iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** V **Month of publication:** May 2018

**DOI:** ttp://doi.org/10.22214/ijraset.2018.5268

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 V, May 2018- Available at www.ijraset.com*

# Security Architecture to Enhanced Privacy of Communication and Storage in Cloud Environment

Kavita Nagar[1] Narendra Kumar Sahu[2]
[1, 2]*Lecturer-CSE Indore Women's Polytechnic College*

***Abstract:*** ***Security of data is the vital goal in all the field of cloud. It does not depend upon the location of the data where the data is kept, it can be in any of the layer may in presentation layer or it may in application layer, the big thing is the security. Many technologies are associated with cloud computing, cloud computing provides with the cloud security and solves the arising issues which are coming at the time of cloud security. Hybrid approach is used using RSA and ECC cryptographic solution with MD5 to maintain integrity.***
***Keywords: ECC; MD5; Cloud environment; RSA***

## I. INTRODUCTION

All the resources are provided by cloud computing to the cloud based applications. Cloud computing is the combination of parallel computing, distributed computing and virtualization. Resources can be accessed in a reliable way and an effective manner on demand. Using browser services can be accessed, which defines the capability of cloud for there user to provide services. Different cloud models and services are used. The cloud environment is designed in such a manner with the architecture to possess and serves with the services. Software and hardware can be accessed is the best part of cloud computing because it saves investment on costly devices.

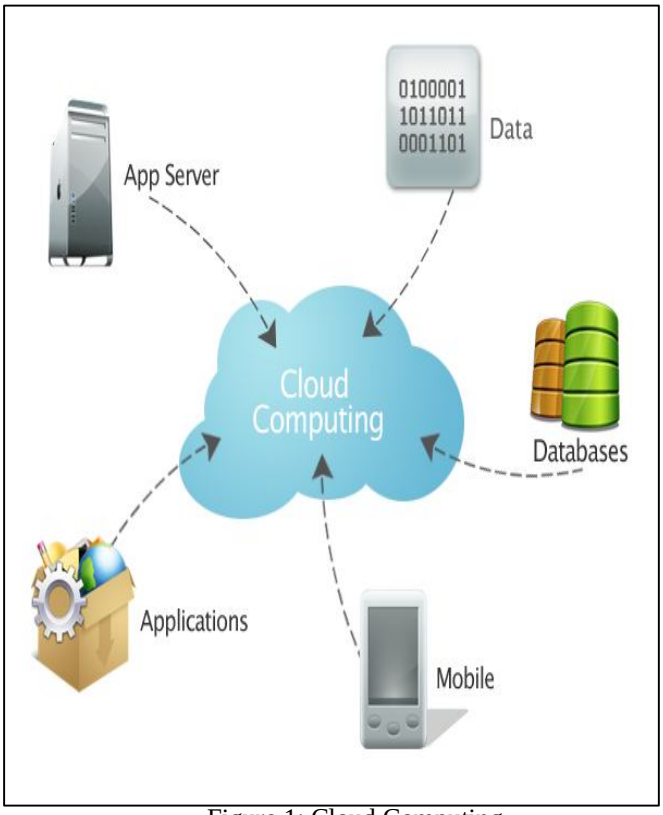


Figure 1: Cloud Computing

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

*A. Features of Cloud*

*1)* Shared resources is the issue in case when one entity is holding the resource then in that case other entity have to wait for that resource to get free from the first entity and not to be used by other entity.

*2)* Cloud is scalable and also the cloud model is considered as a scalable model because of its performance. Its performance does not degrade with the increase in user.

*3)* User can demand for any resource, it's up to user which varies with the requirements. Consumption of resources depends upon the user demand, but if he demands more than the requirement then it's not compulsory to use them all.

*4)* Cost is the major concern, so for every resource cost exists. Here, user does not need to buy whole architecture but have to pay for the service and resource which he demands and using. Means pay as per use.

*B. Services of Cloud Computing*

Cloud computing is a sharing based technology help to share infrastructure, platform and application in form of services. It provides three types of services which are listed below:

*1)* Software as a Service[SaaS]

*2)* Platform as a Service [PaaS]

*3)* Infrastructure as a Service [IaaS]

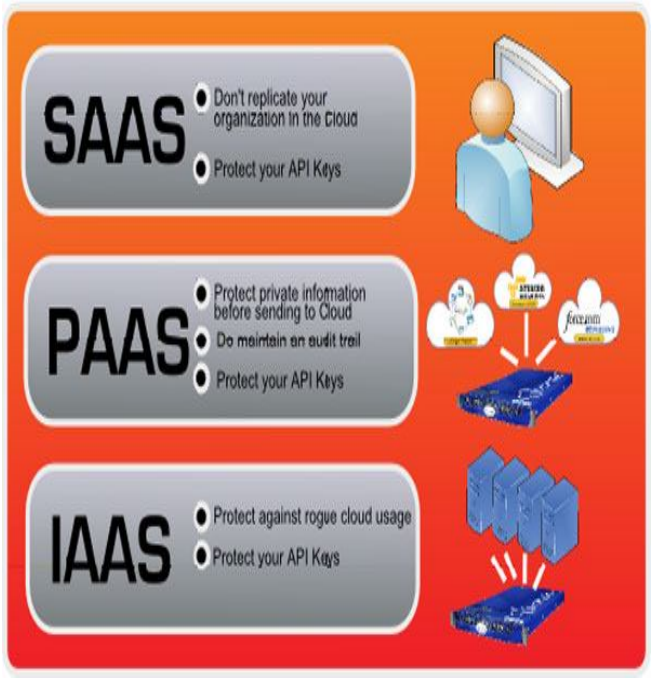



Figure 2: Cloud Computing Services

## II. RELATED WORK

Akashdeep Bhardwaj et. al. In[1] introduces that RSA suffers with issue of heavy computation and memory overhead due to high range key. The study of work and RSA cryptosystem has certain overhead issues which is RSA algorithm is based on concept of public key cryptosystem, demands key distribution before encryption and decryption process. It causes extra overhead to maintain confidentiality. Improved RSA is based on conventional RSA concept. So, it also suffers with all such issues which can be overcome by ECC algorithm.

Bhandari et al. In[2]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. So, strength of encryption cryptosystem is unchanged along with its dark side also.

Miller et al. In[3] address that existing work uses basic HMAC algorithm which can be improved by replacing HMAC-MD5. Study of recent works concludes that HMAC-MD5 can provide more reliable and fast integrity computation over simple HMAC.

## III. PROBLEM STATEMENT

Data privacy in cloud refers to get trust of user due to involvement of third party servers for storage and processing. Cloud users always look data verifiability and privacy before subscribing any cloud services. Minor information leakage may cause big damage on subscriber brand image and lead for loosing of business services. So, cloud security has become sensitive matter for multiple cloud applications. Study of existing work and previous security solutions observe that it lies on four requirement denotes as CIAT are listed below;

*A.* Privacy
*B.* Confidentiality
*C.* Integrity
*D.* Availability
*E.* Traceability

## IV. PROPOSED SOLUTION

Solution proposes an efficient framework to achieve strong secure communication and storage on cloud server. 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.

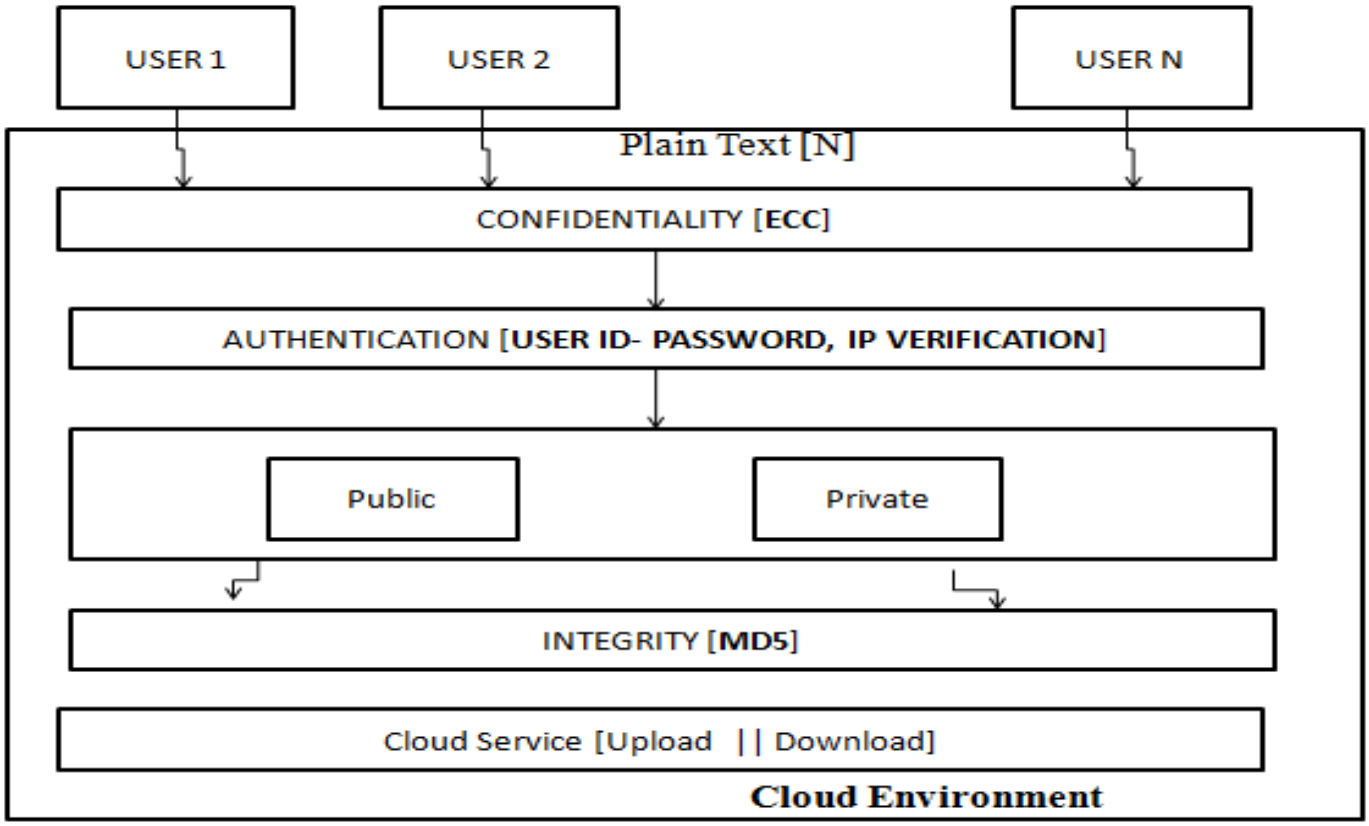



Figure 3: Architecture of Proposed Solution

*A. Salient Features of Proposed System*

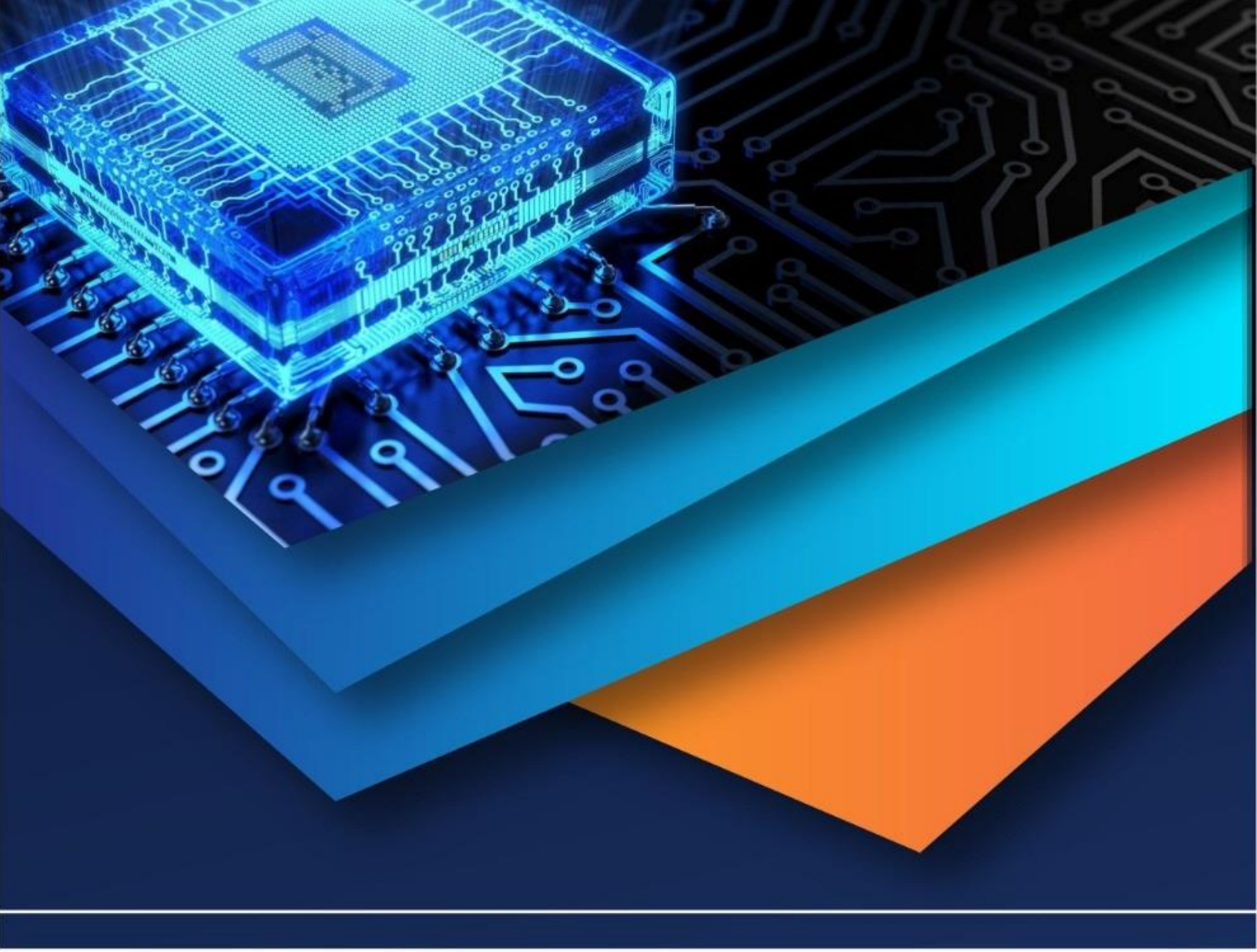
*1)* Proposed System consist an authentication mechanism to classify different security level for external login and internal login.
*2)* Internal login is a step where user can try to get access from Intranet without using public network. Here, there will be choice for user to decide the level of security.
*3)* Low level security option will only implements password authentication.
*4)* External login is a high level authentication scheme where password authentication step would be completed followed by one time password authentication step.
*5)* After authentication step, the message digest is generated.
*6)* The complete communication has been encrypted by ECC and message digest algorithm.
*7)* High level of security is achieved by applying such secure algorithm along with access control policies like RBAC and ABAC which can be understood as Role based access control and attribute based access control.

## V. CONCLUSION

Proposed solution is described in this chapter. Initial stage in development is the study of system which conferred the abstract for the proposed solution. Traditional development went into dark side of development cycle which takes toward misunderstood development. These types of issues can be overcome through technique of object oriented software development. Implementation view, its description, classes, methods used and packages are all described in this implementation phase. It has been concluded that security is the essential part which is achieved using cryptographic techniques.

## REFERENCES

[1] Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastry "Security Algorithms for Cloud Computing" In proceeding of International Conference on Computational Modeling and Security (CMS 2016) 2016.
[2] C Akshita Bhandari, Ashutosh Gupta, Debasis D, "A framework for Data Security and Storage in Cloud Computing", International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 1-7.
[3] Miller V Use of "Elliptic curves in cryptography. Advances in Cryptology"—CRYPTO '85, Lecture Notes in Computer Science, vol 218. Springer, pp 417–426 [22] Ronald Krutz, Russell Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing" Wiley Publishing 2010.
[4] 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.
[5] B. Shereek, "Improve Cloud Computing Security Using RSA Encryption WithFermats Little Theorem", IOSR Journal of Engineering, vol. 4, no. 2, pp. 01-08, 2014.
[6] C. Y. Chen and J. F. Tu2, "A Novel Cloud Computing Algorithm of Security and Privacy", Hindawi Publishing Corporation: Mathematical Problems in Engineering, 2013.
[7] 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
[8] ChorB,GilboaN,Naor M, "Private Information Retrieval by Keywords", Report 98-03, Theory of Cryptography Library, 1998.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY