iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6154

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

Enhancing the Efficiency of Key Management Protocol in Attribute based Encryption for Cloud Data Sharing

Priya Chaturvedi[1], Umang Thakkar[2]
[1]*Department of Computer Engineering, SOCET, Ahmedabad, India*
[2]*Department of computer Engineering, Professor, SOCET, Ahmedabad, India*

Abstract: ***Cloud computing provides its user an economical and easy way of use anything as a service, known also as pay and use service in which anything used and pay only for that . Cloud customers pay only for what they actually use resources, storage, and band- width, according to their changing needs. data transfer costs i.e., bandwidth is an important problem when trying to reduce costs. By loading and uploading the same data again and again and apply encryption and decryption it is very costly to encrypt and decrypt the same data. To secure the data and reduce the network cost use the cryptography technique. By using ABE scheme provide fine-grained sharing of encrypted data, but also give the advantages in the efficiency to overcome the drawback (by reduce of cipher text size and decryption cost) . In particular, an ABE scheme allows provide security from third party (e.g., a cloud server). if third party is untrusted ,the data cannot be safe.in this paper first describe the ABE scheme and then present a approach in which by using verification scheme to verify the outsourced and decreasing the computational cost.***

Keywords: cloud computing, Attribute based encryption cloud service provide, Cloud sharing.

I. INTRODUCION

Cloud computing is two word cloud and computing ,one side of cloud have very advantages but every coin have two side the security issue to protect data over cloud that no one can access the private and confidential data to address security factor which is basically important factor of cloud computing[1]. Data confidential and enforce access control policies correctly. However, security and confidentiality is not provided now a day because the stored data is shared among many service providers. Because the services and hardware that provided by the cloud is manage by the service provider.to protect the data from the untrusted third party the common solution is to masking the data by the use of cryptography.

The encrypted data, however, must be important for sharing data and smoothly access control for the on the cloud . Data encryption using symmetric or public key cryptography is not enough to scalable access control. Security of particular data basically means protecting data, e.g. database, from the untrusted provider and actions of unauthorized users. Basically there are three security goals i.e. Confidentiality, Integrity, Authentication. Our objective is to implement authentication algorithm in our project. Attribute Based Encryption is a security algorithm but it creates many drawbacks on the user of the system[2]. Hence, to minimize this drawback; ABE with outsourced decryption method was introduced. But this method does not give the correctness of the decrypted cipher text. Hence, we proposed a new and improvised method that is ABE with Verifiable Outsourced Decryption with KEM(key encapsulation mechanisms).

ABE scheme was proposed by Sahai and Waters in 2005 year. ABE is the mechanism in which users are allowed to encrypt and decrypt data based on the attributes provided by the user. The attributes that provided by the user are used to make the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible[3].

Therer are two type of ABE policy KP-ABE(key policy ABE) and CP-ABE(cipertext policy ABE) KP-ABE was proposed by Goyal in 2006 which is the extended form of traditional ABE. In KP-ABE the cipher text is connected or associated with a set of attributes and decryption key of user is connected or associated with a tree access structure. If the attributes match or satisfies with the cipher text with the tree access structure, then only decryption of file is take place.. Advantages of KP-ABE: The KP-ABE scheme can achieve more flexibility to control users and fine-grained access control than ABE scheme. CP-ABE data owner can access and policy over the attribute[3]. In KP-ABE scheme, cannot decide who can decrypt the encrypted data. Here only descriptive attribute are chosen for data by these scheme .but not suitable in some application because of untrusted service provider.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

CP-ABE overpowers the short come of KP-ABE of choosing who can decrypt the data In CP-ABE user's private key is a combination of a set of attributes. Hence a user can only use this set of attributes to satisfy the access policy for the particular file.
This paper focus on the security and privacy and confidentiality of the data by using the ABE scheme by verified the outsourced. Given paper is divided into six section in which II describe the existing related work followed by contribution of our work in III , proposed methodology , implementation of algorithm and conclusion in section IV, V and VI respectively.
By this method we decrease the computation cost by decreasing the total execution time and in previous method by adding the extra instances parallel it increase the cost by increasing the transform value which used to check the verified source . by our method it decrease the transform cost which run merging with our method.

II. RELATED WORK

Author GUOFENG LIN, HANSHU HONG ,ZHIXIN SUN explain the collaborative key management technique to overcome the problem of increasing key while uploading and downloading the data, the suggest this technique, technique is useful to overcome the key escrow problem. But disadvantage that method increase the computational cost by adding extra instances to secure the private key from the cloud service provider[4]. To overcome the above problem SUQING LIN, RUI ZHANG, HUI MA, MINGSHENG WANG suggest the verified outsourced encryption method that verified the sourced by using the KEM(key encryption method) that verified the source by using the hash function if the function is match with both in the process of encryption and in process of decryption, by matching attribute. This approach decrease the computational cost but practically the algorithm and set and apply of the method is lengthy[5]. KONDA REDDY GUDDETI, GANGADHARA. Suggest the user group how can encrypt the data with same private key no need to generate nerw private key for individual data, if one user leave the manager will update the group, but there is disadvantage that it authority dependable which cannot be trustable and the method is suggest is impossible to constructed practically[6]. BAODONG QIN suggest the efficient VO-ABE which is efficient way to allow third party (cloud server) that by using the public key transformation key which is provided by the user to transform an ABE cipher text, so it can be decrypted much more efficiently by user. Compared with the original outsourced ABE , our verified outsourced ABE not increases the user and cloud server computational cost except some non-dominant operation. Advantage over cipher text size, but disadvantage is to still need to increase the efficiency[7] By survey the method the ABE scheme is better than other scheme It provide authentication user via attribute as be select unique id, Which are properties of user to be authentication, use environment condition as IP address to access time , take attribute as Ikey (key generation) which is unique In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes. Currently, the only method that provide such policies is to by apply a trusted server for data storage and easy access control, However, if any server which storing the data is not trusted, then the confidentiality of the data will be compromised. In this paper they present a system for typical access control on encrypted data that we Attribute-Based Encryption. By using our techniques the encrypted data is kept confidential even if the storage server is not trusted. ABE is useful and it work when a user wants to be authenticated, he sends a request to the authenticator. The authenticator replies with attribute requirements. If the user owns the required attributes, he uses his attribute keys to generate a signature and sends it to the authenticator. If the signature is valid, the user is authenticated and otherwise rejected. The main goal of basic ABE schemes is to achieve anonymous authentication. They can provide least information leakage for users as well, which means that users only need to provide exactly the required “attributes” rather than a whole package of information.
Capabilities and scalablility virtualized environment of the clouds help the systems to execute the tasks in real time. The proposed technique depends on the adaptive behavior of the reliability weights assigned to each processing node. The technique uses a metric to evaluate reliability. The nodes are removed if the processing nodes fail to achieve the minimum required reliability level.

III. OUR CONTRIBUTION

In this paper I proposed a method to remove the disadvantage by using the ABE scheme to secure the data by encapsulating the data by ABE-KEM method to check the outsourced and the integrity of data, we revisit ABE with verifiable outsourced decryption (VO-ABE), and try to solve these problems. We first present a construction of VO-ABE method, which is based on an AB-KEM which is attribute based key encapsulation method, a commitment scheme and a symmetric-key encryption scheme which can be used to add verification to the outsourced decryption.and also provide the integrity at the time when receiver receive the data [7], we propose an appropriate transform for the actual secret key to achieve outsourcing the decryption.
By this method we provide authentication , integrity, and confidentiality to the data . We proposed a new algoeithm which is the combination of two algoritm of VO-ABE and KEM to secure the data and check the outsourced by using he extra instances without

increasing the computational and cipher text cost. And increase the efficiency of the whole algorithm which is best for the future implementation. Refer paper introduce verification to the outsourced decryption of ABE by adding an extra instance in the encryption/decryption algorithms, which duplicates the computation and communication overhead. Instead of two parallel instances in the encryption/decryption algorithms, we combine a hybrid encryption and a commitment together to bundle the randomness to the cipher text, so that one can verify the outsourced computation easily. Decryption is done in the normal way as performed, but the outsourced transform key is made by an appropriate method of the transform of the actual secret key with some specific properties that ensuring the secure outsourced computation. We define a verification algorithm for the receiver of the data for check the correctness of the outsourced computation. Only if the verification is passed, the data can be recovered. in the decryption algorithm. We prove with our method that we constructed that ABE scheme provide security and meets the verified the outsourced data. Our algorithm is the combination of the ABE and AB-KEM with VO-ABE[7] commitment scheme.

IV. PROPOSED METHODOLOGY

A. *Proposed Algorithm*

We proposed a algorithm by merging the two algorithm ABE and KEM , the algorithm is, the pseudo code is :

1) *Setup* attribute
2) *Key generation* generate master and public key(pp,msk,I_{key})//with AES
3) *Encrypt*(pp, m,I_{enc})
4) *Generate SK*(PP, MSK, I_{key})
5) *Generate TransformKey TK* (PK,SK,MSK)
6) *Transform*$_{out}$(PP,CT,TK) // decrypt the file again and produced CT'
7) *Decrypt*(TK,CT')
8) *Verify*(PP,CT',TK) //verify the outsourced
9) *Decrypt*(pp,CT,CT', TSK)
10) *If (TK, I_{enc})*=1 then decrypt
11) *output* m
12) *Else* error message

In our proposed method first attribute is given and key is generated by given attribute set the master and public key is formed , in their we using AES encryption algorithm to encrypt the data because it given better efficiency and result.

By using primary and masterkey sk is formed which used to generate the transform key by which ciphertext is formed.

To decrypt the ciphertext by using transform key and check the ciphertext with transform key if the transform key and encryption algorithm is match and given the output then the main file is encrypted and given the result by verifying the outsourced.

If an outsourced ABE with verification does not have a verification key (i.e., VK =∅), we refer to it as the standard notion of outsourced ABE (without verification) [8]. We denote by ABEO = (Setup, Encrypt, KeyGen, Transform, Decrypt) an outsourced ABE system. The outsourced ABE essentially works in the KEM setting, where the ABE ciphertext hides a symmetric session key. The formal definition of attribute-based KEM with outsourced decryption is exactly the same as that of ABE with outsourced decryption, except that the encryption algorithm of ABE is replaced by an encapsulation algorithm, which doesn't take a message as an input. We show that any outsourced ABE system can be simply converted to an attribute-based KEM with outsourced decryption via the following method: the encapsulation algorithm takes as input MPK and Ienc. It first chooses a random session key (message) K from M, and then computes CTIenc ← Encrypt(MPK, K, Ienc) using the encryption algorithm of the outsourced ABE. Finally, it outputs (CTIenc, K).

B. *Proposed Model*

The first step has to select list of attributes. Here , we are selecting attributes as Id, Dept, Designation and Salary where we are 0. security parameters are varied and depends on user requirements like salary > 50k or dept ="mkt" or design = "exe". Pk = id (which is unique for individual user) MK - key will be generated based on Pk with aes encryption algorithm.Put this both to two separate files just as pkfile and mkfile. call key generation process to generate sk by taking pk and mk and attribute selected based on security parameters input by user.store that in skfile. generate TK by using combination of pk,sk and mk. encryption algorithm by taking pk,M(message), attribute set and TK perform decryption algo for TKand CT and store it to CT'. put it to verification process and check its TK and CT' is matched.if yes and pass a success message or pass an error message.IT will benefit in upgrading security without taking it to t he knowledge of trespasser and will not give load on process of transferring data over cloud.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

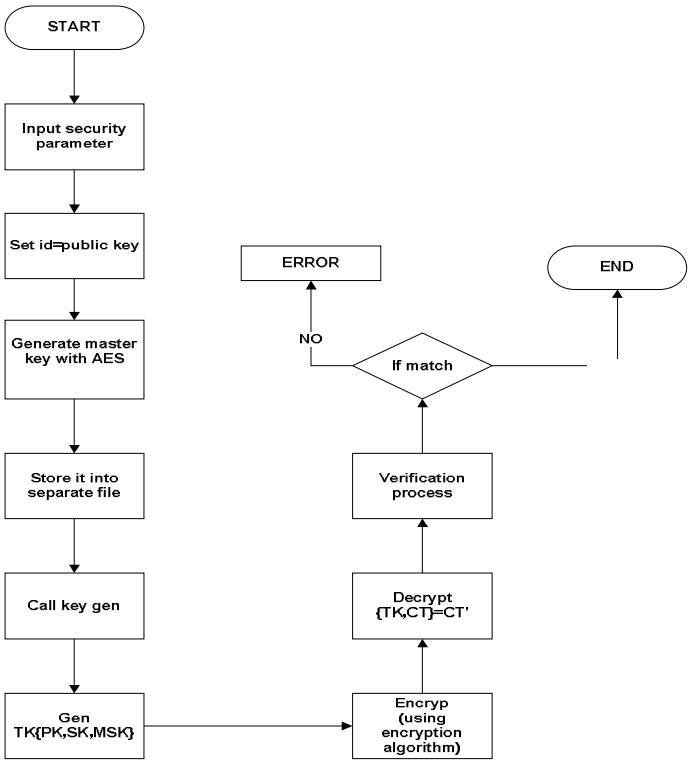


Fig 1 Flow-diagram of Proposed Algorithm

V. IMPLEMENTATION

A. *Software Specification*

For the implementation of our proposed algorithm , we will using For the implementation of our proposed algorithm , we will using java language JDK 8.0 and eclipse IDE.

For code we will be using jar to generate encryption key and cryptomat API.

Java is compatible with many of the API which is available for encryption and decryption so we can get a good result and performance with using java programming.

We implement our scheme that is ABE with Verified outsourced with KEM ,uses a laptop with 2.3 GHz Intel Core i3(second generation) and 2 GB RAM running 64-bit Windows 10 with320 GB Hard Drive.

B. *Result*

Testing of proposed algorithm is done with the references given by the SUQING LIN, RUI ZHANG, HUI MA, MINGSHENG WANG. We formed the result on two parameter that is transform time and the total execution time and the cipher text key size . the result is far better than the previous methodology. Figure shows the improvement in transform time and execution time which is upon the attribute policy of 20 to 100.

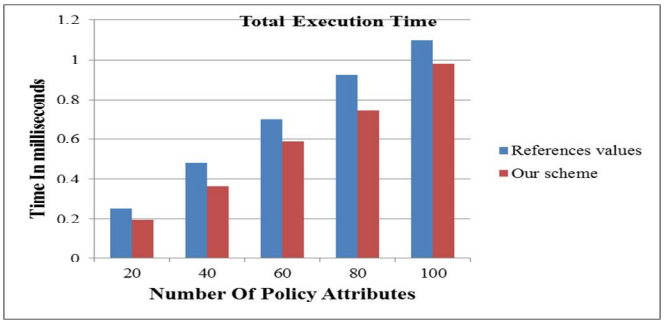


Fig 2 total Execution Time Comparison

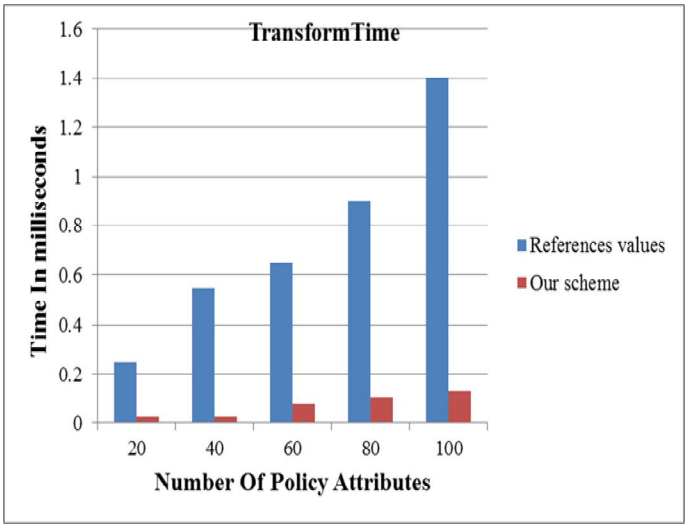


Fig 3 Total transformation Time Comparision

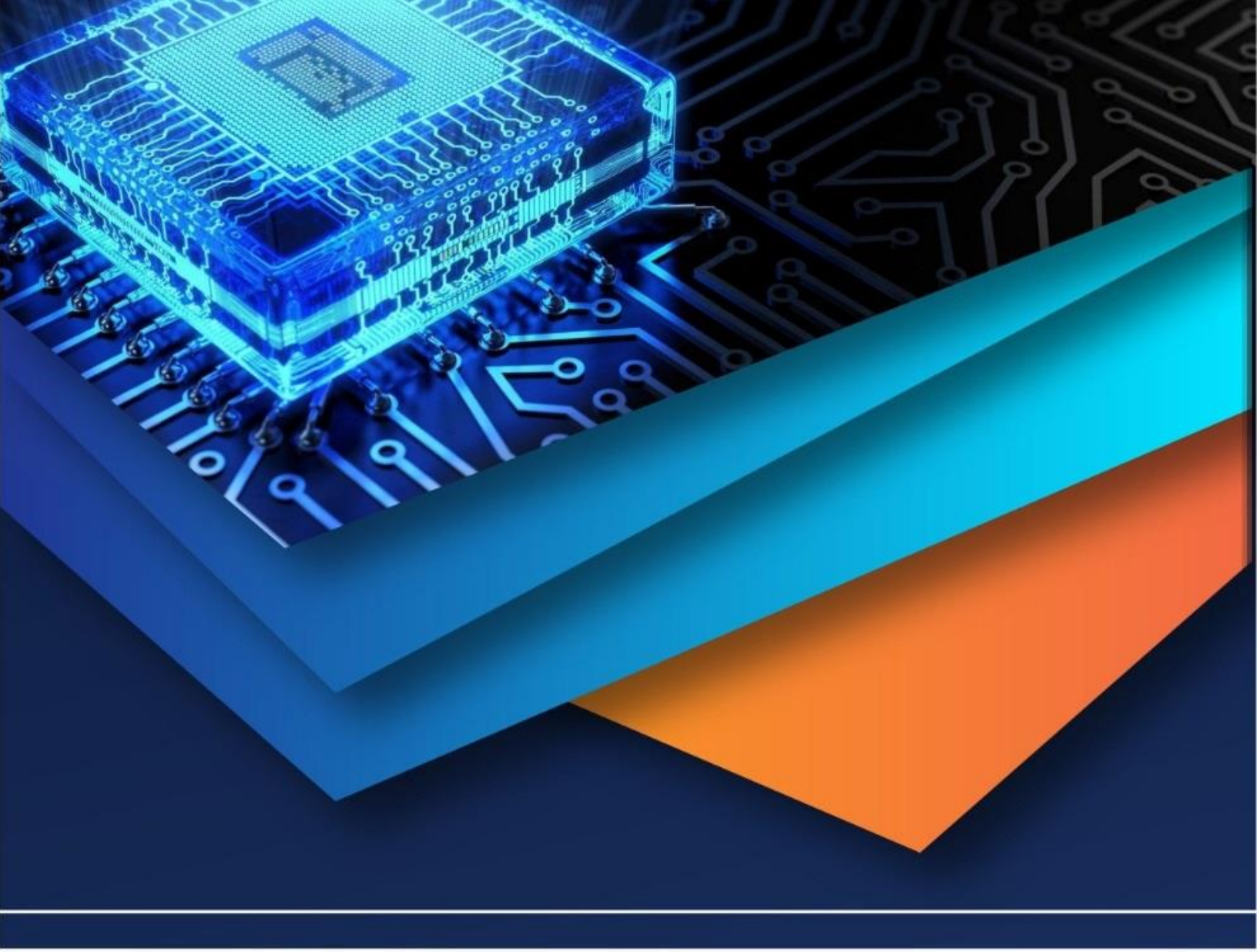
As by reducing the transform time and execution time the hence the encryption and decryption time is also decrease which provide the low computation cost while uploading and downloading the data.

VI. CONCLUSION

Using the ABE method with outsourced decryption the size of cipher text , the encryption cost and time the transformation time and the time of decrypting a transformed cipher text is decrease. In this system, encryptor and decryptor, are able to outsource their computing tasks to the cor- responding service providers respectively, to improve the computational efficiency, and they are also able to verify the correctness of outsourcing calculation efficiently by using the corresponding outsourcing verification services.(ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. In this article, we provided a formal definition and security model for CP-ABE.

REFERENCES

[1] Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption", IEEE, 201
[2] Baodong QIN, Robert H. DENG, Siqi MA,"Attribute-based encryption with efficient verifiable outsourced decryption", IEEE , 2012
[3] abha pandit, aishwarya lamture, pooja sankalp, subham dixit, tabassum maktum,"attribute based encryption with verifiable outsourced decryption"ijtra,2016
[4] Guofeng Lin, Hanshu Hong, and Zhixin Sun," A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing ", IEEE, 2017
[5] Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang,"Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption",IEEE, 2015
[6] konda reddy. guddeti and gangadhara . P," An Efficient Attribute Based Encryption Data Retrieval in Cloud ",IEEE,2017
[7] Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk," A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computsing",IEEE,2016
[8] michael miller, "cloud computing
[9] Barrie sosinsky,"cloud computing bible"
[10]]Manju Khari , Manoj Kumar,V aishali , "Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithms", IEEE, 2016.
[11] Omer K. Jasim Mohammad ,Safia Abbas ,El-Sayed M. El-Horbaty Abdel-Badeeh M. Salem ," Securing Cloud Computing Environment using a new Trend of Cryptography ", IEEE,2015.
[12] Faiza Fakhar*, Muhammad Awais Shibli," Comparative Analysis on Security Mechanisms in Cloud",ICACT,2013.
[13] B.Harikrishna,Dr.S.Kiran,R.Pradeep kumar Reddy, "Protection on Sensitive Information in Cloud -Cryptography algorithms",IEEE,2016.
[14] Lifeng Li, Xiaowan Chen, Hai Jiang Zhongwen Li, Kuan-Ching Li," P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds ",IEEE,2016.
[15] G Bhuvaneswari, Mr. K.Narayana, Erasappa Murali," Prediction System for Reducing the Cloud Bandwidth and Cost ",IJCER,2014.
[16] Hao Wang, Debiao He, Jian Shen, Zhihua Zheng ,Chuan Zhao, Minghao Zhao," Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing",SPRINGER,2016.
[17] www.wikipedia.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY