
Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

**Article DOI:**10.21474/IJAR01/6925
**DOI URL:** http://dx.doi.org/10.21474/IJAR01/6925

*RESEARCH ARTICLE*

# TIME BASED SECURE DATA HANDLING IN PUBLIC CLOUD.

**K. Noorin Rahila[1], L. Nivedha[2] and R. Narayani[3] and Dr. W. Aisha Banu[4].**

1. UG Students, CSE Department,
2. B.S.A.Crescent Institute of Science and Technology.
3. Assistant Professor Sr.Gr, B.S.A.Crescent Institute of Science and Technology.
4. Professor,, B.S.A.Crescent Institute of Science and Technology.

## *Manuscript Info*

***Manuscript History***

Received: 12 February 2018
Final Accepted: 14 March 2018
Published: April 2018

**Keywords:-**
Data security, Access control, Reinforcement Learning.

## *Abstract*

Data sharing in the cloud faces many challenges on security and privacy. Cloud computing is preferred as it reduces cost for data management and its available resources. To protect data from third party cloud server, it is necessary to have an efficient data access control. There are many studies deals with fine grained data access control, but there is no proposed scheme for both access control and time-sensitive data with learning-based methods. Cipher text-Policy Attribute-based Encryption is used for data security in cloud. A time access control is necessary to handle time-sensitive data in public cloud storage. Apart from access control, it is also necessary to have user revocation for efficient access control. An effective solution is needed to let data owners upload the encrypted data using algorithm with time limit such that the intended users cannot access the data beyond the corresponding time. The data that are collected from the software agents will automatically determine the ideal behavior within the specific context in order to maximize the data owner's performance.



## Introduction:-

Cloud computing is an information technology (IT) services which retrieve the data stored on the cloud through the access of the Internet. It saves the user's data to an offsite storage system that is maintained by the cloud provider. Hence, this data are maintained, operated and managed by a cloud storage service provider on storage servers that provides more advantages on easy data sharing and cost reduction. Thus, more and more enterprises and individuals outsource their data to the cloud to be benefited from these services. Although the infrastructure under the cloud is much more powerful and reliable than personal computing device, they are still facing the problem in data confidentially and preservation. Therefore, the secured access control has become a challenging issue in public cloud storage [1].

Securing data is always of vital importance because of the critical nature of cloud computing and the large amounts of complex data. Data security is an important aspect of quality of service and hence security must be imposed on data by using cryptographic strategies to achieve secured data storage.

**Corresponding Author:- K. Noorin Rahila.**
Address:- UG Students, CSE Department, B.S.A.Crescent Institute of Science and Technology.,
#Assistant Professor Sr.Gr, B.S.A.Crescent Institute of Science and Technology.

There are many cryptographic methodology to protect the data and provide access control in the untrusted cloud sever.

One of the useful cryptographic methods is Cipher text-Policy attribute Based Encryption (CP-ABE) [2].In CP-ABE a user's private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. This strategy protects the data by providing flexible access control. This provides constraint on the access of the data [8]. But this will not handle time sensitive data.

To tackle the problem of handling the time sensitive data, Time based encryption can be used to provide access privilege upto specific time. Time based encryption is a two-factor encryption scheme combining public master key and time-dependent encryption which is kept confidential by a time-server upto a specific time.

In some cases, the authorized users may misuse or do fraudulently in accessing the data. The Central authority maintains the records of user, if there is any mismatch of the data entered or misrepresentation the user data will be revoked. Hence, to ensure the security and the revoked user cannot access the data anymore.

Another important aspect of cloud computing security is to provide learning-based methods[11]. This learning method is incorporated to improvise the security of outsourced data by identifying its ideal behavior. It is important in the field of organization using the public cloud to automate the agent to determine the behavior of the outsourced data with increase in vulnerabilities. Hence, Reinforcement learning is best suited for this scenario.

Therefore, proposed methodology enhance the security of data in the public cloud with time access control and also the learning agent area automated to contrive the security and content of the outsourced data.

**Related works:-**

Data on the cloud can be effectively acquired by anyone at any instance of time. Providing data security and data augmentation in cloud storage has dependably been a confounded work. Numerous work and researchers have been chipped away at this issue to give better data access control and data augmentation in the cloud storage.

In the [1], proposed a fine grained and time release access control by using CP-ABE (Ciphertext-Policy Attribute-based Encryption) with TRE(Time Released Encryption). This method has been first proposed in the [2] to implement fine-grained access control of document by taking the typical university setup. This work has been let to the future scope of partial encryption and decryption. But unencrypted data cannot be secured. In this paper the key generation is implemented using bilinear pairing of access structure. This increases energy consumption. To overcome this [3] proposed elliptic curve cryptography which generate the key in constant size which reduce energy consumption and time taken to generate the keys. This access control is needed when the data is shared to the group of users. Along with access control many security aspects of data is required. In [4], proposed secured group data sharing by integrating the following methodology: 1) data confidentiality and integrity 2) access control 3) data sharing without using compute-intensive reencryption 4) insider threat security and 5) forward and backward access control. By using this methodology, two keys are generated per user in which user get only one key to access the files in the cloud and other key is stored in trusted third party server. This paper provide future work of limiting the trust level of third party sever to enhance the system to avoid the insider threats. To prompt more security from various attacks, [5] proposed Hybrid Encryption RSA (HE-RSA) along with AES to ensure consistency and trustworthiness. This methodology proved it is efficient in brute force attacks, mathematical and timing attacks. This methodology has not been implemented in real cloud platform. In the data sharing between data owner and data user [6], proposed a scheme proxy re-encryption. In this data owner encrypt the message using own public key before sharing it in cloud. After receiving the request from data consumer by their own public key, data owner generates proxy re-encrypt key, by re-encrypting the encrypted message by using data owner private key and received public key and upload this re-encrypt message to the cloud. Data Consumers download the message from the cloud and decrypt using own private key. But this research leads to the problem of designing generic framework to implement proxy re-encryption and selective security can be achieved. By extending ciphertext-policy attribute-set-based encryption [7] hierarchical attribute-set-based encryption (HASBE) is proposed to provide access control in a hierarchical structure of users. This work implements fine-grained access control but it lacks in time access control. The data in the cloud are in the different form. One data will be always stayed in the same cloud and other data

needed to be transit from one cloud to another according to users needed. In the [8], suggest data security in cloud. This paper study is based on all three layer of cloud (SaaS, IaaS and PaaS) by dividing the data in two categories: data in rest and data in transit. Data in rest can be stored in private cloud whereas data in transit needs cryptographic strategies like block cipher, stream cipher and hash function. This paper has only given the outline of protecting the data using various cryptographic encryptions. Asymmetric cryptography algorithm has more security in sharing the key between two users. In the [9], proposed data security in cloud using RSA algorithm. As RSA provide high potential data in encryption methodology, it can be suitable for data security. But, this paper does not worked on access control in the cloud. Symmetric algorithm handles large volume of encryption data in speed and efficient manner. In [10], the security of data is enhanced in the cloud by using symmetric cryptosystems. Symmetric algorithm handles large volume of encryption data in speed and efficient manner. Hence, Advanced Encryption Standard (AES) algorithm is implemented which uses less memory space and provide high throughput compare to other symmetric algorithms. Multilevel of security is essential in cloud storage to prevent from various attacks. Thus, [11] proposed a scheme of using multilevel security to encrypt the file in the cloud storage. They implemented this proposal using AES-256 which performs the operation such as splitting of files, compression and encryption of file using RSA key. To improvise the data owner performance in uploading the data, data owner wants to understand the necessity of data user. In [13] proposed supervised machine learning which implemented this learning model in the external dataset.

**Cipher Text-Policy Attribute-Based Encryption:-**
**Cipher Text-Policy Attribute-Based Encryption (CP-ABE);-**
In Ciphertext-policy attribute-based encryption (CP-ABE) scheme user's gets private key is tied to a set of attributes representing that user's permissions. When a ciphertext is encrypted, a set of attributes is designated for the encryption, and only users tied to that access policy are able to decrypt the ciphertext.

**A common framework of CP-ABE contains four algorithms:**
**Setup:-**
The algorithm is executed by the authority incharge of the generation of the Public Master Key PK.
Key generation: The algorithm is executed by the authority and generates a secret key SK according to the attribute set S provided by a user.

**Encrypt:-**
The algorithm is executed by the data owner to encrypt plaintext M.
Decrypt: The algorithm is executed by the data user to decrypt a ciphertext CT with a pre-generated secret key.

**Time Based Encryption:-**
After structuring the access policy, time based encryption of data is needed to provide an access privilege to data user till the specific time. Consider a scenario data owner encrypt the file and upload in the cloud with current timestamp and provides last time to access the file. So, intend users can decrypt the message until the specific time provided by data owner. From the security aspects Time Based Encryption satisfies that 1) Intend user can only access the data 2) Even the intend user need to verify from the central authority to access the file 3) Time privilege is provided such that specific user can use the file up to time period provided by the data owner.

**Access Tree Structure and Time Based Components:-**
Access policy of Ciphertext-policy attribute-based encryption (CP-ABE) is expressed in the form of access tree structure. Hence, the access tree structure with respect to access policies is framed for data owner and data user.

A tree access structure is specified with access condition, in which leave nodes are different attributes and internal nodes are logical gates. The logical gates used is AND, OR operator.

Both for data user and data owner the access tree is created by using its attributes.

Consider the set of n attributes of owner/user $A_1$, $A_2$, $A_{3,\ldots\ldots\ldots,}A_n$. This attributes are taken in Universe set U = { $A_1$, $A_2$, $A_{3,\ldots\ldots\ldots,}A_n$}. The attribute of user is collectively taken in a set Å ⊆ U. To construct an access tree, the particular attributes are selected. For example, if Å = {$A_1$,$A_3$,$A_5$,$A_6$}, this attributes are selected the access tree is constructed using only this selected attributes and access policy requires only the set { $A_1$,$A_3$,$A_5$,$A_6$}.The selected attributes from the U are logically connected using logic gates AND for the access control structure.

Usually bilinear pairing is used to generate Secret Key SK for set of descriptive attributes. This scheme creates a key in infinite size which leads in more energy consumption. Elliptic curve cryptography [13] is used to generate a constant size of Secret Key. In this paper, RSA algorithm is used to generate a Secret Key after the data owner/user matched with access policy while registering their data in the system. The detail uses of algorithms with CP-ABE are explained in the proposed design. After registering into system the data owner is permit to upload the data in the public cloud. To encrypt that data the time period to access the file is provided which encrypt the file with time validation.

**Proposed Design:-**
**System Model:-**

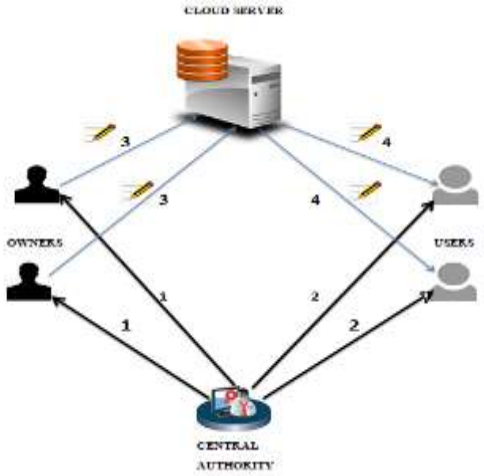


**Fig 1:-**Architecture of proposed system

1. Public Master Key(PMK)and Secret Key (SK) publish
2. PMK and SK Issue
3. Data Encrypt and upload
4. Data Query and Decrypt

The proposed model consists of three parties and the cloud server similar to the CP-ABE schemes. The three parties are: 1) Central Authority 2) Data Owner 3) Data user

**Central Authority (CA):-**
Central Authority is responsible for generating secret keys to the data owner and data user. This secret key is generated when the owner/user satisfies the access policy.

**Data Owner:-**
Data owner has rights to upload the data/files in the cloud. To upload the file first data owner need to enter the generated public master key to get authorization to upload and next step of security to enter secret key. This provides multi-level security and the data owner uploads the files with time period to be used by the intended users.

**Data users:-**
Data Users enters secret Key generated by CA to download the files. Data users query to get the cipher text stored in the cloud. The data user can download the files until the particular time limit provided by the data owner.

**Cloud Server:-**
Cloud server undertake the storage task in which it stores the cipher text data upload by the data owner. Any user who has direct access to the cloud even CA can view only the cipher text stored in the cloud.

**System Overview:-**
To ensure the high confidentiality data various security schemes and algorithm has been implemented in this proposed model.

First, the data owner/users need to satisfy the access policy. This access policy is designed separately for data owner and user. This method is implemented in the registration phase. During registration in the cloud the data owner/ users provide their credentials and the system checks their credential with the access policy attributes. If there is a match with access policy, the data owner / users get the secret key from the Central Authority. This Key is generated by the RSA algorithm.

In the data owner phase, the owner uses master public key to log in to the system. After login, the data owner has authority to upload the files. To upload the file, owner needs to enter the generated secret keys. After verification of the secret key, the data owner uploads the files with time limit. Hence, these files are taken with time limit and encrypt in the form of cipher text and stores in the cloud. To encrypt the file AES with PBE encryption algorithm is used.

In the data user phase, the user can query the files needed and give the request to access the files. These requests are send to the CA who checks with the access policy of the user and approves to download the file. Until this, user can view only the cipher text. After approval, the user enter secret key which is pre-generated during registration phase to get original content of files during downloading. Hence, this user can use this file till the time period to access the file provided by the data owner. This decryption of file is implemented using AES with PBE decryption algorithm.
The user revocation is needed to enhance the fine-grained access control in the cloud. Consider the scenario, any organization like colleges or universities if the working employees like staff or student resign their position or passed out student they should not get access to data of the university public cloud. So, this can be achieved by continuous update of their credential details. This details will be matched with access policy again ,if there is mismatch the user account will be revoked.

**Algorithm Used:-**
Various cryptographic algorithms are used to enhance the security in sharing the data in the cloud. Hence, these algorithms are used with CP-ABE scheme which consist of four phases namely: Setup phase, Keygeneration phase, Encrypt phase and Decrypt phase.

**Setup phase:-**
In this setup phase, the universe of attributes U = { $A_1$, $A_2$, $A_{3,\ldots\ldots,}A_n$} is taken as input and the output of the phase is access tree and access policy for data owner and data user. The construction of access tree and access policy is provided in detailed [2].

**KeyGen phase:-**
In this phase, the key generation algorithm takes an input of access policy attributes Å and generates the Master public key and secret key .This has been implemented in registering data in the cloud. Thus data owner/user intends to provide the data while registering in the system and the data has been checked with access policy. If entered data matched with the access policy, the keys are randomly generated for different users. RSA algorithm is used to generate keys randomly.

**Algorithm-1 Key Generation:-**
**Input:-**
Two prime number p,q

**Computer:-**
Compute n = p*q and (phi) $\varphi = (p-1)*(q-1)$.
Choose an integer e, $1 < e < \varphi$,
such that $\gcd(e, \varphi) = 1$.
Compute the secret exponent d, $1 < d < \varphi$, such that $ed \equiv 1 \pmod{\varphi}$.

**For each user who satisfies access policy do:-**
The public key is (n, e) and the private key (d, p, q).

**End for return private key:-**
n is known as the modulus.
e is known as the public exponent

d is known as the secret exponent

This private key is send to user via their registered mail id. Public key is used as Master public key to hash the account password using Bcrypt algorithm. As user credentials are storing in the cloud database the password is hashed to enhance the security.

**Algorithm-2 Encryption Of Password:-**
**Input:-**
Password, Public Key, Cost, Salt

**Compute:-**
for each account password do
state ← BlowfishSetup(cost,salt,Public Key)
ctext ← Password
hashed ← hashpw (state,ctext)
end for
return hashed value to store in database

**Encrypt phase:-**
The data is uploaded in the form of files. This files uploaded by the data owner in cloud needed to converts as the ciphertext. So, the input of this phase is data in the form of files and the output of the files is encrypted text. This is to ensure the security of the file in the public cloud. So, Data owner uploads the file by entering their own secret key which is generated by the Central authority in the key generation phase. A symmetric cryptosystem uses only one secret key to encrypt the file. Symmetric cryptography encrypts the data faster and more secured manner. There are various symmetric algorithms in this AES algorithm is used with PBE(Password Based Encryption).Instead of generating different key for file encryption, a constant password is taken which is generated as a 128-bit key and goes to 10 rounds of permutation which finally produce cipher text.

**Decrypt phase:-**
This phase has been used by data user who needs to get the original content of file uploaded in the cloud. Before decryption, the data user gives request to download the file and the request is send to central authority. After the approval of Central authority the data user enters the own secret key which is generated in key generation phase and downloads the file. The file decryption is also implemented with AES with PBE algorithm.

**Reinforcement Learning:-**
Reinforcement machine learning algorithm is a learning method that interacts with its environment by producing actions and discovers errors or rewards. Trial and error search and delayed reward are the most relevant characteristics of reinforcement learning. Simple reward feedback is required for the agent to learn which action is best; this is known as the reinforcement signal. The necessity of reinforcement learning in this paper is to data owner need to know about intend users progress and difficulties with using the files they uploaded so that they can adapt their work to meet their user's needs. For this scenario reinforcement learning can be applied in the form of feedback. Feedback is information provided by the data users regarding aspects of understanding of data provided by the data owner. This learning can be well suited in the case of schools or colleges. The data owner is staff and data user is students. The student provides the feedback from the experience they are learning form their staff, this in turn increases student motivation with the subject, but subsequently will also decrease the number of students skipping classes or dropping out. The staff also uses a range of targeted feedback strategies to progress the student's understanding of the requirements of an assessment task. In this paper, the instructive feedback is used .There are various type of instructive feedback among this type Parallel feedback is used ,where the staff gives students a different form of the stimulus material that requires the same response. To gather the feedback from the various users and visualize in the form of graph, K-means clustering is used.

**Algorithm-3 K-Means Clustering:-**
Let $X = \{x_1,x_2,x_3,\ldots\ldots\ldots,x_n\}$ be the set of feedback and $V = \{v_1,v_2,\ldots\ldots\ldots,v_c\}$ be the set of centers.
1. Randomly select *'c'* cluster centers.
2. Calculate the distance between each data point and cluster centers.

| File Size (MB) | Blow Fish (Sec) | AES-PBE (Sec) | DES (Sec) |
|---|---|---|---|
| 0.01 | 2 | 1 | 1 |
| 0.03 | 2.001 | 1.02 | 1.04 |
| 0.05 | 2.5 | 1.05 | 1.9 |
| 1.12 | 2.8 | 1.4 | 2 |
| 2.04 | 3 | 2 | 2.5 |
| 3 | 3.5 | 2.8 | 3 |
| 4.8 | 4 | 3 | 3.5 |
| 5 | 4.5 | 3.9 | 4 |
| 7 | 5 | 4.1 | 4.5 |
| 10 | 5.5 | 4.4 | 4.9 |

3. Assign the data point to the cluster center whose distance from the cluster center has minimum of all the cluster centers.
4. Recalculate the new cluster center using:

**Table-1:-**Comparison of Encryption Time among BlowFish, AES-PBE, DES

$$v_i = (1/c_i) \sum_{j=1}^{c_i} x_i$$

where, *'$c_i$'* represents the number of data points in $i^{th}$ cluster.
Recalculate the distance between each data point and new obtained cluster centers.
If no data point was reassigned then stop, otherwise repeat from step 3).

**Performance Analysis:-**
The important aspect in this paper is to select appropriate algorithm to encrypt and decrypt the file uploaded in the public cloud. To ensure data confidentiality, integrity and faster encryption of data, symmetric algorithm is used. There are various symmetric algorithms in which best three algorithm is selected and compared . Thus in this paper , AES-PBE algorithm is and compared with BlowFish and DES algorithm.

**Encryption Execution Time:-**
Experimental result for Encryption algorithm BlowFish, AES-PBE and DES are shown in table-1, which shows the comparison of three algorithms using ten different file sizes. The results are tabulated.

By analyzing table-1, Time taken by AES-PBE algorithm for both encryption and decryption process is much lesser compare to the time taken by BlowFish and DES algorithm.

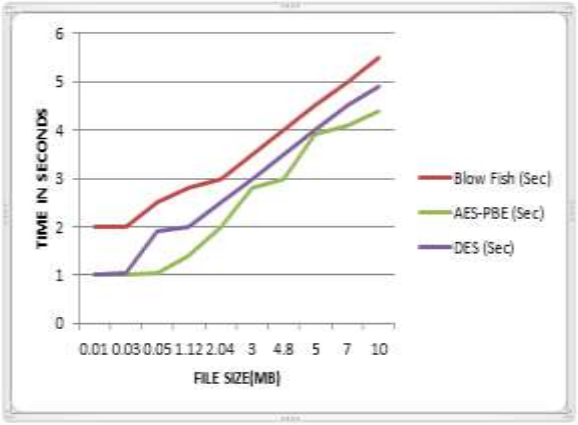


**Fig 2:-**Comparison of Encryption Time among BlowFish, AES-PBE, DES

**Decryption Execution Time:-**
Experimental result for Decryption algorithm BlowFish, AES-PBE and DES are shown in table-1, which shows the comparison of three algorithms using ten different file sizes. The results are tabulated.

| File Size (MB) | Blow Fish(Sec) | AES (Sec) | DES (Sec) |
|---|---|---|---|
| 0.01 | 2 | 1 | 1 |
| 0.03 | 2 | 1 | 1.04 |
| 0.05 | 2.1 | 1.02 | 1.9 |
| 1.12 | 2.3 | 1.3 | 2 |
| 2.04 | 2.4 | 2 | 2.5 |
| 3 | 3 | 2.3 | 3 |
| 4.8 | 3.5 | 2.8 | 3.5 |
| 5 | 4.1 | 2.9 | 4 |
| 7 | 4.4 | 3.7 | 4.5 |
| 10 | 5.2 | 4.1 | 4.9 |

**Table-2:-**Comparison of Decryption Time among BlowFish, AES-PBE, DES

By analyzing table-2, Time taken by AES-PBE algorithm for both decryption and decryption process is much lesser compare to the time taken by BlowFish and DES algorithm.

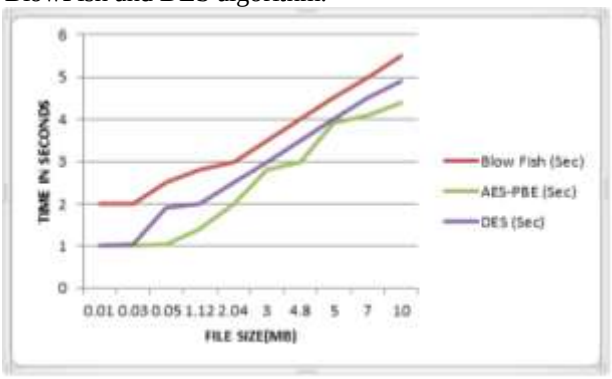


**Fig 3:-**Comparison of Decryption Time among BlowFish, AES-PBE, DES

## Conclusion and Future Work:-

In this paper, various algorithm and a method has been implemented to protect the data shared in the public cloud. Thus CP-ABE method is used to provide fine-grained access control along with Time-based encryption. From the performance analysis the symmetric cryptography, AES-PBE algorithm has the least encryption and decryption time. By constructing the access policy from the access tree structure, the access control and revocation of users to the cloud is bestowed. In order to maximize the sharing of appropriate data in the cloud by the data owner, reinforcement learning method is implemented in the form of feedback. This work can be enhanced in future by using the automatic software agents or machine to determine the security of outsourced data to learn the performance of the security algorithm of data in the public cloud and to prompt the security from the various attacks by the reinforcement learning based methods.

## References:-


1. Jianan Hong, KaipingXue, YingjieXue, Weikeng Chen, David S.L. Wei, Nenghai Yu and PeilinHong,"TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", IEEE Transactions on Services Computing, pp. 1939-1374, 2017.
2. ShardhaPorwal ,Sangeeta Mittal, "Implementation of Ciphertext Policy-Attribute Based Encryption (CP-ABE) for fine grained access control of university data", Contemporary Computing (IC3), Tenth International Conference ,2017.
3. VangaOdelu , Ashok Kumar Das , "Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography",ACM Journal on Security and Communication Networks, Vol. 9 no. 17, November 2016.
4. Albert Y. Zomaya, Fellow, IEEE,Athanasios V. Vasilakos, Senior Member, IEEE, Eraj Khan, Samee U. Khan, RevathiDhamotharan,Senior Member, IEEE, Keqin Li, Fellow, IEEE, Mazhar Ali, Student Member,"SeDaSC: Secure Data Sharing in Clouds" ,IEEE Systems Journal, vol. 11,no. 3,pp. 395 – 404,2016.
5. AkshitaBhandar, Ashutosh Gupta , Debasis Das, "Secure algorithm for cloud computing and its applications", Cloud System and Big Data Engineering (Confluence), 6th International Conference,2016.
6. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing", IEEE Transactions on Services Computing, 2014.
7. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing",IEEE Transactions on Information Forensics and Security, Vol.7, no.2, 2012.
8. Ahmed Albugmi,Madini O. Alassafi , Robert Walters, Gary Wills,"Data Security in Cloud Computing", Fifth International Conference on Future Generation Communication Technologies,2016.
9. PachipalaYellamma, ChallaNarasimham, Velagapudisreenivas," Data Security In Cloud Using RSA", Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference,2013.
10. Vishal R. Pancholi,Dr. Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES",International Journal for Innovative Research in Science & Technology,Vol. 2,no. 09 ,2016.
11. Akshat Kumar Dixit, Dr.Charu, "Multilevel Security framework for Cloud Data",Computing and Communication Technologies for Smart Nation (IC3TSN), International Conference,2017.
12. Ming Li ,ShuchengYu ,YaZheng , Kui Ren ,WenjingLou,"Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems,vol. 24,no. 1,2012.
13. Deval Bhamare , Tara Salman , Mohammed Samaka , AimanErbad , Raj Jain, "Feasibility of Supervised Machine Learning for Cloud Security", Information Science and Security (ICISS), International Conference,2016.