Cipher Text Policy Attribute Based Encryption (Cp-Abe) using Concealed Policy in Public Cloud

A.C.Ashmita, C.Yamini

Abstract*: *Cloud computing focus on the data storage and the management. Since the cloud is open source for the user there have to protect the privacy and the security of the data which are less maintenances. There are several approaches designed to establish a secure data. The Signature work of this scheme is to allow the user to verify the shared in the cloud using the secret key. The anonymzed access policy can be viewed by the Cloud Service Provider (CSP) and the user; hence the recipient information will not be leaked or disclosed. The novel idea of this method is to conserve the privacy of the access policy using Cipher text Policy Access Based Encryption (CP- ABE) scheme. We have proposed a novel system, "Concealed Policy using mandatory and Role based", using time elapsed of 10 secs. Within the required time the user, should response to the cloud using their Secret key(SK) to decrypt the file, and the owners with the Public key (PK), must encrypt the file using the mandatory access and upload it to the Third Party Auditor (TPA).This will improves the security to the user in the cloud environment. The concealed policy relies on two stages, there is Mandatory policy and Role based policy using the signature verification. Which are more efficient to the user to encrypt and decrypt the file. Without verification of the signature, the legitimate user cannot access the particulars in the cloud environment. If the signature of the user is valid, there can access (decrypt) the file using the SK. whereas, invalid signature occurs the TPA (Third Party Auditor) traces the reasonable user responsible for the signature and check with the mandatory access to encrypt the file, Nether less the access den ailed.

Index Terms*: *Cloud Service Provider, CP-ABE, Mandatory Policy, Role based Policy, Third Party Auditor

I. INTRODUCTION

Cloud based storage service have been developing in our daily lives in the integral form, many user uses the cloud storage and there provide the convenient mean for the user to store, access and synchronize there data with the multiple device [1]. Cloud Computing deals with the benefits of business and the end users. By using three types of services, only the cloud computing can be able to store the data's. These are also called as cloud computing stack because they are arranged one after the other [2]. These services are slightly difficult to use, based on the provider, it might be easy to use in a friendly manner in some browser-based dashboard which will be easy for the IT professionals and the software developer to organize their accounts in the cloud [3]. Basic idea is to transmit all kinds of resources through the Internet such as storage resources, computing resources, bandwidth and so forth. Users do not need to purchase a large of computing systems to manage their business [4]. Services are sold on a subscription or pay-per usage basis over internet. Need to pay for the resources according to their needs in order to decrease the cost greatly [5].

The main contribution of this work is to provide a reliable data sharing using the Central authority. The owners and the user are having the respective keys; using mandatory and the Role based policy the flow of the proposed, "Concealed Policy using mandatory and Role based" are proposed. The novel work involved in this study is the elapsed time. When a user demands a file in the cloud, there will give a time span for the request and response of the message. If it overheads the times stamp; the access be denial. At this point there embed the time-release encryption in to (Cipher text Policy Attribute-based Encryption) CP-ABE, by doing this there can develop time sensitive storage data in the public cloud. So, it improves confidentially in time-sensitive data. The Mandatory policy is used to encrypt the particulars in a secure manner using the PK (Public Key). Thus, there are linked to the TPA with the PK sharing after the text are been encrypted. If the user wants to decrypt the plaintext from the cloud means, there have a Role based policy where it obtains a key size of the user demands and also the signature verification for the sign in to the legitimate user. This overall process should not elapse the time of 10 sec.

The main contribution of this paper is to improve the security and provides a legitimate user to access the file in the cloud environment. In order to maintain the reliable authentication between the owners and user a novel scheme of "Concealed Policy using mandatory and Role based", is been introduced in this paper. It provides the robust result in our planned work. The remaining part of this paper is organized into Section II Discussion about the Literature Survey, Section III, describes the System Model of the proposal, Section IV, Explore of the Proposed Work, Section V Analysis the Experimental Result and Section VI Presents the Conclusion.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author

A.C.Ashmita, Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, Tamilnadu, India

Dr.C.Yamini, Associate Professor, Department of Computer Science, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, Tamilnadu, India

II. LITERATURE SURVEY

There have presented an Efficient Revocable Attribute Based Encryption (RABE), which is introduced for dynamic group among the authorized users and it also protects the ciphertext by using some of the concepts there are as Identity based encryption, Attribute based encryption, Subset over the framework and ciphertext encoding mechanism. By using this there obtained better result in encryption and decryption time. Here the drawback is that high number of attributes are been utilized by the many revoked users and there are some complexity that the boundary system will take the typical time for computation [6].

The study is about the Economic Denial of Sustainability (EDoS) that endangered the malicious file used by the user, where the cloud user and the cloud service provider are reduced, when there is a nonexistence of user-to-cloud controllability, to occupy sever-dominated access control an improved safety mechanism is been introduced. The main ideal is to integrate the ciphertext data and providing the confidentiality. The communication and the computation overhead were considerably reduced by the improved model. There ought to improve the time cost taken for the signature verification it happens because of the resource overhead is reduced [7].

The author have discussed about the role based Encryption which works towards the cloud atmosphere to stock up the data in the secure manner. Every user at this time will be handing over a specific task and permission of the data. Besides to encryption and the decryption process the broadcast algorithm will be developed. And also it will reduce the cost maintenance for the individual services. There should focus on the permission access when the new role are been assigned the permission will be restricted and when coming to the complexity it is high when the user employ the better amount [8].

There have studied about the crypto-cloud + which is used for the authority it is also said to be revocable CP-ABE cloud system, the decrypted feature and the access credentials are stored in the secured manner. There uses the prime order group that are hardest to determine each and every factor that relies on the subgroup decision assumption. They must improve the decentralization hope between the cloud user and the cloud service provider and also the ciphertext will be reduced when the credential leakage is done and the malicious cloud user is reduced [9].

They have presented a Data Security for Cloud Environment which provide a Semi-Trusted Third Party (DaSCE) which provide the security for the key administration, access control and the file assured deletion and also it maintenances the purposes of the integrity, access control an data deletion in the outsource. It is used in the session key which will reduce the cryptographic process occasion. They should get better on the result in the increment of the supplementary data and the performance of the group shared data is degraded [10].

The author have discussed about the exchangeable rational secret key sharing system is introduced for sharing data. When the intended user is not found in any cases means the encrypted data is useless. Depending upon the users the data sharing are processed. The experimental results shows that the reconstruction round complexity have been increased in the data usage. It must improve in the computational time is very high for the rational user and it relies on the high communication cost [11].

This study is about the identity and the access management in cloud for authentication and the access management, security and services over the cloud environment will be overcome by this developed technique which will be improved in this kind of services in the cloud related problem in the existing work will be rectified. And a comparative study is done on the previous and the current techniques in the perspective cloud service provider and the cloud user which include the identity and the access management, security issues and the service in the cloud environment is been highlighted [12].

There have presented an EDedup, which is similar in the encryption in the form of deduplication scheme that supports in the flexible access control with revocation of the data in the cloud. The data deduplication is used to reduce the storage in the cloud. The major task of this is to group the files into segments and perform the server aided MLE at the segment level, it reduce the computational consumption that exploits the representive hash. And the experimental shows the storage overhead. The issue here is the storage overhead will be high and the time consumption in the decryption data will be high [13].

This study is about the outsource decryption in the public cloud which will be mainly alter the anonymity of the pseudonyms of the encryption and the symmetric techniques. One of the recent studies here is the data access control management in the remote system. And the planned system works to obtain the better result in the security and the efficiency. The drawback is that hash function are been randomly used here and the computational complexity will be high when the hash function is higher, it consumes higher time complexity when there decrypt the data [14].

The author has presented a CP-ABE in fine grained access control. An essential attribute is built a trust among minimally trusted server for key encryption and updating process a well-defined user-revocation is been developed. So the efficiency and the security will be enhanced in the revocable system. The disadvantage is that the Diffie Hellman key exchange protocol is used for the security validation and the attribute number will be lesser and the polynomial time adversary attack is high to resolve [15].

III. SYSTEM MODEL

Central Authority: Which are responsible for the security protection of the whole system. It publishes the Secret key to the user and the public key to the owners using the time elapsed of 10 Sec.

Data Owners: There are responsible for the publisher of the file and pay for the resource consumption on file sharing. The data owners are used to justify the resource usage, which decides on the attributes (Mandatory).

And encrypt the file in the decided policy before uploading it to the cloud.

Data User: There the secret key is obtained from the Central authority. Only if the attribute (Role-based) satisfied for the queried user using the time elapsed only can decrypt the file from the user.

Cloud: This includes the administrator of the cloud and cloud server. It takes role of the storage entities and executes the access privilege using Role based scheme.

Third Party Auditor: The responsibility of this is to develop auditioning scheme for the secure development and efficient user. Thus it provides the capability such as privacy preserving, public auditing and the data confidentially. Encrypt the file using Mandatory access control using the file name and the password with the numeric and character.

IV. PROPOSED SYSTEM

In this section we have discussed the working flow of our proposed model named,” Concealed Policy using mandatory and Role based “, used to provide the multilevel security for the user. The CP-ABE is the data access method, which are using cryptography method.

CP-ABE SCHEME

CP-ABE scheme are associated with the attribute set. The cipher-text is associated with the access control policy. The CP-ABE is usually consists of the following algorithm to give the access control for the key.

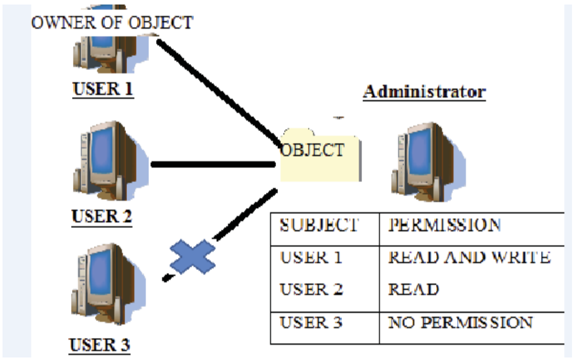
1. Setup: Input a random number c, calculate the setup(c) = {SK,PK}, where SK is a secret key, PK is the Public key.
2. Key Generation: Input SK user’s attribute set α, calculate the CA= Encrypt (PK, MA, T), Where CA is Central Authority, MA is Mandatory and T is TPA, α={u1,u2….ui}, ui is the end user.
3. Bilinear: Input e: $G_1xG_2 \longrightarrow G_T$, CA=Setup(c)= a,bƐZ, $e(g^a,g^b)=e(g,g)^{ab}$, Where Z is the plaintext, a is a generator of the G_1 and b is the generator of the G_2.
4. Encrypt: Input PK access structure T and Plaintext Z, calculate the CA=Encrypt α(PK, Z, T)

5. Decrypt: Input SK CA, calculate Z=Decryptα (SK,CA).

The proposed approach composed of two stages which are explained as follows:

A. *MANDATORY POLICY*

The mandatory policy in the CP-ABE will provide a multilevel security to the attribute and there are done on the classification of subjects and the objects. The object will be storing the passive entities; whereas, the subject stores the active entities which gives a request access to the object [16]. There are accessed by the security classification here it will discussed about two access classes there are of security level and set of categories, the security level will provide a hierarchical ordering which include the data should be on the top secret, confidential, and unclassified shown in fig.1. Thus the set of categories will includes the unordered subsets, which reflects on the elements such as functions and the competence areas (Army, Military, and Financial Administration) [17].



SUBJECT	PERMISSION
USER 1	READ AND WRITE
USER 2	READ
USER 3	NO PERMISSION

Fig.1. Mandatory Access Control

B. *ROLE BASED ACCESS CONTROL*

The notion of this role based access control (RBAC) is the authorization process that is associated with set of roles and the user. Thus the role acts as an intermediate for the user and the permission [18]. When a new system or application are been incorporate the role will give the permission, and there revoke the permission when it is needed [19]. In Role assignment the user, role and permission are interlinked to each other shown in the fig.2. Role authorization composed of operation that are applied to the object which validate the attribute (to be secure only to the role user) and the role validation will be done with the cloud service [20].

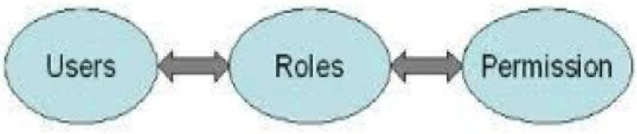


Fig.2. Role assignment

The central authority is responsible to maintain the whole systems protection, here it publishes the secret key (SK) to the respective user and the public key (PK) to owners and also maintain the time elapsed agent as 10 Sec in the cloud. The flow of the proposed, are the central authority publish the public key to the owners and the owners are been linked to the Mandatory access to encrypt the file using the Third Party Agent (TPA). The owner will give access to the TPA which must be mandatory such as Filename, Username and the Password that includes the numeric and capital letter. The owners encrypt the file and upload them to the cloud in a secure message flow. Whereas, the TPA encrypted file are associated to the cloud and there are directly related to the storage cloud environment and shares the public key. When the user request for the particular in the cloud, the cloud environment are maintain the secure flow with the owner. Here the request is carried out on Role-Based which consist of the size of the key the user demand along with the SK. Thus, the secret key is used for the decrypt of the file.

In this proposed work, by using the mandatory policy the security will be protected when compare to the previous studies.

Retrieval Number B2916078219/19©BEIESP
DOI: 10.35940/ijrteB2916.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Thus, there are been used for the reliable security of file sharing using encryption and decryption. And the Role based Access control is used for assigning the role to the particular user such that, which user can access the file at a particular time of 10 Sec in the cloud environment. In this case, when a user have a particular roles to access the file in this situation there cannot be forge other user's secret key. According to the user demands the cloud check for the signature validation in the TPA using the user secret key, if it is satisfies the validation test there can decrypt the file. If the signature is not valid, in this case the cloud checks to the TPA and trace the legitimate user. The two ways mandatory access is used to validate the signature, the verification is the password includes the numeric and the username. The Role based access policy relies on the key size the user request for. In order to obtain the legality of the source input this verification phase is carried out; by this phase the harmful information flow, data leakage, un-trusted administrator is prevented.

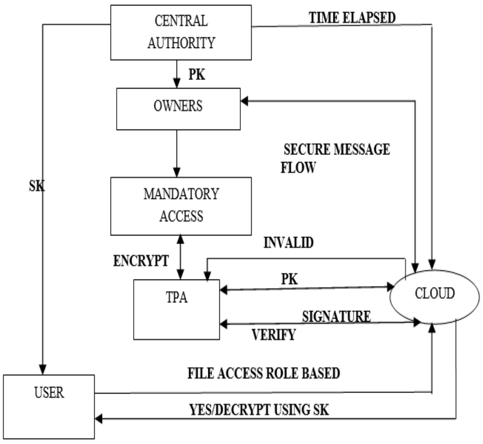


Fig.3. Proposed Flow

V. EXPERIMENTAL RESULT

This section presents the experimental analysis of the proposed model. Let us assume 100 number of user, TPA 3, Owners 2. The central authority generates the key according to the bilinear pairing using the prime number generation attribute set α. Let us take the memory size of 1MB for file. The first central authority provides the secret key for the 40 user, second CA gives the SK to the 30 user and the third CA gives SK to the 30 user. By doing this the 2 owners are been generated a PB by the CA. And the 3 TPA works when there satisfies the mandatory access, the first TPA encrypts the file using the user12name and the password followed by the two TPA the process are carried out in this environment. The previous approach is not satisfied with the security policy. Whereas, in this proposed model there relies on two security access control to access the file.

A. *PERFORMANCES METRICS*

1) *Key Generation*

In this initial phase the key are been generated using the bilinear pairing and thus there are two types of key must be generated there are of Public key and Private Key. Thus time to calculate the key generation in this study is by arithmetic modules function. And the public key is related by e, where e<n; n is the key size. The Private Key is associated by the d, where (ed-1) should be divisible by mod x. To find the greatest common divisor of the prime number the GCD is used. The formula for the generation is as follows:

N= P*Q, f(n)= (P-1)(Q-1)
GCD (f (n)) =e (P-1)+(M+1)
$D=e^{-1}$mod f (n)
Where,
N is the key size
P is the Public Key
Q is the Private Key
E is the relative prime number of P
D is the Relative prime number of Q
M is the Message size

2) *Encryption Time*

The input can be any arbitrary sequence of bytes. It is executed by the owners using the mandatory access policy, which generates the PK for the encryption of the Z plaintext. The calculation for the general process is CT=Encrypt (PK, Z, T) Where T is the access structure CT is Cipher text. The proposed module for the encryption time calculation is as follows:

T=n *p
Whereas,
T is the Encryption time.
N is input data size in bytes
P Processing time begin to start a process.

3) *Decryption Time*

In this phase the decryption is calculated by the mod 26. Which is similar to the encryption process, it is necessary to perform the inverse multiplication of the integer a. The general calculation for this is the decrypt the plaintext Z using the SK. The modules for decryption are as follows:

$T= a^{-1}(x-y)$ mod m
Where,
T is the Time taken to execute the decryption process
a^{-1} is the inverse multiplication
X is the Ending time of the process
Y is the Starting time
M Number of alphabets from A to Z.

4) *Throughput*

The throughput refers to the performance of the message/task by computing service or device over a specific time. Here the time elapsed is used for the calculation of the encryption and decryption of the particular text in the required time period. It refers to the data in bytes (size)/ End time-start time.

$Th=T_S/T_E$

Whereas,
Th is the Threshold
T_S is the Size of the original text (bytes)
T_E is the Total time taken for the encryption and decryption.

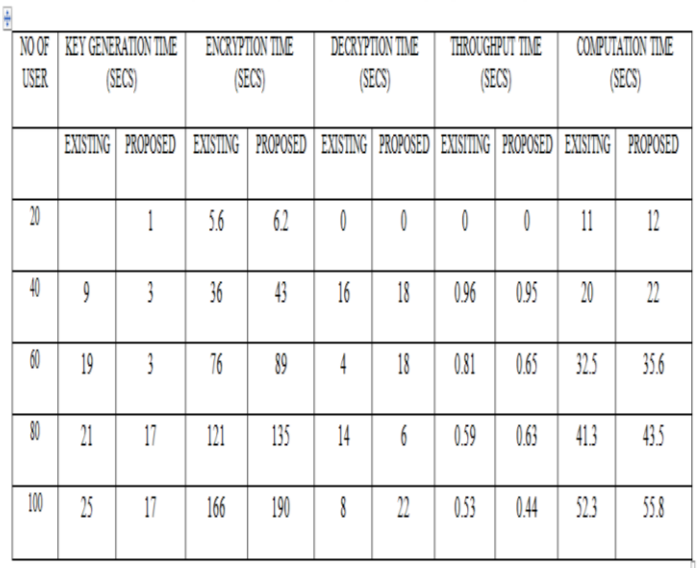
5) *Computational Overheads*

It is the processing time required for the user in the system to compute the data size/bytes. In this phase the computational overheads are calculated by fixing the size of the file, for example it may be 1MB. According to this the overheads are been calculated. If the user is not legitimate, the cloud does not verify the signature. In this case the Overheads are small in size.

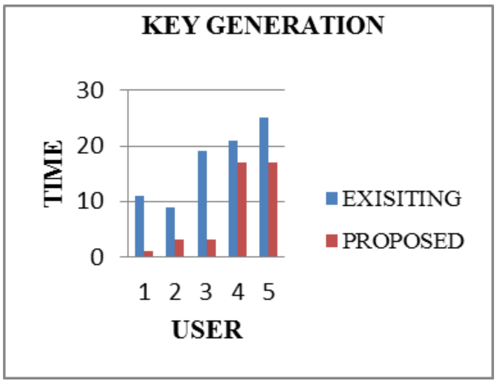
C_c= F+ P_c<1MB
Whereas,
C_c is the Computational overheads in the Cloud.
F is the File upload
P_c is Process completion time.

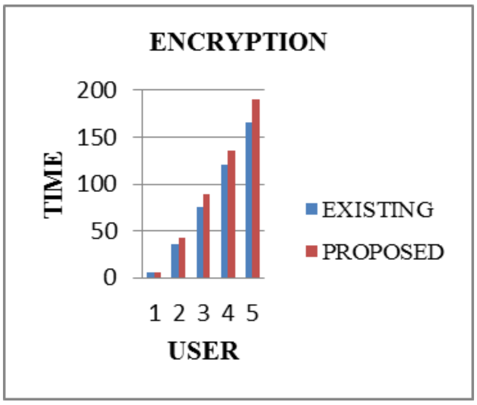
Encryption time of the existing work are having the lesser time to completed the request because the file size is of 1 KB whereas, in the proposed work the encryption process takes higher time because the fie size used is 1MB. So, the proposed model works in better encryption using the mandatory by generating the PK from the owners to the TPA in cloud. When coming to the view of thresholding the value of existing is lesser, proposed are higher in secs so the time taken to process a message in the cloud is lesser since the size of file is higher. Such that the encryption and the decryption of the text are carried out in the fixed time elapsed of 10 secs. Whereas, the computational overheads are been calculated by fixing the file size and with additional the process completion time in cloud, which must be lesser then 1MB. We modeled this aspect according to the fixed size, it satisfies our requirement by the access control such as Mandatory and the Role based.

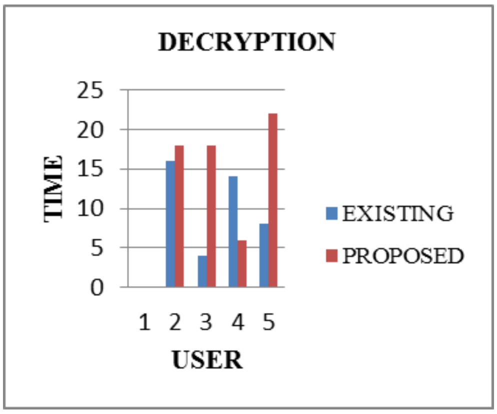
TABLE1. SHOWS THE PERFORMANCE ANALYSIS OF THE PROPOSED WORK COMPARING TO THE EXISTING WORK.

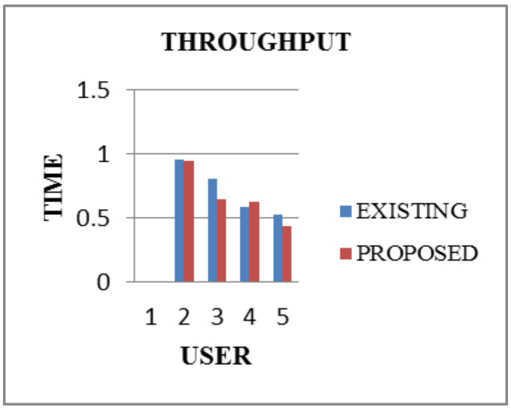


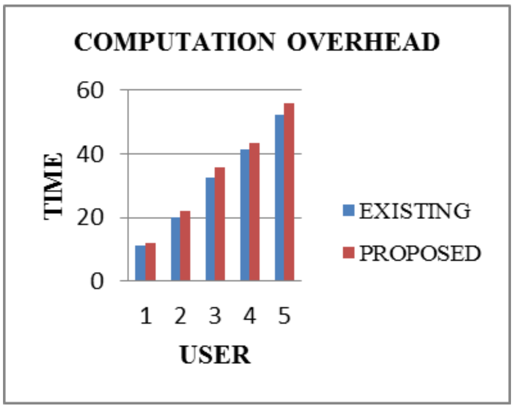
NO OF USER	KEY GENERATION TIME (SECS)		ENCRYPTION TIME (SECS)		DECRYPTION TIME (SECS)		THROUGHPUT TIME (SECS)		COMPUTATION TIME (SECS)	
	EXISTING	PROPOSED	EXISTING	PROPOSED	EXISTING	PROPOSED	EXISITING	PROPOSED	EXISITNG	PROPOSED
20		1	5.6	6.2	0	0	0	0	11	12
40	9	3	36	43	16	18	0.96	0.95	20	22
60	19	3	76	89	4	18	0.81	0.65	32.5	35.6
80	21	17	121	135	14	6	0.59	0.63	41.3	43.5
100	25	17	166	190	8	22	0.53	0.44	52.3	55.8











VI. CONCLUSION

This paper aims to provide a secure message through the cloud environment. One of the challenges faced here is the computation cost and un-authorized access to the cloud. In order to overcome these issues, we have developed an algorithm, "Concealed Policy using mandatory and Role based". This relies on two way security access control to access the file in cloud. Our work seamlessly integrates the elapsed time of 10 secs for cipher text, to encrypt and decrypt the file. The constructed system is secure against malicious data user, un-authorized user and data leakage. And the experimental result shows, the comparison result of the Key Generation, encryption, Decryption, throughput and computation overheads of the existing work. Which show that our work is efficient against the existing approaches and the time elapsed are satisfied in our system. We assume that our file size should be lesser then 1MB, according to time elapse the user and the owners should encrypt and decrypt the file.

REFERENCES

1. C.Lakshmi Devasena et al," Impact Study of Cloud Computing on Business Development", Operations Research and Applications: An International Journal (ORAJ), 2014.
2. Tatjana Vasiljeva et al," Cloud Computing: Business Perspectives, Benefits and Challenges for small and medium Enterprises (Case of Latvia)", Conference on Reliability and Statistics in Transportation and Communication, 2017, Pp.443-451.
3. G. Kiryakova et al," Application Of Cloud Computing Services In Business", Journal of Sciences, 2015, 13(1),Pp. 392-396.
4. John C. John et al," Optimal Rule Mining for Dynamic Authorization Management in Collaborating Clouds Using Attribute-Based Access Control", IEEE 10th International Conference on Cloud Computing (CLOUD),2017,Pp.739 – 74.
5. Maithilee Joshi et al,"Attribute Based Encryption for Secure Access to Cloud Based EHR Systems,IEEE 11th International Conference on Cloud Computing (CLOUD),2018,Pp.932 – 935.
6. Shengmin Xu et al, "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Information Forensics and Security,2018 , 13(8),Pp.2101 – 2113.
7. Kaiping Xue et al, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage", IEEE Transactions on Information Forensics and Security,2018 , 13(8),Pp. 2062 – 2074
8. Lan Zhou et al, "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud", The Computer Journal,2011 , 54(10),Pp.1675 – 1687.
9. Jianting Ning et al," CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage", IEEE Transactions on Services Computing, 2018.
10. Mazhar Ali et al, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing,2017 , 5(4),Pp.642 – 655.
11. Hai Liu et al," A Fair Data Access Control towards Rational Users in Cloud Storage", Information Sciences, 2017, Pp.258-271.

I. Indu et al," Identity and access management in cloud environment: Mechanisms and challenges", Engineering Science and Technology, an International Journal, 2018, 21(4),Pp.574-588.

12. Yukun Zhou et," A similarity-aware encrypted deduplication scheme with flexible access control in the cloud", Future Generation Computer Systems, 2018,Pp. 177-189.
13. Huaqun Wang et al," VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud", IEEE Transactions on Services Computing, 2017.
14. Huaqun Wang et al," VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud", International Conference on Advanced Cloud and Big Data, 2016.
15. Yi Zhu, et al, "Formal verification of mandatory access control for privacy cloud", Proceedings of 2013 3rd International Conference on Computer Science and Network Technology,2013,Pp.297 – 300.
16. Abdul Raouf Khan et al, "Access Control in Cloud Computing Environment" , International Conference on Advanced Cloud, 2015.
17. Madhura Mulimani et al," Analysis of Access Control Methods in Cloud Computing", 2016.
18. Yan Zhu et al," Cryptographic Role-based Security Mechanisms Based on Role-Key Hierarchy", ACM,2010.
19. Sushmita Ruj,et al, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing,2012,Pp.556-563.