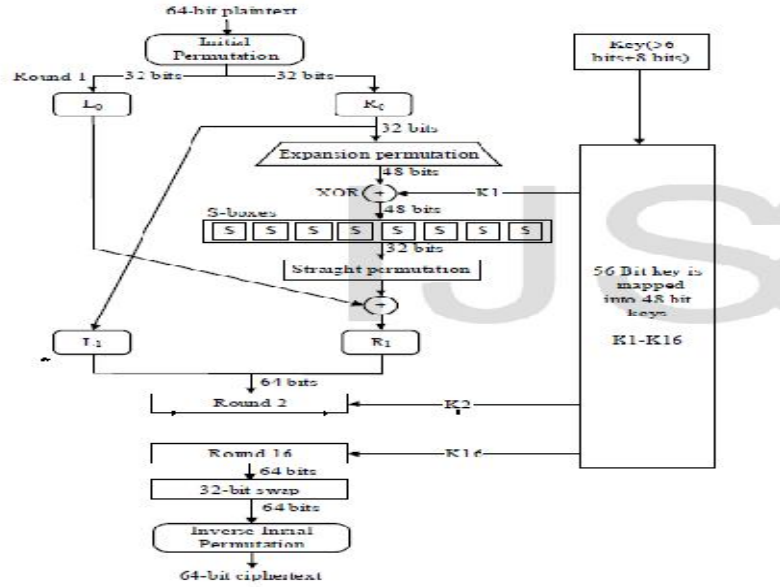


Fig. 3 : Flow of DES Algorithm

The Data Encryption Standard (DES) is a square figure. It scrambles information in squares of size 64 bits each. That is 64 bits of plain content goes as contribution to DES, which produces 64 bits of in good spirits message. A similar calculation and key are utilized for encryption and unscrambling, with minor contrasts. The key length of this calculation is 56 bits; anyway a 64 bits key is really input. DES is consequently a symmetric key calculation.

DES Algorithm :-

function DES _Encrypt (M, K) where M = (L, R)
M ← 1P (M)
For round ← 1 to 16 do
K_i ← SK (K, round)
L ←LxorF(R, Ki)
swap (L, R)
end
swap(L, R)
M←$1P^{-1}$(M)
return M End

ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

Propelled Encryption Standard (AES), otherwise called Rijindael is utilized for anchoring data. AES is a symmetric square figure that has been broke down broadly and is utilized generally now-a-days. How AES works in cloud environment? AES, symmetric key encryption calculation is utilized with key length of 128-bits for this propose. As AES is used widely now-a- days for security of cloud. Implementation proposal states that first. User decides to use cloud services and will migrate his data on cloud. At that point User presents his administrations necessities with cloud administrations supplier (CSP) and picks best determined administrations offered by supplier. At the point when movement of information to the picked CSP occurs and in future at whatever point an application transfers any information on cloud, the information will initially encoded facilitating AES calculation and after that sent to supplier. Once encoded, information is

transferred on the cloud on the cloud, any demand to peruse the information will happen after it is unscrambled on the clients end and afterward torment content information can be perused by client. The plain content information is never composed anyplace on cloud. This incloudsall kinds of information. This encryption arrangement is straightforward to the application and can be coordinated rapidly and effortlessly with no progressions to application. The key is never put away alongside the scrambled information. Since it might bargain the key too. To store the keys, a physical key administration server can be introduced in the client's premises. This encryption secures information and key and ensures that they stay under client's control and will never be uncovered away or in travel.

AES is the new encryption standard prescribed by NIST to supplant DES in 2001. AES calculation can bolster any mix of information (128 bits) and key length of 128, 192 and 256 bits, The calculation is alluded to as AES 128, AES – 192 or AES-256 relying upon the key length. Amid encryption decoding process, AES framework experiences 10 rounds for 128 piece keys, 12 rounds for 192 piece keys, and 14 rounds for 256 piece enters in plain content [16]. AES permits a 128 piece information length that can be isolated into four fundamental activity squares. These squares are treated as exhibit of bytes and sorted out as a framework of the request of 4 x 4 that is known as the state. For both encryption and unscrambling, the figure starts with an Add Round Key stage. In any case, before achieving the last round, this yield goes however nine principle rounds, amid every one of those rounds four change are performed; 1) Sub – bytes, 2) Shift – rows, 3) Mix – columns, 4) Add round key. In the final (10^{th}) round, there is no Mix – column transformation [14], [17]
Each round of AES is governed by the following transformation [12]

1. Substitute Byte change: - AES contains 128 piece information square, which implies every one of the information squares has 16 bytes. In sub byte change, every byte (8-bit) of an information square is changed into another square utilizing a 8 bit substitution box which is known as RijndaelSbox,
2. Shift Rows change: - It is a basic byte transposition, the bytes in the last three columns of the state, contingent on the line area, is consistently moved. For second line, I byte roundabout left move is performed. For the third and fourth column 2 byte and 3 byte left round left moves are performed separately,
3. Mixcolumns change: - This round is comparable to a network augmentation of every Column of the states. A fix lattice is increased to every segment vector. In this task the bytes are taken as polynomials as opposed to numbers
4. Addroundkey change: - It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This change is its own reverse.

Algorithm :

```
Cipher (byte [] input [] output)
{
                byte [4, 4] State;
                copy input [] into State [] Add Round Key
for (round = 1; round < Nr – 1; ++round)
{
SubBytesShiftRowsMixColumnsAddRoundKey
 }
SubBytesShiftRowsAddRoundKey
copy State [] to output[]
}
```

EXPERIMENTAL EVALUATION

In proposed work the AES and DES algorithms are been tested in terms of speed with respect to key size and the file size.

Following tables shows the Encryption and Decryption time taken by the algorithm AES and DES.

Table 1 : Execution time tekaen by AES and DES for Key size 128 bits and the File Sizes 2 , 4, 6, 8 Kb respectively.

Algorithm	Key Size (in Bbit)	File Size (in KB)	Execution Time (in seconds)	
			EcryptionEncryption (in Seconds)	Decryption (in Seconds)
AES	128	2	0.224496022	0.58336
		4	0.226067339	0.71839
		6	0.224621602	0.74655
		8	0.225020381	0.76409
DES	128	2	0.226161003	0.8395
		4	0.224371532	0.80772
		6	0.22980496	0.81643
		8	0.229214565	0.84183

Table 2 : Execution time tekaen by AES and DES for Key size 192 bits and the File Sizes 2 , 4, 6, 8 Kb respectively.

Algorithm	Key Size (in Bbit)	File Size (in KB)	Execution Time (in seconds)	
			EcryptionEncryption (in Seconds)	Decryption (in Seconds)
AES	192	2	0.230372669	0.64489
		4	0.221928997	0.6129
		6	0.221062107	0.59825
		8	0.220219604	0.5.835
DES	192	2	0.221836293	0.4.957
		4	0.223428787	0.60841
		6	0.223817296	0.62478
		8	0.227832462	0.65768

Table 3 : Execution time tekaen by AES and DES for Key size 256 bits and the File Sizes 2 , 4, 6, 8 Kb respectively.

Algorithm	Key Size (in bit)	File Size (in KB)	Execution Time (in Seconds)	
			Encryption	Decryption
AES	256	2	0.225429773	0.48257
		4	0.226459667	0.57929
		6	0.227093386	0.63426
		8	0.230594578	0.65591
DES	256	2	0.227025102	0.60276
		4	0.229705267	0.6101
		6	0.230348215	0.62356
		8	0.231291696	0.65436

CONCLUSION

Cryptography is a key technology for achieving information security in various fields such as computer science, e-commerce, and in the emerging information society. Cryptography is the art of combining some input data, called the plaintext, with a user – specified password (or key) to generate an encrypted output, called cipher text, in such a way that, given the cipher text, it is extremely difficult to recover the original plaintext without the key. A key is an arrangement of images that controls the cryptographic tasks, for example, encryption, decoding, signature age or mark confirmation. The simplicity or complexity of encryption process depends on encryption algorithm and the key which is used in algorithm to encrypt or decrypt the data.

The Data Encryption Standard (DES) is a square figure.It encodes information in squares of size 64 bits each. That is 64 bits of plain substance goes as commitment to DES, which produces 64 bits of happy substance. A comparative figuring and key are used for encryption and interpreting, with minor complexities. The key length of this estimation is 56 bits; anyway a 64 bits key is really input. DES is subsequently a symmetric key calculation.

Propelled Encryption Standard (AES), otherwise called Rijindael is utilized for anchoring data. AES is a symmetric square figure that has been investigated broadly and is utilized generally now-a-days. How AES functions in cloud condition? AES, symmetric key encryption figuring is utilized with key length of 128-bits for this propose. As AES is utilized exhaustively now-a-days for security of cloud. Usage proposition expresses that first. Client chooses to utilize cloud benefits and will move his information on cloud. At that point User presents his administrations necessities with cloud administrations supplier (CSP) and picks best determined administrations offered by supplier. At the point when relocation of information to the picked CSP occurs and in future at whatever point an application transfers any information on cloud, the information will initially encoded facilitating AES calculation and after that sent to supplier. Once encoded, information is transferred on the cloud on the cloud, any demand to peruse the information will happen after it is unscrambled on the clients end and after that torment content information can be perused by client. The plain content information is never composed anyplace on cloud.

While comparing the execution time require for each algorithm, is observed that the encryption time is almost same for different key sizes and for the different file sizes. But decryption time varies with the file sizes. It is observed that the decryption time in AES algorithm is less for the key size 256 bits as compare to the other key sizes. In DES algorithm the decryption time is less for the file size of 2 KB.

REFERENCES :

1) Leena Khanna, Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them",IJARCSSE 2013
2) G Devi, Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm"IJCTT 2012
3) O P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Performance Analysis of Data Encryption Algorithms", 3rd International Conference onElectronics Computer Technology (ICECT) (Volume: 5), pp. 399 - 403, 8-10 April 2011.
4) "Introduction", http://kremlinencrypt.com/concepts.htm
5) IEC 18033-1, Information technology – Security techniques – Encryption algorithms – Part 1: General.
6) Simarjeet Kaur "Cryptography and Encryption in Cloud Computing", VSRD International Journal of CS and IT, 2012
7) Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, MakanPourzandi "A quantitativeanalysis of current security concerns and solutions for cloud computing", Springer 2012.
8) MahaTebba, Saïd Haji Abdellatif Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress onEngineering 2012
9) Cloud Security Alliance (CSA), "Security Guidance for critical Areas of Focus in cloud computing V3.0" CSA 2015
10) AyanMahalanobis, "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups." 2005
11) Neha Jain, Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS and IT, 2012
12) Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.
13) Sriram Ramanujam and MarimuthuKaruppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, pp. 106-111, January 2011.
14) William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.
15) "DES", http://www.tropsoft.com/strongenc/des.htm
16) Gurpreet Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, Volume 67– No.19, pp. 33-38, April 2013.
17) "3DES", http://www.cryptosys.net/3des.html
18) Zilhaz Jalal Chowdhury, DavarPishva and G. G. D. Nishantha, "AES and Confidentiality from the Inside Out", the 12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591, 2010.
19) http://en.wikipedia.org/wiki/Cloud_computing.
20) Rich Maggiani,solari communication. "Cloudcomputing is changing how wecommunicate".
21) Randolph Barr, Qualys Inc, "How to gain comfort in losing control to the cloud".

Dr. Girish Katkar
MSc., Ph.D , Asstt. Prof. , Taywade College,Koradi.

Ms. Punam R. Naphade
M.Sc.(C/S) , Asstt. Prof. RAICSIT, Wardha.