Investigation of Efficient Cryptic Algorithm for Cloud Storage

Ashok Sharma*, Dr R S Thakur** and Dr Shaliesh Jaloree***
* Research Scholar
myofficialid@yahoo.com
** Associate Professor Manit Bhopal
drrsthakur2016@gmail.com
*** Associate Professor,Sati Vidisha
sjaloree@gmail.com

Abstract: The unmatchable progress in Information Technology based Products have encouraged the customers to use free unlimited and ever available cloud storages. The Cloud Storages save hardware investment of customers for storage. Rapid Data migration into cloud storages had been expected by IT industry with all of these developments. However, the growth of data migration has not adopted the pace as expected because of Data security and Speed of cryptographic algorithm's issues in cloud.

In this paper, we are discussing mainly two mostly used Cryptographic algorithms AES and 3DES and in later section we are also comparing AES, 3DES with RC6, Twofish and Blowfish and we are analyzing the performance of these algorithms in terms of encryption and decryption time taken depending upon the four factors namely file type, file size, key type and key size.

For performance analysis, we are introducing in-house developed Crypter tools where we have integrated five cryptographic algorithms 3DES, AES, RC6, Twofish and Blowfish.The Crypter tool is deployed in Amazon Cloud and Tool is capable to encrypt and decrypt different types of files (in terms of size and format) depending upon variable or fixed type of key using AES, 3DES, RC6, Twofish and Blowfish and The performance of these Cryptographic algorithms 3DES, AES, RC6, Twofish and Blowfish can be analyzed in terms of time taken depending upon different types of files and different types of Keys. Analysis of the result obtained will help the user's to take decision regarding the selection of best symmetric algorithm to be used while uploading data in cloud.

Keywords: Cloud Computing, Cryptography, Encryption, Decryption, AES.

Introduction

Moore's law inferences demonstrates the drastic changes in the field of computing form early days and indicates that things have changed totally. The rise in the demand of computing and other resources have given the birth to distributed computing and Cloud computing. Among them, Cloud Computing is the latest computing paradigm where large pool of dynamical scalable and virtual Resources are integrated to offer various services on demand and pay per use model. This paradigm has totally changed the way of doing the things on rental basis and contributing towards various types of services like elastic resources include computing power, platform, infrastructure etc. The feature of cloud supports various users for personal and commercial purpose and keeping data in cloud in open format is good as same can be easily accessible by all authorized users but form security point of view it is not safe and advisable. The paper investigates efficient, secure and low cost cryptic algorithm to secure user's information.

This paper has been organized in Five Sections and in Section I, the Foundation of cloud computing together with traditional Encryption/Decryption algorithms 3DES, AES, RC6, Twofish and Blowfish used for securing data in cloud has been presented first. In Section II, need of Cryptography for cloud has been presented and the investigation process to explore efficient cryptographic algorithm has been presented in Section III, where comparison of AES and 3DES with essential features have been discussed .In Section IV, The Crypter tool and its feature has been introduced. This crypter tool has been developed for comparison of encryption and decryption time taken by cryptographic algorithms 3DES, AES, RC6, Twofish and Blowfish depending upon types of files, sizes of files, key types and key sizes and finally in Section V, the result of efficiency comparison with various file type and key size have been presented together with future scope.

Related work

The birth of cloud computing has drastically changed the everyone's perception of infrastructure. Architectures, software delivery and development models. Cloud computing is treated as innovative deployment architecture following the transition from grid computing, utility computing and autonomic computing. This rapid adoption of cloud computing has fuelled concerns on a major issue for the success of information systems and information security [1].

Since data owner has no control on data location in cloud computing and it is the cloud service provider's responsibility to manage and administer to update, delete and access the database. Since data is placed in plaintext and during any operations on data stored in cloud, there are chances of Tampering with data and compromising with the data security due to untrustworthiness of service provider.Security of outsourced data is a great challenge.The major requirement for achieving security in outsourced databases are confidentiality, privacy, integrity, availability[2].

Cryptography is first step towards the security of the sensitive information of data owners in cloud storage.Issac has introduced the cryptography in cloud which led to rapid adoption of cloud computing. Although secure storage has already captured the attention of many cloud providers.

The Cloud computing has enormous advantages, besides these advantages, adoption of cloud services has still not gained such popularity which was expected. Among various security and legal risks, some risks are very alarming which includes: i) unauthorized access, ii) sensitive data disclosure, iii) data integrity. Cloud data security is the most worrying issue of cloud Technology and before migrating the data to cloud vendors, security must be improved to acceptable levels.

In this regard definitely, Cryptography could help increasing adoption of Cloud. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography no doubt secures the data from unauthorized access but outsourcing of encrypted data is possible only by revealing parameters of key. For enjoying full potential of Cloud Computing, we must provide secure storage and secure processing or computation. Efforts have been made to make possible search on encrypted data, which allows companies to store confidential information in the cloud whilst still being able to access it partially without having to decrypt it [3] but it is contradictory to provide provision of searching encrypted data stored in cloud.

Cryptic Algorithms and Analysis Strategies.

Triple DES:NIST-USA,had introduced the Data Encryption standard (DES) in 1977. DES was the most widely used Encryption and Decryption scheme till the introduction of Advanced Encryption Standard (AES) in 2001.in DES, data is encrypted in 64-bit blocks using 56-bit key transformed from 64-bit key. In DES, 64-bit plaintext passes through an initial permutation (IP) which arranges the bits for producing permuted input following 16 rounds involving substitution and permutation functions.The output of 16th round consist of 64 bits, which is function of the input plain text, and key, left, and right halves of the output is swapped to produce the pre output. Finally, the pre output is passed through permutation, which is inverse of the initial permutation to produce output of 64-bit cipher text.

In case of Triple-DES, instead of one key, two keys have been used, the first key is used to convert a plaintext message into cipher text and the second key is used to decrypt the encrypted message. Since second key is different from first one, so output is not the plaintext. Therefore, the twice-scrambled message is then encrypted again with the first key to yield the final cipher text. This three-step procedure is called triple-DES.Triple-DES is just DES done three times with two keys used in a particular order [4, 5, 6]

AES:NIST has announced that AES will be successor to the aging Data Encryption Standard (DES) which was vulnerable to brute-force attacks.AES consist of three block ciphers, AES-128, AES-192 and AES-256.Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. Symmetric Algorithms uses the same key for encryption and decryption, so both the sender and the receiver must use the same secret key. Depending upon the key length number of rounds differs [6,7,8]. In [9], a tool designed for comparison of performance of DES, 3DES, BlowFish and Two Fish Cryptosystem using SGcrypter has been presented. The performance has been compared with variable input text size and key size. However, no analysis has been done on other file formats and popular algorithm that is currently being used in cloud. In [10], the theoretical background of symmetric algorithm and its scope for Time variant perspective has been discussed. The paper presents one schemes based on Fibonacci-Q matrix.In [11], the trend of increasing key size has been supported by Automatic variable key with Optimal Key Size. In [12], Various Approaches towards Crypt-analysis have been suggested for testing strength of symmetric cryptosystem. In [13], the specialized class of algorithms for analysis of cipher text Cryptic Mining algorithm in case of Automatic Variable Key Based Cryptosystem has been presented. In [14, 16], Variable key for shorter size has been realization with Fibo-Q based Symmetric Cryptosystem. In [15],the auditing of symmetric key based cryptosystem has been analyzed by Association rule on Parameterized Automatic Variable Key based Symmetric Cryptosystem. In [17], Another strategy of symmetric key based cryptosystem using location based information on Sparse approach is suggested .The conversion of cipher text based on some knowledge of plaintext and pattern in the cipher text, cryptanalysis process has been presented [18]in Light of Artificial Intelligence.

For Cloud, platform AES algorithm has been used with parameters mentioned in Table1.The comparison of AES with state of art 3DES has been presented in Table 2.

Table 1: Iterations taken by conventional AES

Key Length	128 bit Keys	192 bit Keys	256 bit Keys
Number of Rounds	10	12	14

Literature surveys shows biclique attack could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. Even this attack, though, does not threaten the practical use of AES due to its high computational complexity.

Table 2: Comparison of 3DES and AES

Parameters	**Algorithms**	
	3DES	AES
Max Key Length	168	256
Max Rounds	48	14
Block Size in bits	64	256
Security Level	Adequate	Excellent
Encryption /Decryption Speed	Very slow	Fast
Cipher Type	Symmetric Block	Symmetric Block
Key Sizes	2168	2256
Key Switching	No Need of Switching	Need Switching After every 32GB transfer

Experimental Setup

The investigation process has been accomplished by designing a Crypter tool with integrated five Symmetric algorithms 3DES, AES, Blowfish, Twofish and RC5 .To support analysis task the Tools automatically detects the configuration of the system on which it is deployed along with the internet speed .various files of different types and different sizes has been given as input to each algorithm to analyse their encryption and decryption speed with variable keys. The experimenter can upload necessary information in the crypto tool in Amazon cloud and in cloud environment; we have to examine the speed of various algorithms by giving different files as input. The Tool is deployed on Amazon server and in first Step user must select any of the four operation mentioned i.e,Encryption with Varying File Size, Decryption with Varying File Size, Encryption with Varying Key Size and Decryption with Varying Key Size.

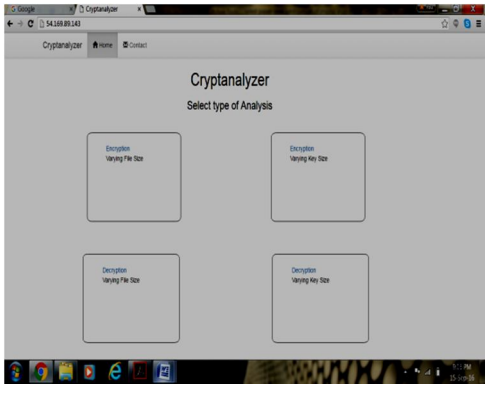

Fig.1. Home Screen of Crypto Tool

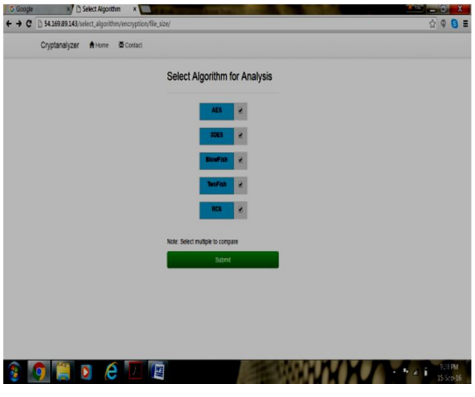

Fig.2. Choice of algorithm for comparison

In 2nd step user must select the algorithms to be compared on any of the four operations.
In Step 3, user needs to select four different types of files of nearly same sizes and key which is to be used

Step 4 gives the result in terms of encryption and decryption speed depending on the size of file and algorithm selected for comparison.

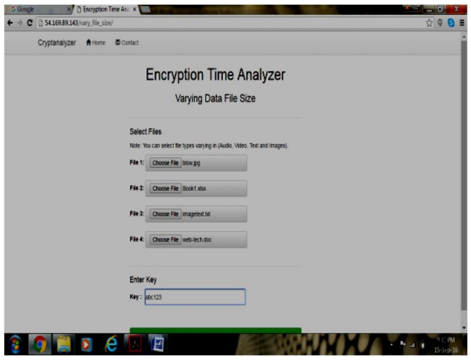

Fig.3. types of files for Encryption Time Analyzer

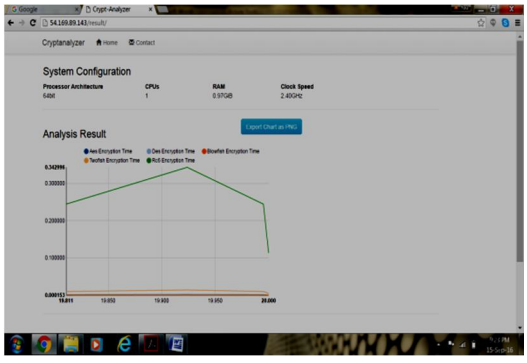

Fig. 4. Plot of performance of Encryption time

Table 3: Encryption time (ms)of Algorithms taken for different file types with varying key sizes

File Name	Key File Size	3DES	blowfish	RC6	AES	Twofish
Image.Txt	0.008KB	0.000952	0.000218	0.112695	0.000165	0.004908
Book1.xlxs	0.009KB	0.000956	0.00021	0.113412	0.000161	0.004928
Blow.jpg	0.010KB	0.000951	0.000215	0.113759	0.000155	0.004982
webtech.doc	0.011KB	0.000968	0.000207	0.112525	0.000154	0.004863

Results and Discussion

We have carried a simulation of uploading four different files of Text, Image, Doc and Word document of nearly same sizes and have used AES and 3DES algorithm for encryption and decryption process using same key and the result produced is as under: In order to evaluate and analyse the performance we have used four files of Text, Image, Pdf and Word documents of same size and then we have analyse the encryption and decryption speed using AES and 3 DES algorithms as mentioned in the Table 2.

Encryption Time: In Table 3, the performance of Symmetric algorithm with respective file variants and corresponding encryption time in seconds has been presented.

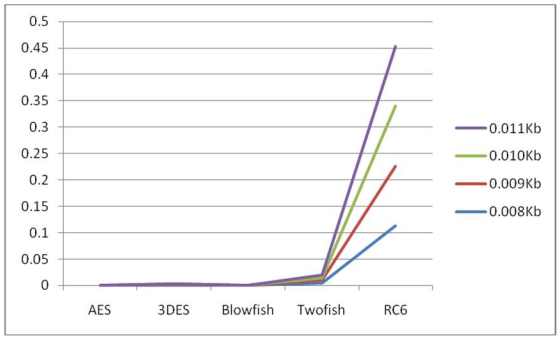

Fig 5.Encryption Time taken by different algorithm for varying key sizes

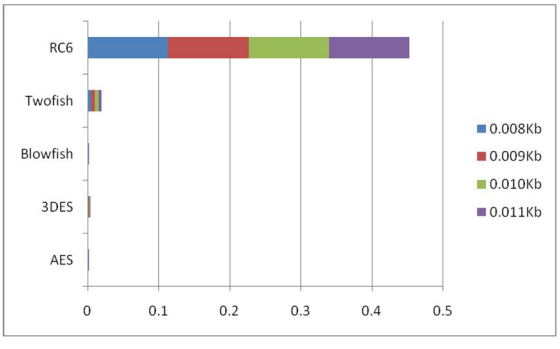

Fig 6. Encryption Time taken by different algorithm for varying key sizes

Table 4: Encryption Time (ms) of Algorithms taken for different file types with fixed key size

AES	3DES	Blowfish	Twofish	RC6
0.000310	0.001969	0.000447	0.010155	0.237101
0.000443	0.002752	0.000620	0.014411	0.331727
0.000325	0.002027	0.000454	0.010397	0.237218
0.000171	0.000903	0.000221	0.004935	0.113279

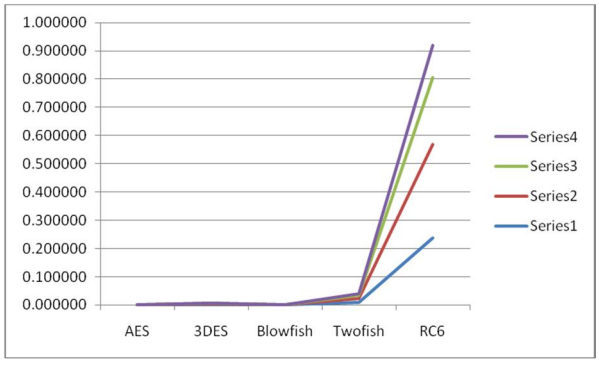

Fig 7 Encryption Time taken by different algorithm with same key

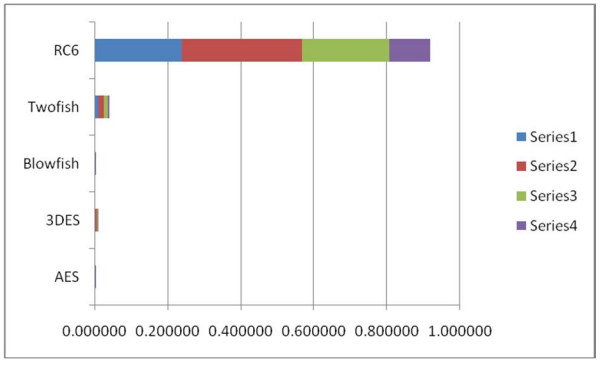

Fig 8 Encryption Time taken by different algorithm with same key

Decryption Time: In Table 5, the performance of Symmetric algorithm with respective file variants and corresponding decryption time in seconds has been presented.

Table 5: Decryption Time (ms) of Algorithms taken for different file types with varying key size

File Name	Key File Size	3DES	blowfish	RC6	AES	Two fish
Image.Txt	0.008KB	0.000968	0.000213	0.107916	0.000168	0.004787
Book1.xlxs	0.009KB	0.000971	0.000216	0.107813	0.000164	0.004746
Blow.jpg	0.010KB	0.000947	0.000203	0.106526	0.000165	0.004599
webtech.doc	0.011KB	0.000952	0.000205	0.107463	0.000158	0.004736

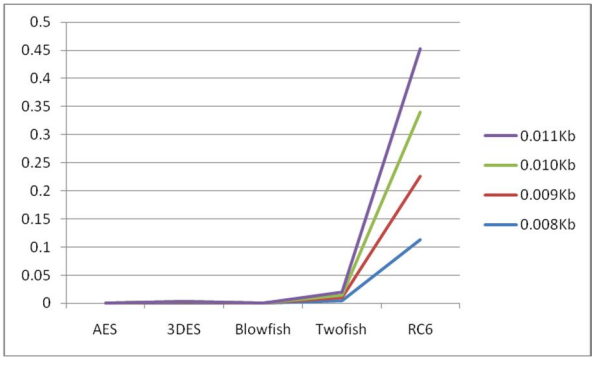

Fig 9 indicating Decryption Time taken by different algorithm for varying key sizes

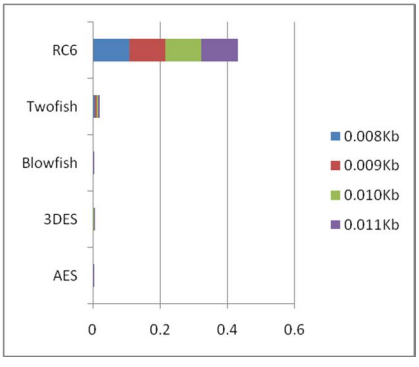

Fig 10 indicating Decryption Time taken by different algorithm for varying key sizes

Table 6: Decryption time of algorithms taken for different file types with same size

AES	3DES	Blowfish	Twofish	RC6
0.000308	0.001997	0.000430	0.009832	0.226394
0.000435	0.002744	0.000586	0.013539	0.316460
0.000322	0.002031	0.000436	0.009910	0.228233
0.000158	0.000944	0.000212	0.004747	0.106504

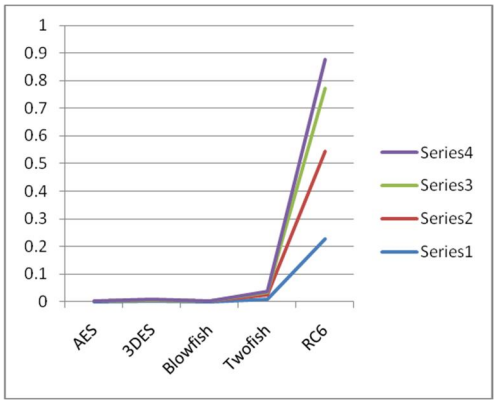

Fig 11 indicating Decryption Time taken by different algorithm for same size of key

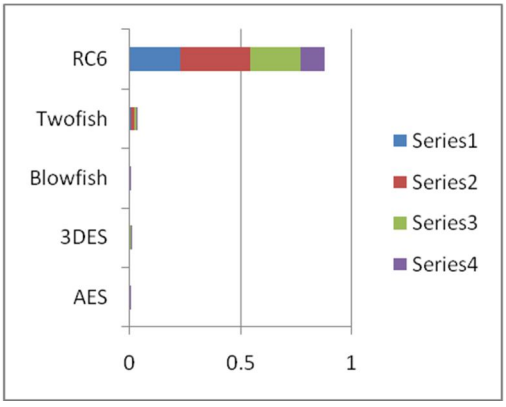

Fig 12 indicating Decryption Time taken by different algorithm for same size of key

Conclusions And Future Directions

1. Fig 5 and Fig 6 indicates that AES Encryption algorithm takes very less time in Encrypting and uploading files of different format files in cloud environment among document type Text, Image,excel and txt file of 20 KB Sizes. Therefore, for encryption process AES algorithm must be preferred for uploading different files in case of varying key sizes and it has been seen that AES takes less time in encryption of Text file and more time in xlxs format among selected.
2. Fig 7and Fig 8 indicates that AES Encryption algorithm takes very less time in Encrypting and uploading files of different format with fixed key size in cloud environment among Text, Image, excel and txt file of 20 KB Sizes. Therefore, for encryption process AES algorithm must be preferred for uploading different files in case of fixed key size and it has been seen that AES takes less time in encryption of Text file and more time in xlxs format among selected.
3. Fig 9 and Fig 10 indicates that AES Decryption algorithm takes very less time in Decrypting and uploading files of different format with varying key sizes in cloud environment among Text, Image, excel and txt file of 20 KB Sizes. Therefore, for Decryption process, AES algorithm must be preferred for uploading different files in case of varying key sizes and it has been seen that with the increase in key size, decryption time reduces. Therefore, for better security of files, increase in key size does not increase decryption time.
4. Fig 11 and Fig 12 indicates that AES Decryption algorithm takes very less time in Decrypting and uploading files of different format with fixed size key in cloud environment among Text, Image, excel and txt file of 20 KB Sizes. Therefore, for Decryption process, AES algorithm must be preferred for uploading different files in case of fixed key
5. It has been seen that AES algorithm is very good in both for encryption and decryption process with variable or fixed key and among different format selected for simulation, in text file it takes lesser time and in excel file it takes much time. Since in AES-Symmetric crypto algorithm C=Confusion and D=Diffusion is achieved by row and column mixing. The N=Nonlinearity is achieved by S-Box, without which AES based cryptosystem is prone to linear attack. Thus, nonlinear operation with key mixing enhances confusion and diffusion [19]. We have to examine the structure of AES and investigate the equivalent low cost operations for nonlinear transformation, key mixing and reduction in time consumed during rounds without compromising in the quality of cryptosystem.

References

[1] Dimitrios Zissis, Dimitrios Lekkas Addressing cloud computing security issues Future Generation Computer Systems28, pp.583–592, 2012.
[2] Mayuri R. Gawande Analysis of Data Confidentiality Techniques in Cloud Computing IJCSMC, Vol. 3, Issue. 3, March 2014, pg.169 – 175, 2014.
[3] Isaac Agudo Cryptography goes to the Cloud part of the ICT PASSIVE project (http://ict-passive.eu/).
[4] Carl H. Meyer and Stephen M. Matyas, Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, New York, 1982.
[5] Dorthy Elizabeth Robling Denning, Cryptography and Data Security, Addison-Wesley Publishing Company, Reading, Massachusetts, 1982.
[6] D.W. Davies and W.L. Price, Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, Second Edition, John Wiley & Sons, New York, 1984, 1989.
[7] Noura Aleisa, A Comparison of the 3DES and AES Encryption Standards International Journal of Security and Its Applications Vol.9, No.7, pp.241-246, 2015

[8] Hamdan.O.Alanazi et.al, New Comparative Study between DES, 3DES and AES within Nine Factors Journal of computing,vol. 2, issue.3,ISSN 2151-9617,2010.
[9] Shaligram Prajapat, Gaurav Parmar ,R.S.Thakur, "Towards investigation of efficient Cryptosystem using Sgcrypter",In Special Issue of International Journal of Applied Engineering and Research (IJAER), Vol. 10 (79), pp. 853-858, 2015.
[10] Prajapat, Shaligram, D. Rajput, Ramjeevan Singh Thakur, "Time variant approach towards symmetric key", In proceedings of IEEE Science and Information Conference (SAI), London 2013. , pp.398-405, 2013.
[11] Prajapat, Shaligram, Ramjeevan Singh Thakur. "Optimal Key Size of the AVK for Symmetric Key Encryption."in Covenant Journal of Information & Communication Technology, Vol.3(2), pp. 71-81. 2015.
[12] Prajapat, Shaligram, Ramjeevan Singh Thakur. "Various Approaches towards Crypt-analysis." International Journal of Computer Applications, Vol. 127(14), pp. 15-24, 2015. (doi: 10.5120/ijca2015906518)
[13] Prajapat, Shaligram, Ramjeevan Singh Thakur. “Cryptic Mining for Automatic Variable Key Based Cryptosystem”,Elsevier procedia Computer Science, Vol. 78 (78C), pp. 199-209, 2016. (doi: doi:10.1016/j.procs.2016.02.034) .
[14] Prajapat, Shaligram, Ramjeevan Singh Thakur. "Realization of information exchange with Fibo-Q based Symmetric Cryptosystem." International Journal of Computer Science and Information Security, Vol 14(2), pp. 216-223, 2016.
[15] Prajapat, Shaligram, Ramjeevan Singh Thakur."Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem."International Journal of Computer Science and Information Security, Vol. 14 (2), pp. 233- 246, 2016.
[16] Prajapat, Shaligram, Jain A. Ramjeevan Singh Thakur, “A Novel Approach For Information Security with Automatic Variable Key Using Fibonacci Q-Matrix”, IJCCT, ISSN: 2231 – 0371, 0975 – 7449 Vol-3(3), 2012, p.p. No. 54-57, 2012.
[17] Prajapat, Shaligram, Sharma A., Swami S., Rajput D., Singroli B., R. S. Thakur. "Sparse approach for realizing AVK for Symmetric Key Encryption", International Journal of Recent Development in Engineering and Technology (IJRDET) Vol. 2(4), pp.15-18, 2014.
[18] Prajapat, Shaligram, Thakur, A., Maheshwari, K., & Thakur, R. S., “Cryptic Mining in Light of Artificial Intelligence”, IJACSA , Volume 6(8), pp. 62-69, 201510.14569/IJACSA.2015.060808) .
[19] Ajlouni N. A. El-Sheikh and A.Abdali Rashed, New Approach in Key Generation and Expansion in Rijndael Algorithm, International Arab Journal of Information Technology, vol. 3, no. 1, January 2006, www.IAJIT.org.