ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Hybrid Cryptosystem for Secure Text File for Cloud

Sarika U. Kadlag[1]
M.E Scholar
Dept. of Computer Engineering
Amrutvahini College of Engineering
Sangamner - India

Rahul L. Paikrao[2]
Assistant Professor & HOD
Dept. of Computer Engineering
Amrutvahini College of Engineering
Sangamner - India

Abstract: ***Cloud computing is distributed environment. It allows consumers and organizations to use application without installation and access their own files at any computer using internet. In this paper proposes cloud computing based on the concepts integrating of encryption and decryption process, Data storage as service. Data Storage as a service (DaaS) allows users to store their data on remote servers and also direct accessed anytime from anywhere to their data using the internet. The data transmission on the internet or over any networks is at risk to the malicious intruders, hacking, etc. Therefore, Users authentication procedures will be design for data storage and retrieval. The user text file will be secured using Hybrid Cryptosystem before storing in cloud and building secure communication channel for text based files transmission and improve performance between client and server by reducing communication time. For this, we propose a method for secure text based files storage and secure text based files retrieval in cloud computing environment by using the Hybrid Cryptosystem. It provides two tier security using Vigenere cipher and reverse circle cipher with symmetric key multi rotational technique.***

Keywords: Cloud computing, Security, Data Storage, Data Encryption, Data Decryption, Cipher, Hybrid Cryptosystem.

I. INTRODUCTION

Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.". - U.S. National Institute of Standards and Technology (NIST). Cloud computing provides three services are SaaS (Software as a service), PaaS (Platform as a service), IaaS (Infrastructure as a service).

Confidentiality Protecting is a technical challenge for cloud provider. In cloud environment, this challenge is complicated by distributed nature of clouds and lack of user knowledge over where the data is stored i.e. about data center and accessibility of the users. In cloud computing have problem like security of data, file systems, backups, network traffic security. Cryptographic encryption is certainly the best practice. Encryption techniques should also be used for data in transmission. In addition authentication and integrity protection ensure that data only goes where the user wants it to go and it's not modified in transmission. User authentication is often the most important for access control. In the cloud environment authentication and access control are more important than since the cloud and all of its data are accessible to anyone over the internet, and also Secure Communication is more important.

The proposes System model is based on the combination of the poly alphabetic cipher Vigenere and the reverse circle cipher with symmetric key multi rotational technique to give a new and more secure two tier security model. In this technique the plain text is encrypted using the Vigenere cipher which keys are generated randomly by the system. For one file, only one

key is generated then re-encrypt the resulted cipher text using reverse circle cipher with symmetric key multi rotational technique to be a more secure cipher text. Three servers, means distributed server concepts are used here for ensuring high security.

In this paper we are going to discuss two tier security approaches for cloud data storage and secure communication channel and the time complexity in cloud. The main feature of the this proposed system is that all cryptographic operations are performed on the client side, which provides the users more control on the security of their data, and thus the data are not dependent on the security solutions provided by the servers. In this proposed system, user data will be secured using Hybrid Cryptosystem before storing in cloud server. This system also helps to solve main security issues like malicious intruders, hacking, etc of cloud storage. Reverse circle cipher with symmetric key multi rotational technique is used for secured communication between the users and the servers. The proposed two tier Security approach in this paper is based on conventional crypto techniques that uses less time requirements and still maintain a adequate level of security.

II. PROPOSED HYBRID CRYPTOSYSTEM

Hybrid cryptosystem is based on the combination of the poly alphabetic cipher Vigenere and the Reverse circle cipher with symmetric key multi rotational technique to give a new and more secure two tier security model. User who wants to go for cloud storage service must be an authorized user and register themselves as a client. The proposed system ensures that unauthorized users are not permitted to login. The authorized client can apply first tier security in text file using Vigenere cipher then Vigenere encrypted text file output will be given to second tier encryption i.e. Reverse circle cipher with symmetric key multi rotational technique as input. Finally output of reverse circle cipher with symmetric key multi rotational generate encrypted file that file upload into cloud. Fig.1. Shows the Outline of proposed hybrid cryptosystem. It provides processes for secure data storage and retrieval in cloud is as follows:

1. Registration Process.
2. Authentication Process.
3. First tier encryption. (Vigenere cipher)
4. Second tier encryption (Reverse circle cipher with symmetric key multi rotational technique).
5. Generated Encrypted & metadata file and Upload.
6. File Download and twice Decryption Process.

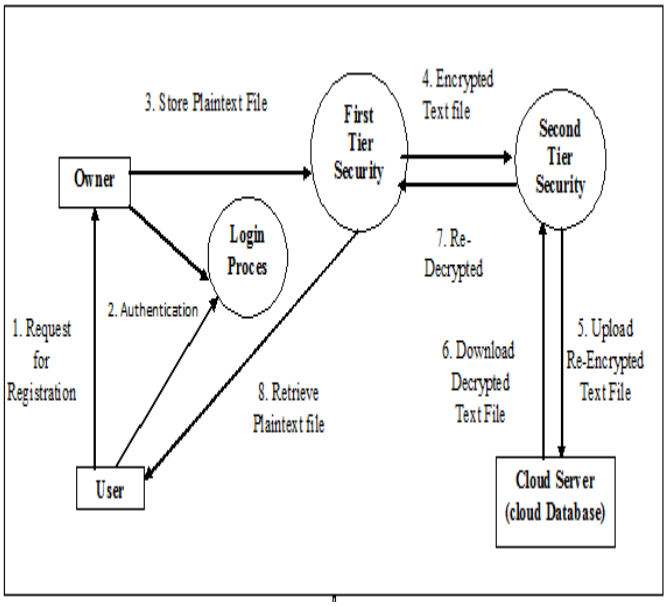

Fig.1. shows the outline of proposed hybrid cryptosystem.

III. System Architecture

Following Fig.2 shown System architecture. These architecture shown steps for system flow from plaintext to cipher text and vice versa.

IV. Two Tyre Security Approach

The Proposed system consists of two tier Security approach mainly works with the following security algorithms:

1. Vigenere cipher algorithm.
2. Reverse circle cipher algorithm with symmetric key multi rotational technique.

1. Vigenere Cipher Algorithm

Vigenere cipher is a simple poly alphabetic version of shift cipher, in which the cipher text is obtained by modular addition of a (repeating) key phrase and an open text (both of the same length).

In Vigenere cipher, generate Pseudo key using Pseudo key generation algorithm using input file.

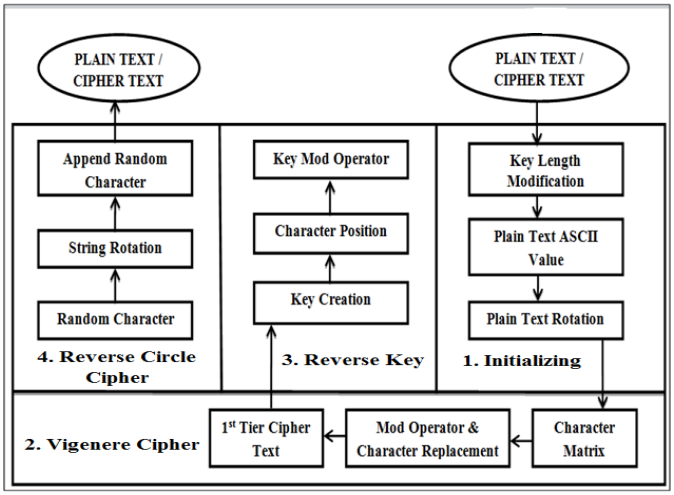

Fig. 2 System architecture

Pseudo key generation algorithm Equation:

$$f(x) = \sum_{i=0}^{i=n} Y_i \qquad (1)$$

$$\text{.....} \qquad (2)$$

$$Ps = P(f(x)) \qquad \text{.....}$$

Where,

1. $f(x)$ is function to read the content of file in string
2. Y_i is each word of file
3. Ps is Pseudo key
4. $P(f(x))$ is Random Function to calculate Pseudonym.

Steps of Vigenere cipher algorithm:

1. Take user Plain text/cipher text file.
2. Take user key length for plaint text.
3. Take ASCII value of each plain text character.

4. Plain text rotation for each rotation of Multi rotational technique.
5. Rotate multiple characters and arrange through character matrix.
6. Identify the character ASCII value.
7. Apply Mod operator and replace the character from result of MOD operator.
8. First tier cipher text of Vigenere cipher achieved.

2. Reverse Circle Cipher with Symmetric Key Multi Rotational Technique

The Reverse Circle Cipher algorithm uses a concept called circular substitution with reversal transposition. It is a symmetric poly alphabetic block cipher[18].To make reverse circle cipher we use confusion and diffusion principle by using ASCII (American standard code for information interchange) or UTF (Unicode transformation format) based on arithmetic coding for algorithm. We use circular substitution to reduce both time and space complexity to provide security for both personal and network security domains.

The complexity of algorithm is always based on size of encryption key. If the key is large, more complex is encryption program. In reverse circular cipher classical crypto technique is use whose algorithm weakness lies in the user selection key to run cryptanalysis using the weakness of reverse circular cipher algorithm is that after encryption if we change in cipher text which cause error in whole system and destroy data. This simple block cipher scheme reduces both time and space complexity. Brute-force attacker tries every possible key on cipher text till plain text is obtained.

A. Implementation of the reverse circle cipher

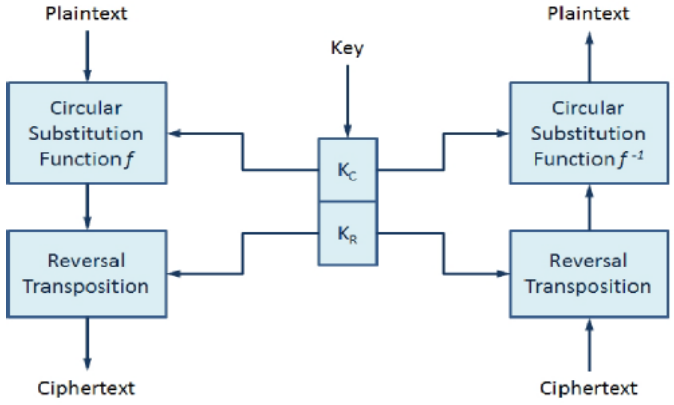

Fig. 3.System architecture of the Reverse Circle Cipher

The input circular character key is KC and reversal length integer key KR. During encryption, the circular substitution takes place with plaintext as circular key input. The output is reversal transposition with the reversal length of key. In decryption only difference is circular substitution function is arithmetic reverse of function used in encryption as shown in figure 2. Following are the equations used for cryptanalysis.

$C_i = f(P_{i,k}(0+\text{len}(k)\ i)$…….. (1)

$P_i = f^{-1}(C_{i,k}(0+\text{len}(k)\ i)$…….. (2)

Where,

+ len (k) is the modular addition

i= correspondence to position under operation.

Ci, Pi, (k)i correspondence to i^{th} binary digit of cipher text, plain text and key respectively and (+) is XOR operation.

B. Algorithm design

To achieve confusion principle, use of symmetric key multi rotational technique is used instead of linear rotation which produces further confusion using ASCII code characters shown in fig. 4.

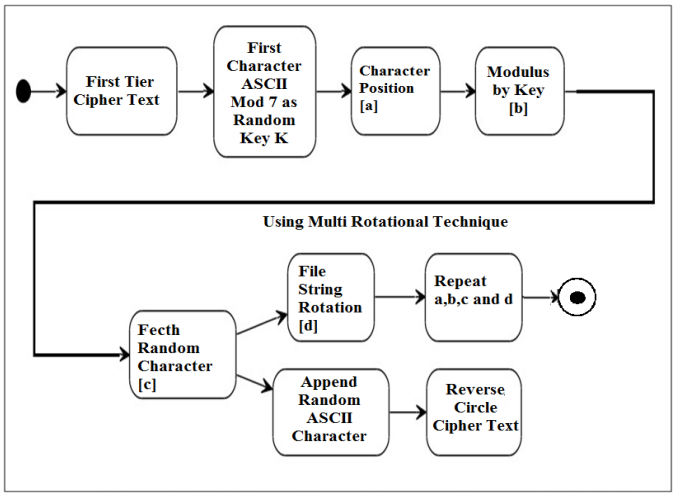

Fig. 4. Encryption using Multi rotational technique

Algorithm:

Reversal Circle Cipher with multi rotational substitution instead of linear substitution.

Where,

P: encrypted text buffer,

C: Cipher text buffer,

R: Reversal length hence buffer size.

Pi: Character at position i of encrypted text buffer,

Ci: Character at position i of cipher text buffer.

Ki: Character at position of i of the key.

+len(k): Modular addition with respect to key length taken as number of character.


```
Encryption:
1.  Start
2.  Clear all buffers;
3.  Open first tier vigenere cipher encrypted file as an input file;
4.  Open ciphertext output file;
5.  Obtain key.
6.  while ( !e of (encrypted text))
7.  {
8.  load p from encrypted text file;
9.  for( i=0;i<R; i++)
10. {
11. for (j=0; j<buffer_size;  j++)
      Multi rotational substitution
12. Ci = f (Pi,k(0+im(k)i) )
13. Reverse the content of C;
14. Append C to cipher text file;
15. Clear C & P
16. }
17. Close all files;
18. End

Decryption:
1.  Start
2.  Clear all buffers;
3.  Open first tier vigenere cipher encrypted file as an input file;
4.  Open ciphertext input file;
5.  Obtain key.
6.  while ( !e of (encrypted text))
7.  {
8.  load C from encrypted text file;
9.  for( i=0;i<R; i++)
10. {
11. for (j=0; j<buffer_size;  j++)
          Multi rotational substitution
12. Pi = f-1 (Pi,k(0+im(k)i) )
13. Reverse the content of C;
14. Append P to Plain text file;
15. Clear C & P
16. }
17. Close all files;
18. End
```

Fig. 5. Algorithm Encryption and Decryption

Mathematical equation:

$P_i = f^{-1} (c_{i,k} (0+len (k) i)$…….. (2)

From equation (2) we get equation (3)

$$\mathbf{R_{cp}} = \sum_{i=0}^{R} \sum_{j=0}^{B} Pi \quad \text{……} \quad (3)$$

Where,

R_{cp}= multi rotational cipher for plain text and cipher text.

R= reverse circle cipher.

B= buffer size.

V. EXPERIMENTAL RESULTS

Cloud computing characteristics

There are several key characteristics of a cloud computing environment. Service offerings are most often made available to specific consumers and small businesses that see the benefit of use because their capital expenditure is minimized. This serves to lower barriers to entry in the marketplace, since the infrastructure used to provide these offerings is owned by the cloud service provider and need not be purchased by the customer. Because users are not tied to a specific device (they need only the ability to access the Internet) and because the Internet allows for location independence, use of the cloud enables cloud computing service providers? customers to access cloud enabled systems regardless of where they may be located or what device they choose to use.

There is a level of agreement emerging around the essential characteristics of cloud computing, or the capabilities that must be adhered to an offering to be considered as a cloud It is designed for parallel computing. Client nodes are usually diskless, dumb terminals. Client nodes are connected to a server node through a network, such as Ethernet and Ethernet switches. It uses Parallel Virtual Machine (PVM) software, which enables multiple networked computers to appear as a single parallel processor. It uses open-source operating systems such as Linux or Solaris. It incorporates the Message Passing Interface (MPI) API specification, which enables multiple computers to communicate to form a cluster.

Fig .6 Sample Plaintext

o.VQK eEMDbPPp8 C7HNHeJEFPOak4Sx.8KE J98 K8OEasD C8R CQsJ46MEa0KLA7S Xx 4 6DHUM uGEHNTR5 8FOIa6FE8GTu k8JNBCN 6998KIWyK CFL CUHZ Q5a6T BGF4 HLG9RC1S6 ZD YR4J L9I ECUlaBKTG HDJ HSC.S 3aHOP4ZIKH ZJ0a IK5 ZJ4 I6T5LKH EK fKR G84FfKR Y.6Nc 6NUAJFW 8kU8DITLhW8 X XAaNE eP7y . X d8ea8I YZ Dbb8H GLJeN8HX eG RSLHd TF nullnullnullnull J8 FHFD8KK T7 Y.8J8 Y9GQ E4Q G6 NG64LJ5 QJ O.4Y 5GNA68 Y9GQ 6.GTIG LG MKJbnullH.IKM97 aK BT J 9LNJTB MG IA DUILAKASK 5K H MUP8qH IO 88TE6NA8 9PN DAN5DMA. CKFHVP8NCenullnullxU.ibI8a BFh 0O.LSFid NOPU6IONdnullFJYORSR8I HGPQbLJWK WP HHUJ4U BZ 4 XNFJML HFW4OMLD UWGFFZKTWdnullnullKDPCJ KF09SEU SM.PPPNK 6CIWUVKJG PV CQSEIJPCCZ8 HK MOTS 4 2HbSVKJZ

Fig 7 Cipher text Encrypted by Vigenere cipher

¢ÏÀ»µÁÏ¯·®]º¤£¢Á-¡²¸²Ï´¯°º¹ËÕÕ½«Ï¢µ¯Á´£¢Áµ¢¹¯Ë¦®Á-¢¼ Á-»¦´Õ×·¯ËÑµ¶«¡½ÁÂ«ÁÕÁ×®²¿·Á¨±¯²¸¾¼ÖÁÁ¢°¹³Ë×°¯¢± ¾¨ÁÕ¢´¸¬¸Á×££¢µ³Á¬µÁ-°¶Á-¿²ÄÁ»ÖË×¾Á¬±°ÕÁ²¶±£¼-Ò½×ÁÄ®ÁÃ¼Õ´Á¶£³Á¯-¿³Ë¬µ¾±Á²®´Á²½-Ï½ÁÔË²¹ºÕÄ³µ²Á Ä´ÑËÁ³µÖÁÄ´ÕÁ³×¾Ö¶µ²Á¯µÁÐµ¼Á±¢Õ°Ðµ¼ÁÃÏ×¸ÍÁ×¸¿ «´°ÁÁ¢Õ¿¢®³¾¶ÒÁ¢ÁÁÂÂÂ«Ë¸¯ÁÏº¡¬ÁÁÏÁÂÂÍĉÏË¢³ÁÃÄÁ® ÌÌ¢²Á±¶´Ï¸¢²ÂÁÏ±Á¼½¶²ÎÁ¾°Á¡¨ÖÖ¡¨ÖÖ¡¨ÖÖ¡¨ÖÖÁ´¢Á°²° ®¢µµÁ¾¡ÁÃÏ¢´¢ÁÃ£±»Á¯Õ»Á±×Á¸±×Õ¶´ÖÁ»´Á¨ÏÕÃÄÖ±¸« ×¢ÁÃ£±»Á×Ï±¾³±Á¶±Á·µ´Ì¡¨ÖÖ²Ï³µ·£¡ÁËµÁ¬¾Á´Á£¶¸´¾¬ Á·±Á³«Á®¿³¶«µ«½µÁÁÖµÁ²ÁÁ·¿º¢¤²Á³¹Á¢¢¾¯×¸«¢Á£º¸Á ®«¸Ö®·«ÏÁ-µ°²À º¢¸-Ïį¨ÖÖ¡¨ÖÖ«¿ÏÓÌ³¢ËÁ¬°ÒÁÑ¨Ï¶½°ÓÎÁ¸¹º ¿×Ö¹¸Îį¨ÖÖ°´Ã¹¼½¼¢³Á²±º»¶´ÁµÁÁºÁ²²¿´Õ¿Á¬ÄÁÕÁÂ¸°´· ¶Á²°ÁÕ¹·¶®Á¿Á±°°Äµ¾ÁÎį¨ÖÖ¡¨ÖÖµ®º-´Áµ°Ñ£½¯¿Á½·Ïº º¸µÁ×-³Á¿Àµ´±ÁºÀÁ-»½¯³´º--Ä¢Á²µÁ·¹¾½ÁÕÁÓ²Ì½Àµ´Ä

Fig. 8. Cipher text Encrypted by the Reverse Circle Cipher symmetric key multi rotational technique

VI. CONCLUSION

In Recent times, cloud computing facing many security challenges. Users most worry about data security, so data security is the main problem of the cloud computing security. In this paper proposed secure communication in Cloud using Hybrid Cryptosystem to provide confidentiality and authentication of data. The main aim is to securely store and manage the text based files using Vigenere cipher and the reverse circle cipher with symmetric key multi rotational technique so that only authorized users can have access stored files. The main advantage of this system is every time unique key is generated. This proposed system ensures strong authentication is implemented in performance with encrypted transmission. When the size of text file is increased then its computation time is increased, but we proposed one can decrease computation time by using appropriate approach and only space required for the plaintext and cipher text buffers, there is no additional space required for the computational part of the algorithm.

Acknowledgement

It gives me immense pleasure to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed guide Prof.Rahul L. Paikrao,(HOD) & Asst. Professor, Computer Dept.,AVCOE, Sangamner for their valuable guidance, encouragement and help for completing this work. Their useful suggestions for this whole work and co-operative behavior are sincerely acknowledged. Finally, I am highly obliged to all my family members for their support and blessings.

References

1. Jing-Jang Hwang and Hung-Kai Chuang, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", National Science Council of Taiwan Government (Project Number NSC 99-2410-H-182 -025 -MY2, 2011.
2. D.Kesavaraja, R.Balasubramanian and D.Sasireka, "Implementation of a cloud data server for providing secure service in E-Business", International Journal of database Management System (IJDMS),Vol 2,No.2,May 2010.
3. S. Subashinin, V.Kavitha, "A survey on security issues in service delivery models of cloud computing",, Journal of Network and Computer Applications 34(2011)pages 1-11.
4. Anurag Porwal, Rohit Maheshwari, B.L.Pal, Gaurav Kakhani, ``An Approach for Secure Data Transmission in Private Cloud", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
5. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,"Ensuring Data Storage Security in Cloud Computing",proceeding of International workshop on Quality of service 2009aĂİ, pp.1-9.
6. Lombardi F, Di Pietro R., "Secure virtualization for cloud computing",Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.
7. Kresimir Popovic , Zeljko Hocenski "Cloud computing security issues and challenges", in the Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
8. Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307, Volume-2, Issue-3, July 2012.
9. Amanjot Kaur, Manisha Bhardwaj, "Hybrid Encryption For Cloud Database Security", International journal of engineering science advanced technology ISSN: 2250aĂŞ3676 Volume-2, Issue-3, 737, 741,May-Jun 2012
10. Wang, Ayesha Malik, Muhammad Mohsin Nazir ,"Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, VOL. 3, NO. 3, March 2012
11. Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.
12. John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation,Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807,pp. 147-158, 183-212.
13. Ramgovind S, Elo MM, Smith E, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10/2010 IEEE.
14. B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues",in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.
15. Mohamed Al Morsy, John Grundy and Ingo Muller, "An Analysis of The Cloud Computing Security Problem", in Proceedings of APSEC 2010 Cloud Workshop,Sydney,Australia,30th Nov 2010.
16. Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma , "Towards Analyzing Data Security Risks in Cloud Computing Environments", ICISTM 2010, CCIS 54, pp. 255-265, 2010.
17. Danish Jamil,Hassan Zaki, "Security Issues In Cloud Computing And Countermeasures", International Journal of Engineering Science and Technology (IJEST),ISSN : 0975-5462 Vol. 3 No. 4 April 2011.
18. Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, "Reverse Circle Cipher for Personal and Network Security".

AUTHOR(S) PROFILE

Sarika Kadlag received the B.E. degree in Computer Engineering from Amrutvahini College of Engineering, Pune University, Sangamner (MS),India in the year 2007. Presently She is a working as a Lecturer in Amrutvahini Polytechnic, Sangamner. She is currently a M.E. scholar in the Department of Computer Engg. at AVCOE, Pune University, Sangamner. Her current research interests include cloud computing and its security.

