iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1095

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 :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

An Improved Security Framework for Cloud Environment using ECC algorithm

Silki Jain[1], Abhilasha Vyas[2]
[1]*Research Scholar* [2]*Asst. Professor, Department of Computer Science & Engineering Patel College of Science & Technology, Indore*

Abstract: ***Cloud computing is a very popular technology in the field of delivering services to their user. It is elaborating for providing benefits to consumers. Configuration, storage, sharing are all possible in cloud environment. User outsources their data to store on cloud. In this paper we are computing on the security approaches used for increasing the level of security for the data. Purpose is to prevent from attacks, intruders and sniffing of message. Mitigation approach used in this paper works on HMAC (Hashed message authentication code), ECC and MD5. A resource pool of digitization with increasing data rate is observed. Security establishment on the basis of access control, authentication, confidentiality, integrity and encryption is achieved in this work. Experimental analysis of proposed solution concludes that very low overhead has been observed for upload and downloads service time.***
Keywords: Data security; ECC; HMAC; cloud computing; MD5

I. INTRODUCTION

On the basis of cloud based application, cloud computing provides resources to there users. The combination of virtualization, distributed and parallel computing defines the cloud computing. On demand services and resources are accessed by user in an effective manner. But needed browser for accessing services. Cloud provides with various cloud based models and services which are used by user. Architectural design of cloud environment is such that it serves with the services. Using cloud computing saves the expensive investments in software's and hardware's and user can access them without purchasing.

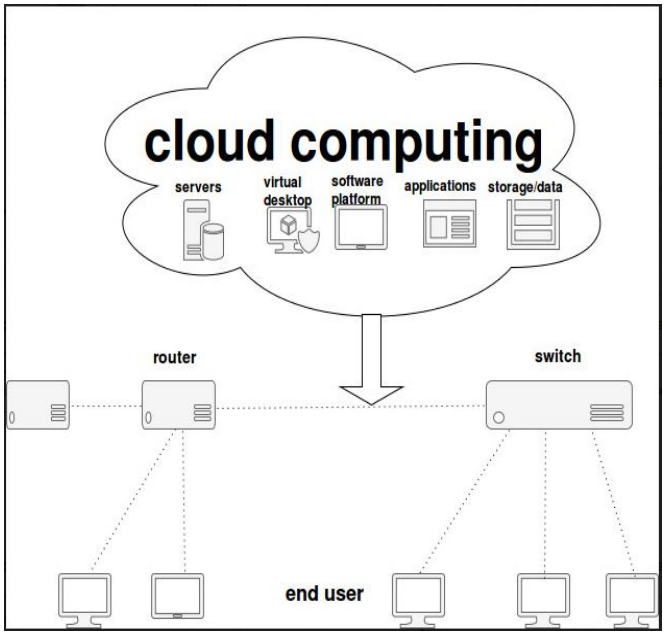


Figure 1: Cloud Computing

A. Features Of Cloud Computing

Cloud computing serves with several features which are mentioned below:

1) *Pay as per use :* Cloud computing provides with the cost effective services because purchasing of resource is very costly and an individual can not own that much of cost. Pay as per use service is provided by cloud where user have to for what he used and does not need to but whole architecture.

©IJRASET (UGC Approved Journal): All Rights are Reserved

2) *Sharing of Resources:* If one entity is using the resource and other entity have to wait for the release of that resource, this type of issue arises when there is no sharing of resource. Cloud computing provides with the feature of sharing resources where number of user can use the resource at the same time with no issue.
3) *Scalable Feature:* Because of the performance cloud is considered as the scalable model. With the increase in number of user. Its performance does not decrease.

B. Cloud Services

Cloud provides services to user in the following manner :

1) *Software-as-a-Service:* It is a complete package which serves with software which are pre installed and configured. All the technical issues are handled in SaaS. Its package involve applications like social networking sites, email etc.
2) *Platform-as-a-service:* It is the top layer of IaaS and serves with platform provided with software, hardware. This service have only basic technical knowledge. Its package involves database, server etc. and mainly used by developers for developing applications.
3) *Infrastructure-as-a-Service:* It is the basic layer which servers with the infrastructure, where user can also install any software or operating system. Its package involves virtual machine, storage, server, network etc. It is popular among researchers and developers.

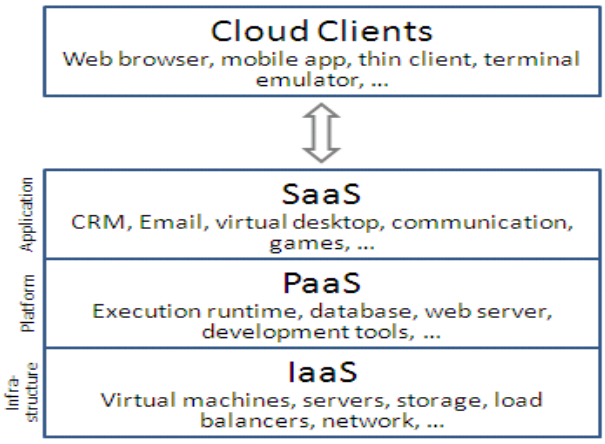


Figure 2:Service layers of cloud

C. Deployment Models Of Cloud

Deployment model describes the cloud into four category that is public, private, hybrid and community cloud.

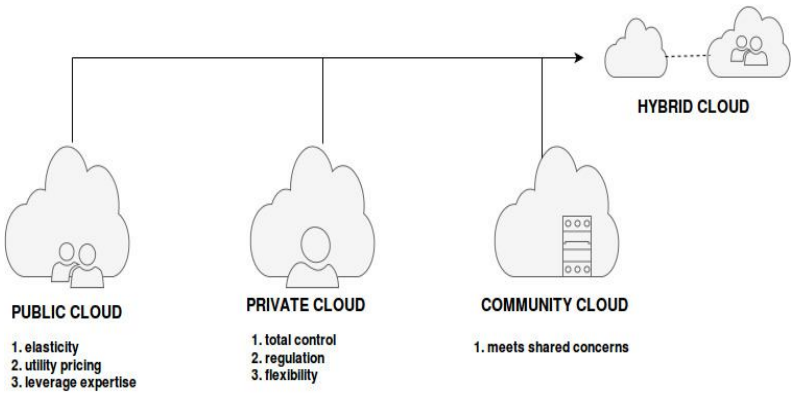


Figure 3: Types Of Cloud

1) *Public Cloud:* Public cloud is publically exposed where anyone can access services of cloud. It has the feature of multi-tenancy which means having an shared environment to store data. Location of data center on cloud can be anywhere depending upon the

©IJRASET (UGC Approved Journal): All Rights are Reserved

location of service which are provided by cloud. Cloud service management manage services of cloud. Cloud service provider provides hardware and ensure for its working. Cloud service provider provides full set up of network on the basis of service level agreement.

2) *Private Cloud:* Private cloud is only for the specific organization. It has a single tenancy feature which means only the specific organization can use the data stored on cloud. Location of data center is inside the network of organizations. Cloud services can be managed by that organization who owned it and its administrator manages it. Organization has to purchase physical server for building private cloud. It is expensive, managing its hardware and network is also expensive
3) *Hybrid Cloud:* It is the combination of both public and private cloud. Here services can be accessed public for the public cloud and services can be used by particular organization for private cloud. It serves with both multi-tenancy and single-tenancy feature.
4) *Community Cloud*: It is used internally and externally with the cost effective feature and is beneficial for user, it is called community cloud.

II. RELATED WORK

C. Wang et al. In[1] proposed about the cloud computing services and outsourcing of data on cloud by the data owners which results in providing low cost and easy to use and maintenance. Three entities are there in cloud architecture, these entities are individual, cloud service provider and third party auditor. Third party is an intermediate between user and provider.

B. Samanthula et al. In[2] introduces about data security, its maintenance, its confidentiality, authentication and integrity. Security is important because it protects data from intruders. Encrypted data is outsourced over cloud but faces issue of efficiency by user.

B. Shereek et al. In[3] addressed about cryptographic algorithm which works on the basis of keys. RSA is used by author on attacks for security purpose, this cryptography uses public key.

C. Y. Chen et al. In[4] stated the scheme called Fully Homomorphic Encryption which solve some essential issues in cryptography. The issue is elaborated by Rivest. FHE is used for preserving confidentiality of any system.

Prakash G.L et al. In[5] proposed about security challenges faced in cloud environment. Also stated that it reduces the unwanted time and deals with attacks.

Table 1: Comparative Table

S.No.	TITLE	AUTHOR	PROPOSED WORK	YEAR
1.	Secure and Dependable Storage Services.	C. Wang, Q. Wang	proposed about the cloud computing services and outsourcing of data on cloud by the data owners.	2012
2.	A secure data sharing and query processing framework.	B. Samanthula, Y. Elmehdwi	Introduces about data security, its maintenance, its confidentiality, authentication and integrity	2015.
3.	Improve Cloud Computing Security Using RSA Encryption.	B. Shereek	Addressed about cryptographic algorithm which works on the basis of keys.	2014
4.	A Novel Cloud Computing Algorithm of Security and Privacy.	C. Y. Chen	Stated the scheme called Fully Homomorphic Encryption which solve some essential issues in cryptography.	2013
5.	Data Encryption and Decryption Algorithms using Key Rotations for Data Security	G. L. Prakash, M. Prateek	Proposed about security challenges faced in cloud environment.	2014

©IJRASET (UGC Approved Journal): All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

III. ROBLEM DOMAIN

For achieving data security, privacy of the information and data integrity plays an important role. The emerging technology cloud is very beneficial and helpful for the growth of any business. Resources can be shared through it, reduce cost, enable access of service so as to fulfill the requirements of user. In multi domain it has many uses but lacks in the domain of security. Issue observed in this work is the authorization, access control, storage, integrity and data privacy as the major factor of security issue in cloud computing. Observation concluded that integrity and data security comes up with the main issue of security and which will lead to suffers with difficult problems. Data privacy involves issues of key management and access control. The study of existing solution explore that confidentiality and data integrity are major concern for secure data communication and storage. Bhandari[1] et. al. proposed security framework based on RSA cryptographic algorithm and HMAC integrity approach. They observe need of index builder layer before encryption and after chunk preparation to improvise distribution and integration time. They do not modify encryption or description process instead they change the chunk distribution and storage policy.

IV. SOLUTION DOMAIN

Here, complete encryption process has been replaced by ECC cryptosystem to overcome computation and memory overhead. The concept of ECC cryptosystem comes from the study global sign on RSA and ECC. They address that RSA keys and its recommended size is increasing with rapid rate to maintain desire cryptographic strength. Rising in key strength also raise computation overhead during encryption. Here, ECC has observed as alternative for RSA due to overwhelming strength. Both encryption algorithms are asymmetric and share public key cryptography policy. However, ECC offer reduced overhead over RSA, because ECC can offer same level of security strength at much smaller key size.

A. The complete system is elaborated below;

1) Initially user needs to create own profile on cloud application and register with personal credentials and IP address.
2) Afterwards, user can upload file on cloud server using upload services. Upload service call upload feature and convert file into byte format.
3) HMAC –MD5 module will create and store the message digest of complete information file to manage data originality.
4) Chunk preparation and index builder is no need to use in ECC algorithm. So it can save lots of computation effort cause due to chunk preparation and index building.
5) All unique chunks will be forwarded to ECC block to convert human readable data into cipher text.
6) Upload service distribute all ciphered chunk to different storage location.
7) When user attempt to download any file it calls download service.
8) Download service lookout requested file and proceed for decryption.
9) Recalculation of HMAC-MD5 will perform to evaluate originality of requested message.
10) Comparison of stored HMAC-MD5 with new will help to evaluate originality of message. If it found same value then forward to download otherwise consider as suspected file and raise error.

The complete discussion is also represented in flow chart form shown in figure 4 and figure 5.

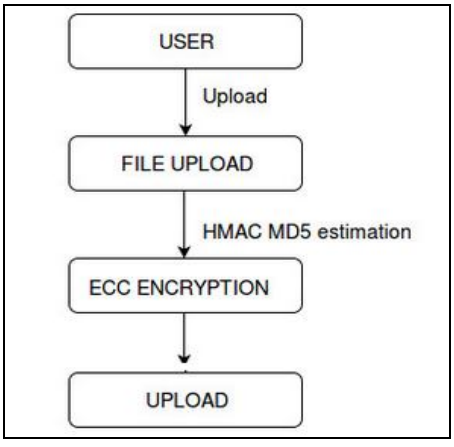


Figure 5: Flowchart of Upload Service

©IJRASET (UGC Approved Journal): All Rights are Reserved

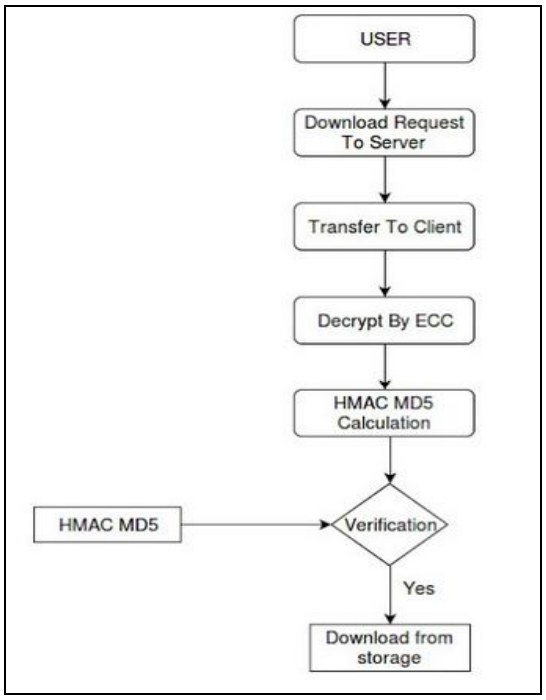


Figure 6: Flowchart of Download Service

V. RESULT ANALYSIS

The complete solution has been deployed as public cloud application and evaluated on basis of different file type with variable data size. Performance of proposed solution is evaluated on basis of computation time overhead of ECC algorithm with RSA and Improved RSA. A graph to demonstrate overall performance is shown below;

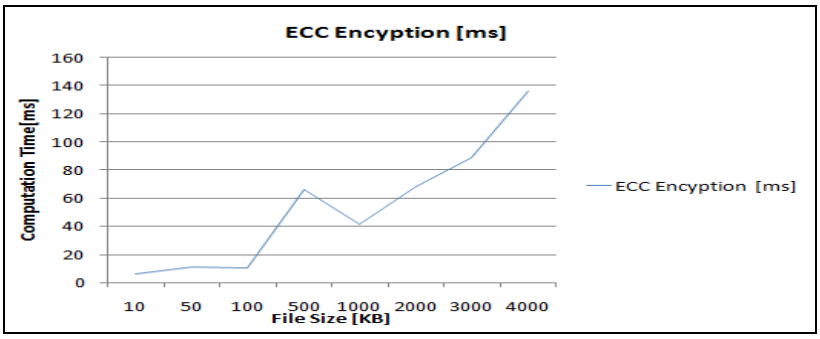


Figure 7: Performance evaluation of ECC encryption of proposed solution

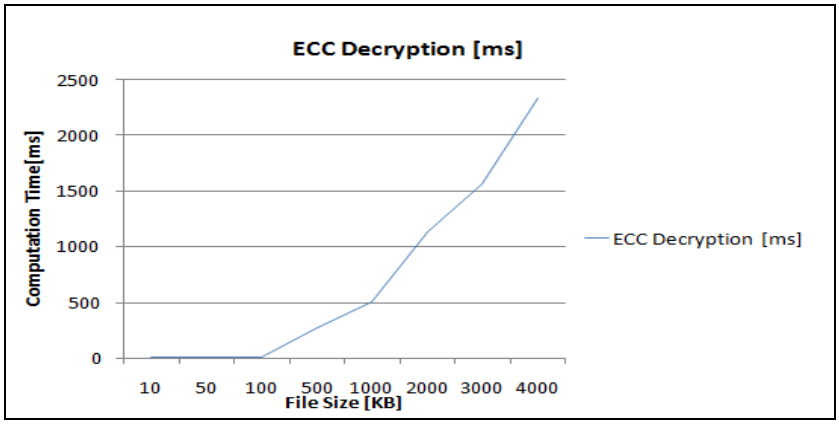


Figure 8: Performance evaluation of ECC decryption of proposed solution

©IJRASET (UGC Approved Journal): All Rights are Reserved

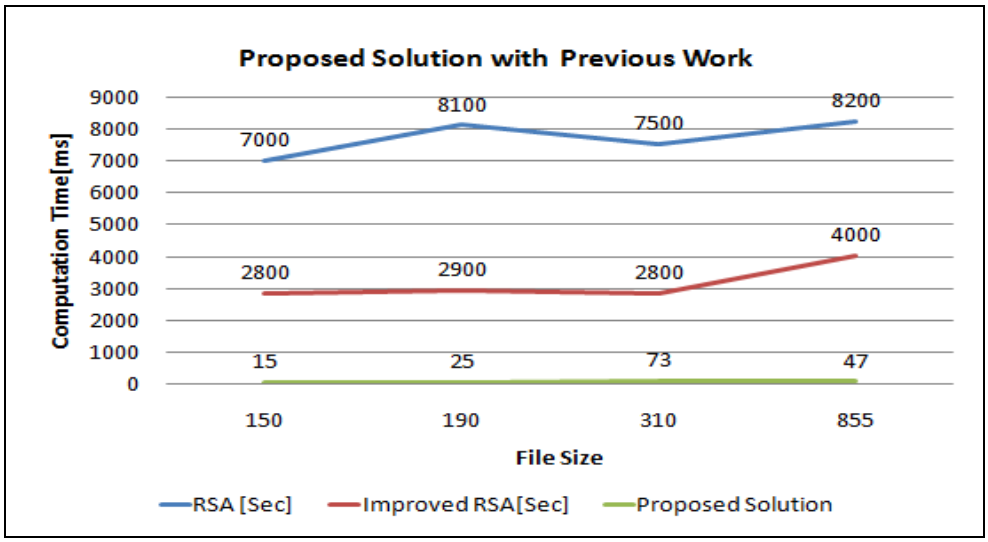


Figure 9: Overall Performance Comparison

IV. CONCLUSION

Security feature is demanded in the work, because the existing system only deals with the confidentiality and integrity feature. With this authentication, data access, privacy are also key feature which should be maintained and using HMAC with MD5 it is achieved in the work. The mitigation approach gives the uploading and downloading of file using techniques of ECC, HMAC and MD5. Study and analysis of key parameters on the basis of result is done. Work suggest about uploading and downloading of file in an secure manner.

A. The complete work concludes with certain logics which are listed as below;

1) With respect to previous work Improved RSA perform well than conventional RSA and consume very less computation time.

2) In improved RSA Computation overhead is stable for small file size but raise with high value for 855 KB [Nearby 1 MB] file size.

3) Saturated but very low encryption overhead is observed with respect to raise in file size in proposed solution. A very small computation overhead has been observed for file less than 100 KB size.

4) Exponential raise in computation has been observed for large file size input. Highest 136ms encryption time has been examined for 4MB file size.

5) Exponential raise in decryption similar to encryption has been observed with respect to raise in file size. A very small computation overhead has been observed for file less than 100 KB size. Highest 2.5 sec encryption time has been examined for 4MB file size.

6) Overall performance examination conclude that proposed solution perform much better than conventional RSA as well Improved RSA.

7) Study on different file size address that overall time of proposed solution is just 47ms where RSA consume more than 4000 ms to accomplished task.

8) Performance evaluation also gives strength to decision of removal of chunk preparation which create unnecessary load on upload and download service.

The complete work conclude that proposed solution perform much better for encryption as well decryption during upload and download service with respect to proposed solution.

This paper mainly focuses on security on the content of data which will be secure using important parameters.

REFERENCES

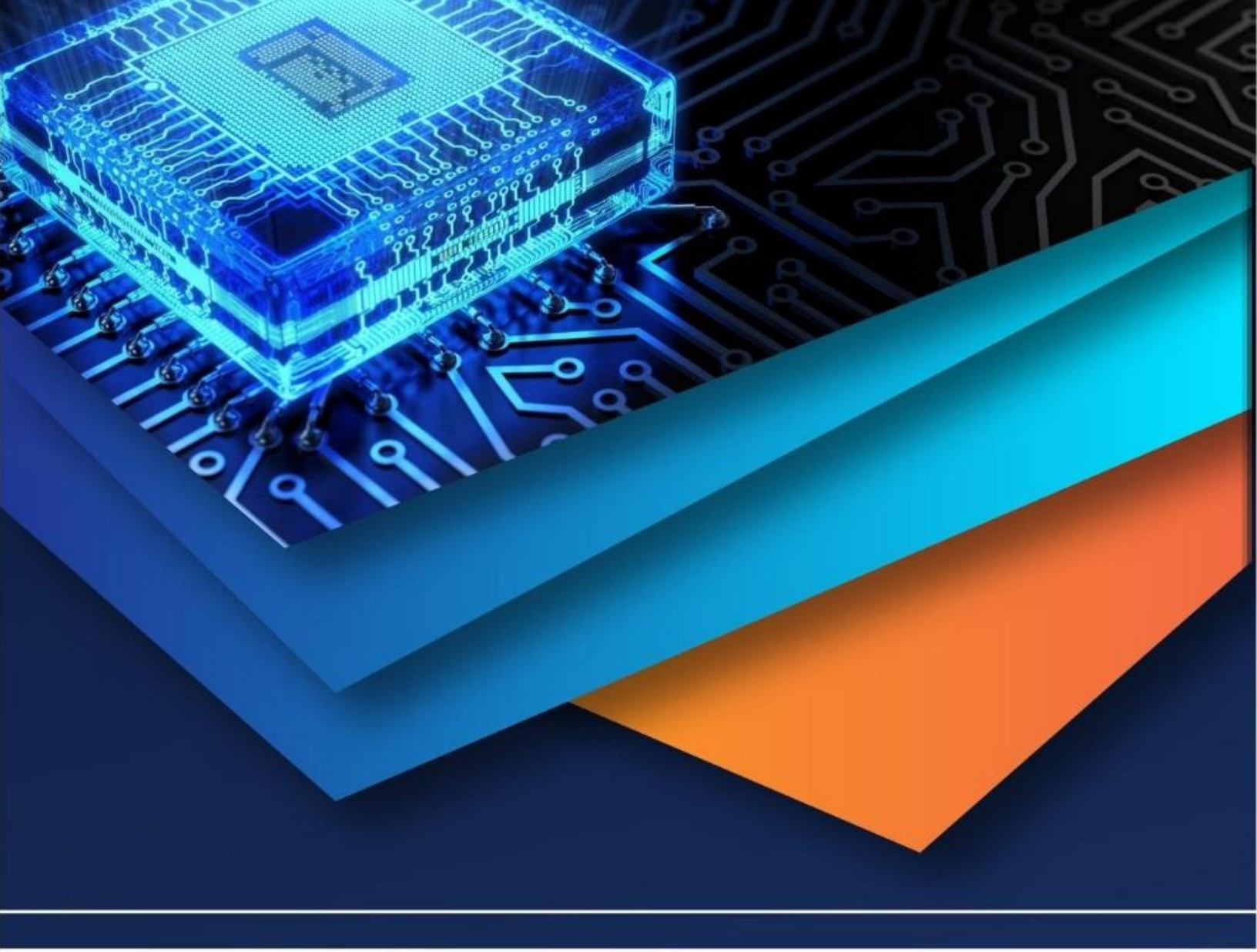
[1] C Akshita Bhandari, Ashutosh Gupta, Debasis Das, A framework for Data Security and Storage in Cloud Computing', International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016

[2] [2] B. Samanthula, Y. Elmehdwi, G. Howser and S. Madria, 'A secure data sharing and query processing framework via federation of cloud computing', Information Systems, vol. 48, pp. 196-212, 2015.

©IJRASET (UGC Approved Journal): All Rights are Reserved

[3] [3] B. Shereek, 'Improve Cloud Computing Security Using RSA Encryption With Fermats Little Theorem', IOSR Journal of Engineering, vol. 4, no. 2, pp. 01-08, 2014.
[4] [4] C. Y. Chen and J. F. Tu2, 'A Novel Cloud Computing Algorithm of Security and Privacy', Hindawi Publishing Corporation:Mathematical Problems in Engineering, 2013.
[5] [5] G. L. Prakash, M. Prateek and I. Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal Of Engineering And Computer Science vol. 3, issue 4, pp. 5215-5223, April 2014.
[6] [6] Chor B,Gilboa N,Naor M, 'Private Information Retrieval by Keywords', Report 98-03, Theory of Cryptography Library, 1998.
[7] [7] Arora, Rachna, Anshu Parashar, 'Secure user data in cloud computing using encryption algorithms', International Journal of Engineering Research and Applications Vol. 3, pp.1922-1926, 2013.
[8] [8] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on Vol 62.2, pp 362-375, 2013.
[9] [9] D. Zissis and D. Lekkas, 'Addressing cloud computing security issues', Elsevier Journal of Future Generation Computer Systems, vol. 28, pp. 583592, 2012.
[10] [10] F. F. Moghaddam, M. T. Alrashdan and O. Karimi, 'A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments', Journal of Advances in Computer Network, vol. 1, No. 3, Sep. 2013.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)