iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51058

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: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Secure Data Encryption Scheme for Cloud Computing

Abhimanyu Jarwal[1], Kamlesh Kumar[2], Ajay Kumar[3]
[1]*Research Scholar,* [2, 3]*Assistant Professor JECRC University, Jaipur*

Abstract: ***The cloud computing is the architecture in which no central controller is present due to which various breaches occurred in the network. To secure data transmission from source to destination two type of encryption schemes i.e: fully homomorphism and fully disk encryption are introduced. The fully homomorhic encryption scheme is more security and light as compared to fully disk encryption. In the paper, improvement in the fully homomorphic encryption is proposed using elliptic curve cryptography and OTP generation.***
Keywords: Homomorphic encryption, OTP, Elliptic Curve

I. INTRODUCTION

Cloud Computing is the environment which provides on-demand & convenient access of the network to various computing resources as well as services that can be available with least efficiency. The data that is stored by an organization in centralized manner can be retrieved as well as modified by the user as per the requirement. A system through which services are provided to the user by the cloud service provider as per the demand is known as a cloud. Cloud Service Provider is another name for this system that is generated based on its functioning. This system thus works on the fundaments that the cost and facilities charged to the user depend upon the services required by him. Thus, large numbers of applications are given under several topologies within this technique. Further, some new specialized services are provided by each of the topology. Cloud security is termed as the mechanism through which the network and the information being exchanged are secured from any unauthorized users. Various types of data and applications that exist within the cloud computing scenarios are secured by applying various sets of policies, technologies and controls [1]. To avail any service, security is considered to be the most important factor. Each field requires both internal as well as external security approaches. The integrity as well as privacy of a cloud is ensured through privacy measures. However, every security mechanism has certain loopholes due to which the privacy of the system is interrupted. Security is the only issue which we need to focus in the cloud computing. You actually don't know what is going on with your data, because it is stored by the third party like application and web browser. Centralized of data is the major benefit to cloud computing. When data is stored on the hard disk drive without any encryption, there are many chances of leakage of the data. When you upload your data to the cloud, there are proper encryption standard to encrypt the data and no one can take the advantage in case the data achieved is encrypted [2]. Overall conclusion is your data is secure on the cloud as compare to the local storage. The major advantage of the cloud is, you don't have to do anything yourself. Everything depends on the provider. They will provide you the security. If you think your data has been compromised, there is a service or online service for this. You can clone up the whole data offline and can analyze it.

Fully Homomorphic encryption provides the better security than full disk encryption. Unlike FDE the encryption is not applied on full disk, encryption is applied on each function. The cipher text and plain text is not related but the emphasis is on the algebraic operation that works on both of them [3]. After the invention of RSA, Rivest, Adleman and Dertouzos introduce the idea of fully Homomorphic schemes. Without providing any preliminary decryption of the operands, the data is encrypted using encryption function. The privacy homomorphism is known as the approach that collectively operates those schemes. Fully Homomorphic Encryption can be used to inquiry a search engine, not including, what is being searched. More accurately, FHE has the many properties. The whole physical disk is encrypting with physical key for the better speed and simplicity in disk firmware in the case of fully disk encryption. In case of stolen laptop it is very effective technique to protect the etc. Therefore it cannot fulfill the requirement of data protection goals in the cloud but physical theft is not the main threat [4]. Full Disk Encryption is one of the most successful ways protect our private data on laptops, tapes etc. Your data could be permanently lost when an encrypted hard drive goes bad. FDE solution comprises a number of methods for receiving admittance to the drive when a consumer can no longer authenticate. This may be a recovery key, a recovery password or an emergency log-on account. Once common with the practice, make sure that the recovery information is centrally backed up, test your recovery strategies.

Diffie Hellman was the first public key algorithm or we can say that it is symmetric key agreement ever invented. Before establishing a symmetric key, the both the two parties need to choose two numbers n and p. Let n be a prime number and p be an integer [5]. The Diffie Hellman Problem (DHP) is the problem of computing the value of p^{ab}(mod n) from the known values of p^{a} (mod n) and p^{b} (mod n). In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. For encryption or decryption of the messages symmetric key is used. We knows that Diffie Hellman algorithm is used for only key agreement or key exchange, but it does not used for encryption or decryption. Before starting the communication, secure channel is established between both the parties [6]. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

II. LITERATURE REVIEW

Haohao Zhou, et.al, (2016) proposed a queuing system within which on the basis of stochastic process, the base can be touch by the user and several resources can be requested to be used. The cloud computing system provides a shared pool of configurable computing resources. For enhancing the usage of system within stable state, a relationship amongst the utilization and stability of cloud systems is provided through this paper [7]. The effects caused by several parameters on the algorithm are also studied here. Various factors are need to be considered when scheduling is done on the real cloud such as utilization, QoS.

Huangke Chen, et.al, (2015) proposed the major concern of green cloud computing in all the fields such as industry and academia. Since the cloud computing scenarios are assumed to be deterministic and pre-computed schedule decisions, the scheduled execution will be followed [8]. Author in this paper raised this issue. For describing the uncertainty of computing scenarios, an interval number theory is also introduced by the authors. They proposed three strategies in order to improve the energy efficiency, improve resource utilization for the cloud data center. PRS is compared with the four typical baseline scheduling algorithms on the basis of the performed experiments. On the basis of the performed experiments it is concluded that the proposed method of PRS is superior to existing algorithms as it improves the performance of the data centers.

Doulamis ND, et.al, (2014) proposed that in the dispersed computing environments, the task assignment and resource selection are the essential operations as compared to grid and the cloud as they also required resources for their working. Metrics related to client satisfaction are not only the criterion to measure the corresponding algorithms for making decision. Most of the tasks are performed without breaking the requirements of quality of services on the basis of the performance metrics of the used resources. As large number of resources are used to fulfill the tasks and their utilization efficiency [9]. With the help of the proposed method the derived concepts graph partitioning are grouped together in order to minimize the time overlapping of the tasks assigned to given resources and it also maximize the time overlapping among the allocated task to various resources. On the basis of the experiments it is concluded that ht proposed method is superior to other scheduling algorithms.

Abdul Hameed, et.al,(2014) proposed a major issue in the allocation of the energy efficient resources to various virtualized ICT resources such as servers, storage disks, and networks and many more. This issue is addressed by the various research papers for improving the allocation of the energy resources in the cloud computing environment to all the application that provide success in minimizing thus issue. According to author, they searched various papers but not find any optimal solution to the above mentioned issue [10]. The main objective of this paper is to presents the major issue and challenges that are connected with energy efficient resource allocation. The presented accessible techniques in the literature are integrated on the basis of the energy-efficient research-based taxonomy.

Peidong Sha, et.al, (2016) presented a study related to the partially homomorphic cryptosystem known as RSA. An encryption system is designed here depending upon the characteristics of RSA algorithm. Initially, depending upon the availability of prime number within the values of public and private key generated during the encryption process, the discrimination of encryption system is done initially. Further, the Pascal's triangle theorem, RSA algorithm model and the inductive approaches are combined within this approach for generating new cryptosystem. The fully homomorphic encryption is completely satisfied by the new cryptosystem [11].

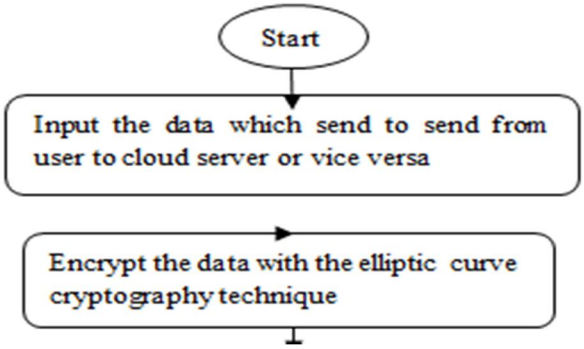
Ahmed EL-YAHYAOUI, et.al (2017) proposed a novel approach to provide security within cloud systems. This approach is known as fully homomorphic encryption since it is highly symmetric, free of any noises and is a probabilistic cryptosystem. Since it is easily applicable to the big data security, several applications related to smart computations being performed on encrypted data can be applied by this proposed encryption mechanism [12]. The issue of calculations of an over-defined system is solved by providing the security through this efficient and practical approach.

III. EXPERIMENTAL RESULTS

The Elliptic Curve Cryptography algorithm is applied in the proposed work to establish secure channels and provide mutual authentication to the systems. Amongst the two devices, only two messages are required to be exchanged by the proposed scheme. A secure channel will be generated once these messages are exchanged. As compared to the existing authentication procedure, this approach is very secure. For the authentication of users, minimal time is required. Further, the performance of mobile devices present in the network is improved. Against any kind of attack within the network, safety is provided by applying elliptic curve cryptography key exchange algorithm. The PIN key cannot be stored or exchanged within the ECC algorithm. Therefore, the network devices can be protected from any kinds of attacks by applying this approach.

A. Algorithm

Selectednode supposes user1
1. Login
2. Key generation
2.1 Enter prime numbers
2.2 Enter random numbers by client and cloud service provider
2.3 Secret key generation and secure channel establishment
3. OTP (One Time Password) generation
3.1 cloud server will set count1=0, count2=0...count5=0 for respective user at its side.
3.2 Cloud Server will request for the OTP from user 1
3.3 user1 enter (secret key+count) as OTP
3.3 server match it because server knows both secret key and count of each user.
3.3.1: count1++; // so for user 1 it will be count1=1; for remainig user their count will be still 0;
3.3.2 if (secret_key+count(x) == secret_key+count(y))
{ Access granted;
display message by server : print ("please enter the operation”);}
else{ display message by server: print(" wrong password, your login number is count1);}
4.4 clinet will enter the operation using HMAC digest
4.4.1: hmac(already generated secret key || v, file1,ver1 || sha1)
{if(ope==v)
{ server will check the file name and version;
if (file1,ver1== file1,ver1)
{ printf("file is valid");}
else { print (file is invalid, please replace the file)
}} if(ope==I) { insert new file file2 }
5. encryption/decryiton
6.data operation
7.logout;
note: // 1.at client side, user will enter prime number, random number for generating secret keys, once generating secret key user will enter otp, after inserting otp, user will enter operation(Insertion) with corresponding file name(file1 or file2).



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

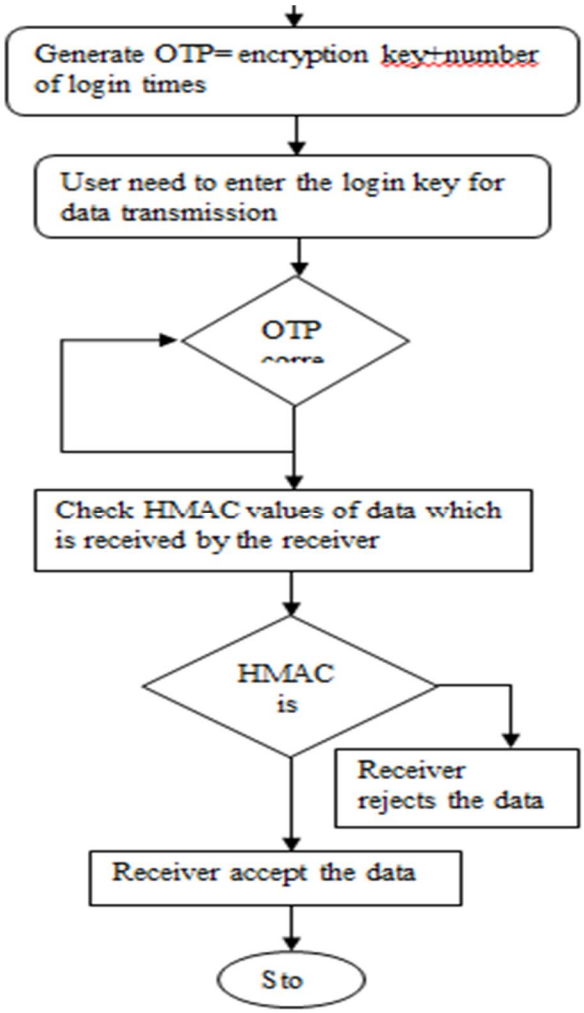


Fig 1: Proposed Flowchart

B. Experimental Results

The proposed approach is implemented in MATLAB and the results are evaluated in terms of delay, space and probability.

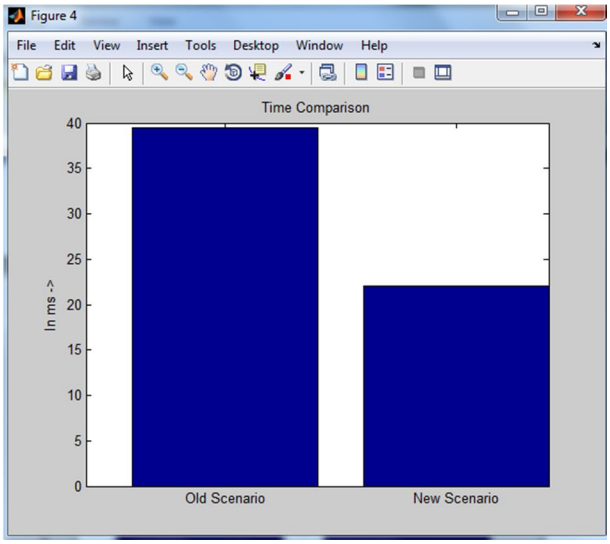


Figure 2: Comparison graph of delay

As shown in figure 2, the comparison between previous and proposed approach is shown in terms of delay. The delay in previous technique is increasing, when numbers of exchange messages are increased. In the proposed approach the delay is less due to increasing the number of message.

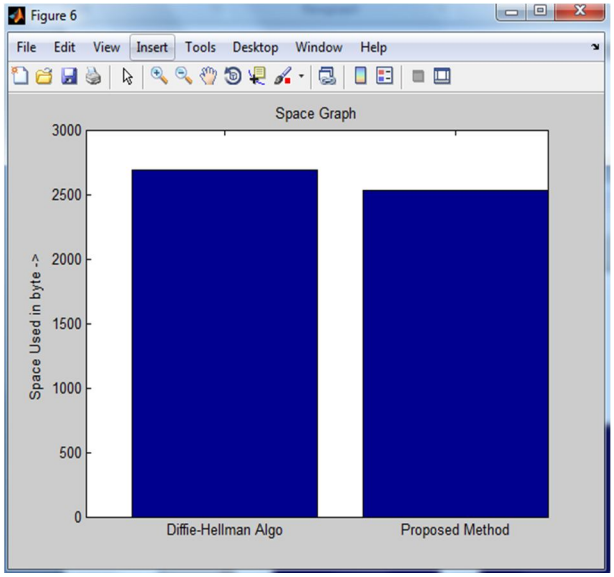


Figure 3: Comparison graph of Space

As shown in figure 3, the space utilization of existing Diffie-Hellman Algorithm is higher in comparison to the space utilization of proposed algorithm.

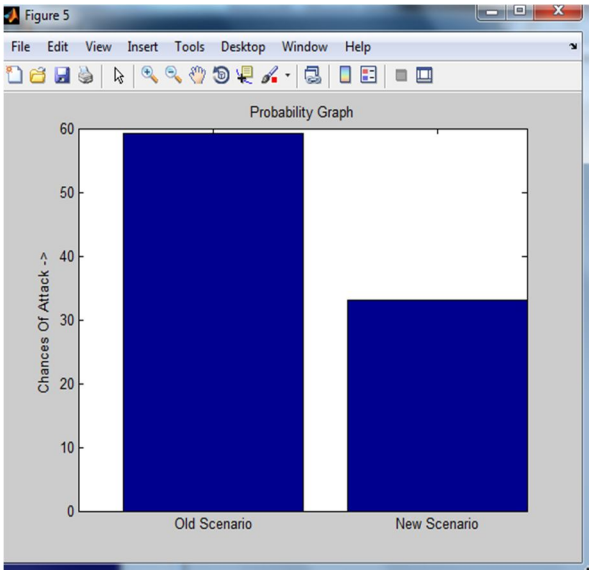


Figure 4: Comparison graph of probability

As shown in figure 4, the probability of existing scenario is higher and there is reduction in probability of novel proposed algorithm.

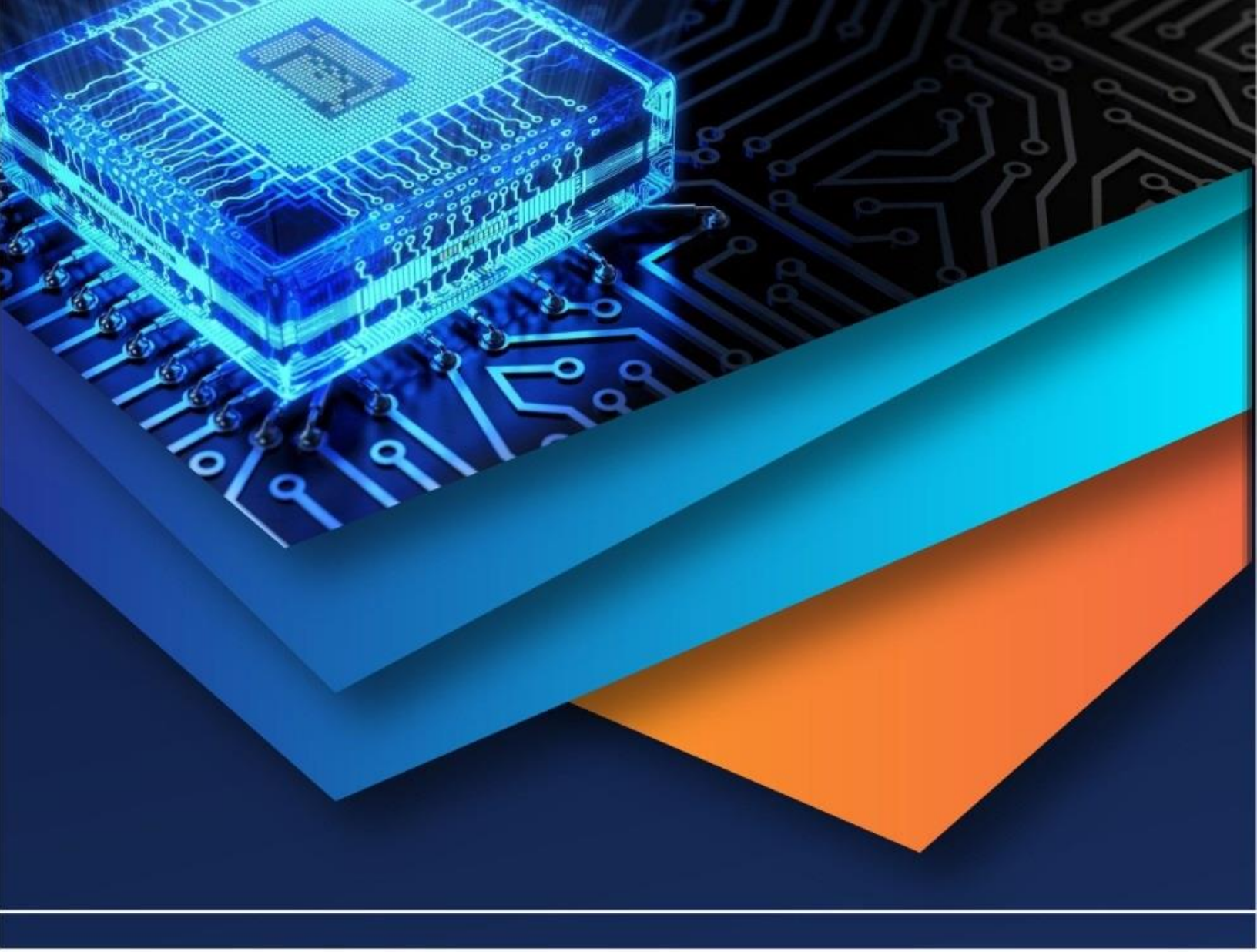
IV. CONCLUSION

In this work, we find that fully homomorphic encryption technique is more efficient than full disk encryption. But the main problem exists in fully homomorphic encryption is of key management and key sharing which reduces the reliability of the scheme. For key management and key sharing, enhancement is being proposed in the encryption scheme and enhancement is based on Elliptic Curve Cryptography algorithm and HMAC and OTP is generated on the basis of secret key generated from Elliptic Curve Cryptography algorithm. This algorithm creates session key between user and cloud.

Each time new key is generated between two before communication. This reduces the time takes place in management and sharing of keys and secure channel is established between both i.e. user and the cloud service provider. The simulation shows that proposed enhancement is more efficient and reliable than the existing one. In future we will extend this work for access control management using fully homomorphic encryption scheme.

REFERENCES

[1] Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II
[2] Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45
[3] Deyan Chen, Hong Zhao, 2012" Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, pp 647-651
[4] Young-Gi Min, Hyo-Jin Shin and Young-Hwan Bang, 2012 "Cloud Computing Security Issues and Access Control Solutions" Journal of Security Engineering, pp 135-140
[5] Simarjeet Kaur, 2012 "VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249. Cryptography and Encryption In Cloud Computing, pp 242-249
[6] Dian-Yuan Han, Feng-qing Zhang, 2012 "Applying Agents to the Data Security in Cloud Computing" International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128
[7] Haohao Zhou, Su Deng, Hongbin Huang, 2016. "Stability property of clouds and cooperative scheduling policies on multiple types of resources in cloud computing", J Supercomput volume 72, issue 46, pp- 2417–2436
[8] Huangke Chen, Xiaomin Zhu, Hui Guo, Jianghan Zhu, Xiao Qin, Jianhong Wu, 2015. "Towards Energy-Efficient Scheduling for Real-Time Tasks under Uncertain Cloud Computing Environment", J Syst Softw volume 99, issue 58, pp- 20–35
[9] Doulamis ND, Kokkinos P, Varvarigos E, 2014. "Resource selection for tasks with time requirements using spectral clustering", IEEE Trans Comput Vol. 63, No. 2, pp. 461–474
[10] Abdul Hameed, Alireza Khoshkbarforoushha, Rajiv Ranjan, Prem Prakash Jayaraman, Joanna Kolodziej, Pavan Balaji, SheraliZeadally, Qutaibah Marwan Malluhi, Nikos Tziritas, Abhinav Vishnu, Samee U. Khan, Albert Zomaya, 2014. "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems", Computing, volume 5, issue 6, pp- 1–24.
[11] Peidong Sha, Zhixiang Zhu, "THE MODIFICATION OF RSA ALGORITHM TO ADAPT FULLY HOMOMORPHIC ENCRYPTION ALGORITHM IN CLOUD COMPUTING", Proceedings of CCIS, 2016
[12] Ahmed EL-YAHYAOUI, Mohamed Dafir ECH-CHRIF EL KETTANI, "A verifiable fully homomorphic encryption scheme to secure big data in cloud computing", 2017, IEEE



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY