



(Print)

JCIT Vol. 9(3), 33-39 (2018). Periodicity-2-Monthly

(Online)



**JOURNAL OF COMPUTER & INFORMATION TECHNOLOGY**  
An International Open Free Access Peer Reviewed Research Journal of Computer  
Science Engineering & Information Technology  
website:- [www.compitjournal.org](http://www.compitjournal.org)

## Encryption and Obfuscation :Confidentiality Technique For Enhancing Data Security in Public Cloud Storage

SAMARJEET YADAV<sup>1</sup> and VIJAY TIWARI<sup>2</sup>

<sup>1,2</sup> Centre For Advanced Studies

Dr. A.P.J. Abdul Kalam Technical University (AKTU) Lucknow Uttar Pradesh (India)

Corresponding Author Email: [17mcs11@gmail.com](mailto:17mcs11@gmail.com)<sup>1</sup> [vktiwari@gmail.com](mailto:vktiwari@gmail.com)<sup>2</sup>

<http://dx.doi.org/10.22147/jucit/090301>

Acceptance Date 20th May 2018,

Online Publication Date 2nd June, 2018

### Abstract

Modern technologies witness lot more developments. Cloud Computing (CC) is one of the rapid developments. The demands, the importance and the usage of CC is on the increase every day. As the importance is on the increase, so is the security problems and its threats. The problems have caused great influences on the development and popularization of cloud computing. The data storage has become an indispensable part in cloud computing. The data could be either numeric or non-numeric. The data to be stored need to be protected with confidentiality measures. The data must be encrypted before deposited into cloud database. The cryptographic techniques play a vital role in enhancing the security. This paper proposes a technique to store the data of numeric and non-numeric type by obfuscation and encryption methods. This paper also proposes the technique to enhance security level. The paper produces minimum time data size and service while uploading into the cloud storage.

**Key words:** Cloud Storage, Obfuscation, Encryption, Cryptography, Confidentiality.

### 1. Introduction

The problems in Cloud Computing (CC) influence greatly on the development and popularization of CC. Hence security and performance in CC with CSPs need to be more efficient. The Data Storage (DS) has become an indispensable aspect in CC. Either numeric or non-numeric, the confidentiality of data must be protected by encryption before deposited into Cloud Storage (CS). Encryption is to make data unintelligible against unauthorised access and to make extremely difficult to decipher when attacked. It provides strong security for data to extend sensitive data the highest level of security.

Cloud computing proposes new model for computing and its related issues like compute, storage, software. Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivations and purposes to move over to the cloud. If cloud users are academia, the security and performance of computing and the cloud service providers (CSPs) need to be efficient. Most of the enterprises possess lot of data and they look for a storage space in cloud environment to secure the data. Hence, security plays a vital role in protecting those sensitive data. There are many CSPs who provide the security of data of the users. In the process of providing security for data, the CSPs develop a tendency to tamper

or misuse the sensitive data without the prior knowledge of the users. So, the users are forced to hide the originality of their data before storing into cloud storage. There are many traditional existing cryptographic techniques which help the users to encrypt the data before storing into cloud storage. Every day the demand for these cryptographic techniques increases tremendously. The goal of encryption is to make data unintelligible to unauthorised users and extremely difficult to decipher when attacked. Encryption can provide strong security for data to give sensitive data the highest level of security<sup>1</sup>.

The paper proposes a technique to encrypt the data before stored into cloud. The data could be numeric and alphanumeric and alphabetic. In order to protect the security of data, they must be encrypted. This paper proposes encryption technique to encrypt the non numerical data and obfuscation technique to obfuscate the numerical data. By applying these techniques separately, service cost for processing will take more. Hence the proposed technique combines both the encryption and obfuscation methods to encrypt the data before uploading into cloud. Thus providing the methods, the confidentiality is maintained and the security of data is enhanced. This technique takes minimum time for process and consumes minimum data size. The desired results prove to be satisfactory by applying this technique. The organisation of this paper is as follows: Section II enumerates the related works relevant to this paper. Section III provides the proposed confidentiality technique of encryption and obfuscation. The section also includes the sample data with expected results of confidentiality, thus enhancing security. Section IV concludes the paper.

## II. Related work :

Atiq U.R. Rehman *et al.*<sup>2</sup> proposed a framework to store sensitive data with a combination of encryption and obfuscation. The cloud users maintained data storage to store keys that are used for encryption. This paper further proposed mechanism to query over encrypted and obfuscated data on server side. Once the required data are filtered on server side, then data are transferred on user's side where de-obfuscation and decryption are performed. . The authors<sup>3</sup> presented three approaches such as separating software and infrastructure service providers, hiding data owner's information in cloud and, data obfuscation technique for security. The approach was further presented by Manpreet Kaur *et al.*<sup>4</sup> with two-step encryption process which is used to completely protect the encrypted sensitive

data from users to cloud and cloud to users. Yu *et al.*<sup>5</sup> proposed one of the works, which combined ABE, Proxy Re-encryption and lazy encryption schemes for Cloud and security. The scheme works by data owner encrypting his data using a symmetric key and then encrypting the symmetric key using a set of attributes according to KP-ABE scheme. The data owner determines minimum number of attributes to the new user to access and to update the data with the corresponding secret key. The secret keys of the remaining users will also be updated. Because of heavy burden of the data owner which may require him to be online at all times to provide key updates, proxy re-encryption is introduced to allow the cloud to carry out these tasks. The data owner's data are kept secure and confidential at all times as the cloud is only exposed to the ciphertext and not the original data contents.

They proposed<sup>6</sup> a security policy and procedures to increase data storage security in cloud. They had a Control Access Data Storage (CADS) to include the necessary policies, processes and control activities for the delivery of each of the data service offerings. To maintain an environment which supports the effectiveness of specific controls and the control frameworks, they used collective control data storage includes the users, processes, and technology. This effectiveness is guaranteed by providing the security policy and procedures for data storage, defence in depth for the data storage, correctness verification and error localization computing. These recommendations are only theoretically proposed.

Cunsolo *et al.*<sup>7</sup> proposed a mechanism to protect the data in distributed systems (grid, cloud, autonomic, etc.). This technique consists of the use of combination of symmetric and asymmetric cryptographic algorithms. In this scheme, only data owner can access the data which contradicts the concept of sharing resources in cloud environment. S. Hadi *et al.*<sup>8</sup> proposed a new related-key impossible differential attack on 7-round AES-128. They attacked 7round AES-128 with the time complexity of (105), the fastest attack of all the previous ones from time and pre-computation complexities points of views. A fundamental point to construct such attack is to use a special property of mix column operation of AES.

Kazys *et al.*<sup>9</sup> who presented a new version of AES by generating random S-Boxes coinciding with every secret key generation. He described in details that how to generate random S-Box, key-independent, and ratio of independence. The breach of this study was not debating any type of cryptanalysis attacks. However, contrast to the above studies, the first cryptanalysis was deployed by

Alex B. *et al.* and Bernstein *et al.*<sup>10,11</sup>. Alex and Bernstein evaluated the cost of cryptanalytic attacks on the full AES by using special-purpose hardware in the form of multicore AES processors. Also, Alex and Bernstein also analysed different time cost trade-offs and evaluated the implications of progress in VLSI technology under the assumption that Moore's law will continue to hold for the next ten years. These calculations raised some concerns about the long-term security of the AES.

Zhao *et al.*<sup>12</sup> suggested a progressive elliptic curve encryption scheme (PECE) where a piece of data is encrypted a number of times using multiple keys and later decrypted using one key. It is an effective technique, as it keeps the data confidential as data are encrypted through the entire stages thus never allowing a malicious user to view the plaintext data. The main problem however with this technique is that it requires the data owner to be online at all times and hence makes it inefficient for everyday users. Attribute-Based Encryption (ABE) is an effective and promising technique that is used to provide fine-grained access control to data in cloud. Initially, access to data in the cloud was provided through Access Control Lists (ACLs). However, this was not scalable and only provided coarse-grained access to data<sup>13</sup>. This ABE was first proposed by Goyal *et al.*<sup>14</sup> to provide a more scalable and fine-grained access control to data in comparison to ACLs.

Tran *et al.*<sup>15</sup> used the idea of proxy re-encryption scheme where the data owner's private key is divided into two parts. The first half is stored in the data owner's machine while the other is stored in the cloud proxy. The data owner encrypts the data with half of his private key, which then gets encrypted again by the proxy using his other half of the key. Other user who has been granted access rights will then have the same key divided with different parts. One half will be kept on the granted user's machine and the other half stored on the cloud proxy. The user who has access rights can retrieve the data as the proxy will decrypt the cipher text with half of the user's private key in the proxy and then decrypt again on the user's side to retrieve the full plaintext. When the data owner wishes to revoke a user from accessing data, he simply informs the cloud proxy to remove the user's key piece.

As with the PECE scheme described above<sup>16</sup> this scheme does not allow outsiders to view the original plaintext at any point as the data remains in an unreadable format in the cloud. Only users with granted access rights can view the original plaintext. The main problem with this

scheme is that of collusion attacks. If a revoked user and the proxy collude, then the entire users get access to private key in the group. Also, the proxy may suffer from too many encryption and decryption operations.

### **Existing Data Obfuscation Techniques :**

It is a method or technique of data hiding where data is purposely scrambled to prevent from unauthorized access. Result of obfuscation is an unintelligible or confusing data. This technique is used to prevent the intrusion of sensitive data stored in the cloud. However, issues have stemmed from an inability to vigorously prevent security attacks. The different types of obfuscation technique are as follows:-

A. *Base64-Encoding* : In this Obfuscation technique ,it is commonly used when there is a need to encode binary data that need to be stored and transferred over media that are designed to deal with textual data. This is to ensure that the data remain intact without modification during transport. The Base64 encodes a word "Man" with "TWFu". The Base64 encodes the word "Man", by determining the related ASCII 8-bit values for each letter.

B. *Base32 Encoding* :In this Obfuscation technique it is designed to represent arbitrary sequences of octets in a form that needs to be case insensitive but that need not to be human readable. For the subset of US-ASCII 33-character is used, enabling 5-bits to be represented per printable character. This encoding process represents 40-bit groups of input bits as output strings of 8 encoded characters. Proceeding from left to right, a 40-bit input group is formed by concatenating five 8-bit input groups. Now, this 40-bits will treated as 8 concatenated 5-bit groups, each of which is translated into a single character in the Base32 alphabet. When a bit stream is encoded via the Base32 encoding, the bit stream must be presumed to be ordered with the most-significant-bit first. That is, the first bit in the stream is the high-order bit in the first 8-bit; the eighth bit will be the low-order bit in the first 8-bit, and so on. Now,each 5-bit group is used as an index into an array of 32 printable characters. The character referenced by the index is placed in the output string.These are identified from the Base32 index table in19 are selected from US-ASCII digits and uppercase letters.

C. *ASCII Encoding*: ASCII encoding Obfuscation technique is a character encoding scheme originally based on the English

alphabet. ASCII encoding is a method of representing characters with Base2 (binary) strings. These strings can then be further converted to other formats as needed like Hexadecimal, Base64, etc.

**D. Hexadecimal Encoding:** Hexadecimal encoding Obfuscation technique is a positional notation system with a base of 16. It uses sixteen distinct symbols. symbols 0–9 will represent the values zero to nine, and A, B, C, D, E, F represent values ten to fifteen respectively. For example, the number 2AF3 is equal, in decimal, to  $(2 \times 16^3) + (10 \times 16^2) + (15 \times 16^1) + (3 \times 16^0)$ , or 10995. four binary digits (bits) is representing as each hexadecimal digit, and the primary use of hexadecimal notation is a human friendly representation of binary coded values in computing. The data obfuscation is focused for the security of data in the cloud storage recently. Normally, obfuscation technique is not using keys to obfuscate the data unlike encryption. The key can be easily broken by brute force attack if it is Simple obfuscation technique. The proposed MONcrypt SSA is using a key to obfuscate the data in cloud. The key is kept by the user to de-obfuscate the data.

### III. the proposed confidentiality technique :

As by encrypting the non-numerical data and obfuscating the numerical data by single method cause more service cost and consumes more time and size. So by applying this technique both types of data converted into unreadable types simultaneously. When this technique is applied by the user, the keys are generated in the cloud side. The keys are sent to the user and the process is done in the user's side.

Cloud storage provides an efficient mechanism to store and retrieve the data. Ensuring data security is a prime concern of the user as the user deploys the sensitive data with the CSPs. This paper proposes confidentiality technique to avoid the problem of security issues. The Figure 1 depicts the procedure of data storage of non-numerical and numerical data using encryption and obfuscation technique respectively.

The proposed technique is to encrypt the non-numerical and numerical data simultaneously, by applying the proposed algorithm. The algorithm uses both encryption and obfuscation techniques. When the particular technique is selected by the user, it works simultaneously to process both numerical and non-numerical data. The symmetric cryptosystem is used to encrypt the data due to its computational efficiency of handling large volume of data while compared with the asymmetric cryptosystem.

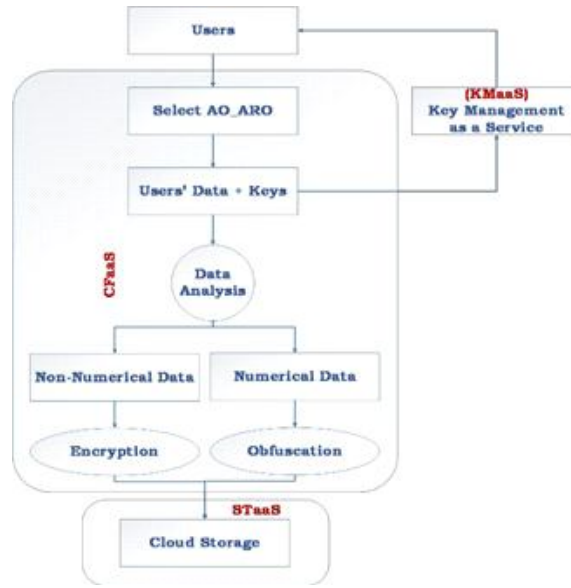


Fig.1. The proposed technique for obfuscation and encryption.

Algorithm 1 is used to find out the type of data to be encrypted and stored in the cloud storage. The data of different types will be applied on this technique by the user. If the data are non-numeric then the encryption technique will be activated. If the data are numeric then the obfuscation technique will be executed for the process. Both the techniques will be executed by call function simultaneously. The data are either encrypted or obfuscated and stored into the cloud storage.

Algorithm

#1

1. encry\_obfus(PT)
2. start
3.  $PT \leftarrow$  plaintext
4.  $K_i \leftarrow$  keys from KMaaS submitted to the user
5.  $N \leftarrow$  sizeof(PT) // Determine the numerical values in num
6.  $num(i) \leftarrow$  isdigits(T(i)) // Determine the non-numerical in non-num
7.  $nonnum(i) \leftarrow$  (isdigit(T(i)))
8. Execute the encryption procedure for non-numerical valuesThread.encryption\_text(nonnum(i),K<sub>i</sub>).
9. Execute the obfuscation procedure for numerical valuesThread.obfuscation\_digit(num(i),K)
10. Ciphertext (CT) is produced by the simultaneous execution of encryption\_text() and obfuscation\_digit().
11. End

Algorithm #2 is used for encryption. The algorithm is used for encryption of non-numerical data. The proposed encryption technique is used to protect non-numerical data in the cloud storage. When the user wants to hide only the non-numerical sensitive data, then this proposed encryption becomes very comfortable. This technique is based on symmetric cryptosystem. This algorithm uses three keys for encryption and decryption. Among the three keys two keys are integer and one is string type.

If user want to protect non-numerical data then the proposed technique is more suitable to them to secure their data in cloud. This proposed technique uses square matrix to manipulate the plaintext and it processes the users' data at three levels. First, the data are split based on even and odd column in the matrix. Second, the Key K1 and K2 are applied on the data alternatively. Third, data are filled in a square matrix in column-wise and read it in row-wise based on the order of characters in key K3. Finally, the ciphertext is produced for submitted plaintext. Decryption is done while reversing the process of encryption steps with same keys.

Algorithm #2

//AO\_Enc CT for CFaaS (non-numerical data)//

1. Start
2. Get the Plaintext (PT)
3. Find the size of the Plain text (N)
4. Covert the PT into ASCII code
5. Form a square based on N
6. Fill the SM [R] [c]by PT from left to right
7. Split the matrix into two blocks EB → Even column  
OB → Odd Column
8. Merge the EB and OB
9. Generate k1 and k2
10. Form a matrix by column in k3
11. Fill matrix by column by column
12. Read the matrix by row in order of k3 (AS)
13. Convert AS into ASCII character
14. Get the cipher text
15. End

Algorithm #3 is proposed for obfuscation technique to protect the numerical data in cloud storage. If user wants to encrypt the sensitive numerical data by obfuscation technique, then this proposed technique is suitable and convenient. This technique is a symmetric cryptosystem. There are two keys used in this proposed algorithm for encryption. And both the keys are of integer values. With these two keys, the obfuscation of numerical data is possible for protecting the data in public cloud.

Algorithm #3 //Proposed ARO\_Obfus CT for CFaaS (numerical data)//

1. Users submit the plaintext (PT) and keys (Ki)
2. Determine the numerical values in the PT.
3. Find the number of values in the N=sizeof(PT)
4. Generate a key K1 from cloud for ARO\_Obfus CT
5. Find the Product(MT) of K1 and PT
6. Calculate the square (SQ) for each value in the MT, SQ=square(MT).
7. Generate a key K2from cloud for ARO\_Obfus CT
8. Rotate SQ at K2 number of times, K2 is incremented by 1 for consecutive value in the SQ. Rotation\_SQ (RTN) = RK+j(SQ )j = 1,2,...<N // (R denotes Rotation)
9. Calculate modulus (MOD) for RTN by 256, MOD=RTN% 256
10. Convert the MOD into ASCII code to produce ciphertext (CT).

For better understanding of the proposed cryptographic technique, sample transactions of students' details are considered as shown in Table 1. The data in Table 1 are the plaintext before being encrypted and obfuscated. The proposed technique is utilized to encrypt and obfuscate the data before stored into the cloud storage.

Reg. No	NAME	M1	M2	M3	Total	Grade
17mcs100	Ravi	60	92	72	224	B
17mcs200	Sam	59	96	56	211	C
17mcs300	Sanjay	86	49	87	222	B
17mcs400	Vijay	45	65	68	178	D
17mcs500	Vikram	66	59	86	211	C
17mcs600	Aayansh	87	93	46	226	A

The Proposed cryptographic technique is implemented in JAVA running in windows 7 operating system. As the proposed algorithm #1 is executed, the encryption algorithm #2 is called and the non-numerical data are encrypted in the Table 1. Table 2 represents the encryption of non-numerical data of the students by applying Algorithm #2, where the numerical data remain the same.

Table II Transactional Table with text after Encryption

&^%	(*&	!*^	\$%	+?>	<^%	!@^%
\$NJP						
Ki*&^	#)(&	*&^	)#*	<o(	!+^	(*&
)((#%	Mk&	&^\$	&^	?!(	&^%	*)&
\$	H	%	%			
MKJ\$	J)(#	?>U	*Mj	~&?	\$nK	#N)
#						
)(*#I	%N :	J7H	)><	^H	?*%	?#C
				%		
NI(*\$	@(^%	)\$(	\$*^	&^	#)%	G&%
				%		
+?< :	nH%! 0	&#B	!)(	(@*	*&^	H&#

Now the algorithm #3 is executed to obfuscate the numerical data and the data are shown as in Table 3. Hence Table 3 shows the data after encryption and obfuscation process. The data are stored in the cloud storage.

Table III Transactional Table with text after encryption and obfuscation

&						
^%\$N	( * &	! * ^	\$ %	+?>	<^ %	
JP						
( ) (# %	^H %	\$^*	MJ\$#	^ & % *	J#\$	H&#
				&	F & %	\$%
MKJ&#	r@#(	%\$&g	(><G	( ) & ^ & *	@(^ % )	
)( * #)I	nH%!0	J7h	)ZX@ (	& \$ * & \$ (	\$ ( & HG	) & ^ GH
NI\$&^	Jk( &	( ) ^ & H	* ( & ^ GH	^ & %	\$ ( ) # @	)( * # !I
+ _ * (^J	Sa^\$	#\$&c	@#\$G	( ) % % G	\$nK	^\$*HG
LK )( * # !I	& % # (	& # B	( @ *	^ % &	J7H	HG\$%(

From the observation of the above three tables, it is shown that combination of encryption and obfuscation is possible at simultaneous process and it gives more security to the data stored in the cloud storage. The proposed technique gives better results of minimum data size, produces minimum process time, and minimum service cost. The proposed technique produces better security since it encrypts and obfuscates the data. Supposing a hacker tries to tamper or retrieve the data from the table. By decrypting the non-numerical data alone, the hacker will not achieve his goal, Or by de-obfuscating the numerical data alone, it is of no use for the hacker. Hacker will not fulfill his malicious attacks by partially hacking the data. Hence the proposed technique is proved to be better in security.

#### IV. Conclusion

This paper proposed a technique to protect the confidentiality of data of numeric and non-numeric data by obfuscation and encryption. Encryption of non-numeric data alone will not provide security. In the same way, obfuscation of numerical data alone will not provide security to the stored data. So, the encryption and obfuscation process are needed for confidentiality of data. Both these techniques are processed simultaneously in order maintain confidentiality.

With modern scientific advancements, cloud computing is a technology of rapid development. However, the security problems have become obstacles to make the cloud computing more popular. Various existing techniques are utilized to solve these security problems. The proposed

technique also reduced the service cost, minimized the data size and process time while uploading into the cloud storage. This technique put forward a series of solutions for the present security problems that cloud computing meet. This technique proved to be better in providing confidentiality of data stored in the cloud storage. Hence security is enhanced.

#### V. References

1. Dr. L. Arockiam, S. Monikandan, G.Parthasarathy - Cloud Computing: A Survey , International Journal of Internet Computing, Vol. 1, Issue 2, ISSN: 2231 – 6965, pp. 26-33 (2011).
2. Dr. L. Arockiam, S. Monikandan, -Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Volume 2, Issue 8, ISSN : 2278-1021, August, pp. 3064-3070 (2013).
3. Atiq U R Rehman, and M. Hussain, - Efficient cloud data confidentiality for DaaS , International Journal of Advanced Science and Technology, Vol. 35, pp. 1-10 (2011).
4. Yau SS, An HG, - Confidentiality protection in cloud computing systems, International Journal Software Informatics, Vol. 4, Issue 4, pp. 351-365 (2010).
5. Yu S, Wang C, Ren K, Lou W, - Achieving secure, scalable, and fine-grained data access control in cloud computing, In: INFOCOM, proceedings IEEE, pp. 1-9 (2010).
6. Bernstein, D., Chen, H., Chen, M., Cheng, C., Hsiao, C. and Lange, T., - The Billion-Mulmod-Per-Second PC, In SHARCS '09: Special-Purpose Hardware for Attacking Cryptographic Systems, Lausanne, pp. 131-144 (2009).
7. V. D. Cunsolo, S. Distefano, A. Puliafito, and M. Scarpa, - Achieving information security in network computing systems , Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'09.), pp. 71-77 (2009).
8. Hadi, S., Alireza, S., Behnam, B. and Mohammadraze, A., - Cryptanalysis of 7-Round AES-128, International Journal of Computer Application, 10, pp. 21-29 (2013).
9. Kazys, A. and Janus, K., - Key-Dependent S-Box Generation in AES Block Cipher System. Informatica 20, pp. 23-34 (2012).
10. Alex, B. and Johann, G., - Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware, Journal Fundamental Informatics—Cryptology in Progress , 10th Central European Conference on Cryptology, 10-12, Vol. 114, pp. 221-237 (2010).
11. Nashaat el-Khameesy, Hossam Abdel Rahman, - A

- Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems , Journal of Emerging Trends in Computing and Information Sciences, Volume 3, Issue 6, pp. 970-974 (2012).
12. Zhao G, Rong C, Li J, Zhang F, Tang Y, - Trusted data sharing over untrusted cloud storage providers , IEEE second international conference cloud computing technology and science (CloudCom), pp 97–103 (2010).
  13. Zhao G, Rong C, Li J, Zhang F, Tang Y, - Trusted data sharing over untrusted cloud storage providers , IEEE second international conference cloud computing technology and science (CloudCom), pp. 97–103 (2010).
  14. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y, - Fine-grained data access control systems with user accountability in cloud computing , IEEE second international conference on cloud computing technology and science (CloudCom), pp. 89–96 (2010).
  15. S. Arul Oli and L. Arockiam, - Confidentiality Technique for Data Stored in Public Cloud Storage, International Journal of Engineering Research and Technology (IJERT), Vol. 5, Issue 2, 2016, ISSN: 2278-0181, pp. 44-48.
  16. S. Arul Oli and L. Arockiam, - Confidentiality Technique using Data Obfuscation to Enhance Security of Stored Data in Public Cloud Storage , International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 5. Issue 1, ISSN: 2278-909X, pp. 169-174 (2016).