IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.8, August 2020 E-ISSN: 2347-2693

Hybrid Cryptographic Solution to Overcome Drawbacks of RSA in Cloud Environment

Rupal Yadav[1*], Kaptan Singh[2], Amit saxena[3]

[1,2,3]Dept. of Computer Science & Engineering TIEIT Bhopal, India

[*]*Corresponding Author: rupalyadav41@gmail@gmail, Tel.: +91 9685233507*

DOI: https://doi.org/10.26438/ijcse/v8i8.5660 | Available online at: www.ijcseonline.org

Received: 16/Aug/2020, Accepted: 21/Aug/2020, Published: 31/Aug/2020

Abstract— Cloud Computing is the technology, which is growing more and more in the area of information technology. It is a big platform to deliver services to user. It provides with the benefit of storage, configuration, resources and sharing and all this is possible in cloud environment. Data is outsourced by the owner to store it on cloud because they have to serve there user at every possible stage. Presented work establishes security approach to secure and enhance the security of data at every step. Purpose of proposed work is to prevent from intruders and attackers and from sniffing messages. Proposed work is implemented using hybrid system (RC6+AES) and MD5 to calculate integrity. Using essential measurements like integrity, confidentiality, encryption, authentication, and authorization security in achieved in presented work.

Keywords— Data security; AES; RC6; MD5; cloud computing

I. INTRODUCTION

A vast pool of resources that serves with on-demand services called as Cloud Computing. Bulk amount of data is stored in cloud environment with providing bulk resources and services to consumers. Security authentication policies are discussed in this paper for the improvement of better security.[1]

Talking about Cloud Computing, it is very convenient to use and easy to access. It serves with advantages and disadvantages too, advantage of flexibility and reduced cost with a very big disadvantage of security is the challenge for IT sector. Cloud computing deals with the big concern of privacy and security because of loss of data and third party dependency. Attackers can attack on data at the time of data transformation in cloud, which is a big risk to handle. By using security measures most of the security concerns can be reduced but then also security is not completely provisioned.[2]

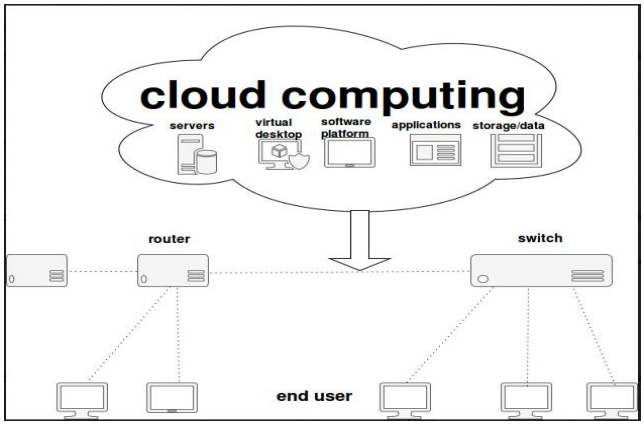

Fig.1. Cloud Computing

Security Policies in Cloud:

- *Availability:* Hardware maintenance is important for proper functioning of every operating system. Availability of resource at the time of requirement is very essential, if resources are not available then will lead to event like disasters. Availability of resources provides safety from loss of data.
- *Authentication:* Authentication cannot be ever changed, it is used for the purpose to maintain security using valid identity and password. Authentication is a medium through which user communicate with system. It is used to manage risk of security.
- *Confidentiality:* Confidentiality and privacy are equivalent to each other in term of security. Information is secured if confidentiality is achieved. Confidentiality most importantly secures the message from delivering it to wrong person. Rights to access data are in the hands of only authorized person.[3]
- *Integrity:* Accuracy is integrity, where data alteration and data transformation is not possible by unauthorized person. At the time of transmission of data, data is altered, this activity is performed by unauthorized person. In this activity, data is deleted or error is created.

II. LITERATURE SURVEY

Bhandari et al. In[1] proposed about the outsourcing of data by the data owners to cloud. Many owners outsource there data on cloud which provides a cost-effective service with simple, easy and less maintenance. He introduces about asymmetric key cryptosystem and explores solution for the need of security in cloud. Author used RSA cryptography algorithm and with it, uses index builder technique to improve the performance. Moreover, for establishing integrity HMAC is used. The below figure

demonstrate the work in picture format, shown in figure 2.1

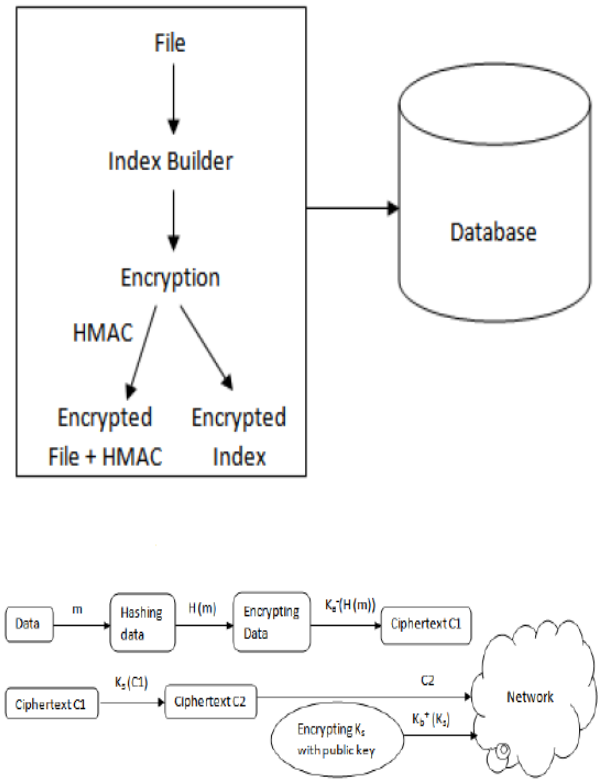

Fig.2. Existing framework for recommendation system

III. PROBLEM STATEMENT

Data integrity and privacy are the major concern of security of data and act as an important aspect in multiple domains, but face the challenging issue of security. Important parameters of security in cloud computing are storage, access control, privacy, authorization and integrity.

- *Detailed Problem Statement:*

The four requirements that are needed in work is denoted as CIAT:

1. *Data Confidentiality*
2. *Data Integrity*
3. *Data Availability*
4. *Data Traceability*

Privacy and Confidentiality are one in the same thing that assures that access of information can be possible by the authorized user. Ensuring that information will not leak at the time of storage or at the time of transmission. Originality of information is also an important aspect at the time of delivering of information and is possible by data integrity. [4]

Existing work consumes more time and more memory, which is overcome in this work. Also they divide the data in chunks for further process which requires more time.

Below table shows, security threats which is described in full description.

Table 1. Comparative Table

Title	Author	Year	Existing Work	Gap Area
A secure data sharing and query processing framework via federation of cloud computing	B.Samanthula,Y. Elmehdwi, G. Howser and S. Madria	2015	Described about security maintenance of data and protecting data from intruders.	Efficiency issue, while encrypting data using private key it fails and shows error.
Improve Cloud Computing Security Using RSA Encryption WithFermats Little Theorem	B. Shereek	2014	Proposed about public key cryptography algorithm using RSA , with the advantage of providing security.	Only works for large prime number.
A Novel Cloud Computing Algorithm of Security and Privacy	C. Y. Chen and J. F. Tu2	2013	Author used FHE strategy for solving issues of cryptography. It works on privacy of data.	No decryption is required on encrypted data.
Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System	G. L. Prakash, M. Prateek and I. Singh	2014	Worked on security challenges in cloud. Deals with security attacks and reduce time.	Only worked on security measures.

Table 2. Security threats and there description

S.No.	Security Attacks	Description
1.	Replay Attack	In this attack, attacker holds the information and after time delay it resends the packet information.
2.	Repudiation	Information and services are claimed to be refused by the attacker.
3.	Identity Spoofing	Identity of server, node or client can be killed or misused by the attacker in this attack.
4.	Tampering	Alteration and fabrication of information by the attacker is called tampering.
5.	Viruses and worms	Some source code are used by the attackers.
6.	Man in the Middle	Interruption in the communication which leads to involvement of third party.
7.	Eavesdropping	Reading and listening of information at the time of communication.

IV. PROPOSED SOLUTION

Proposed solution concludes the efficient framework for strong and secure storage and communication of cloud server. Encryption process in this work is performed by AES cryptosystem because it lowers the computation and memory overhead. RSA size is increasing and with the increase in key size computation overhead increases, this is the reason why hybrid system (RC6+AES) is used in the proposed work, it overcomes the observed overheads of RSA. Security level and strength is better in RC6+AES with smaller key size.

Complete study shows that hybrid system is better alternative of RSA, which provides with better security strength with minimal computation overhead and memory overhead. Proposed work uses MD5 to achieve integrity of data to form more stable and robust solution.

Solution proposed deals to reduce time and memory consumption, which is the drawback of existing system. Existing system does not divides the data into chunks that is established in presented work. Proposed solution is the improved version of existing work where data is encrypted using AES and then is uploaded, integrity is achieved using MD5 and after it RC6 is applied on that integrated data for encryption.

V. SYSTEM ARCHITECTURE

Proposed Architecture shows that n number of user will login to cloud application. Cloud provides user with many service like upload and download of file. After login, using authentication and access control service, user is authenticated. Authentication is checked by validating user's id, password and IP address.

Now, integrity is calculated using MD5 to digest message. Hybrid system is used for maintaining confidentiality and encryption of message at every end. At last, user can download the requested file through download service.

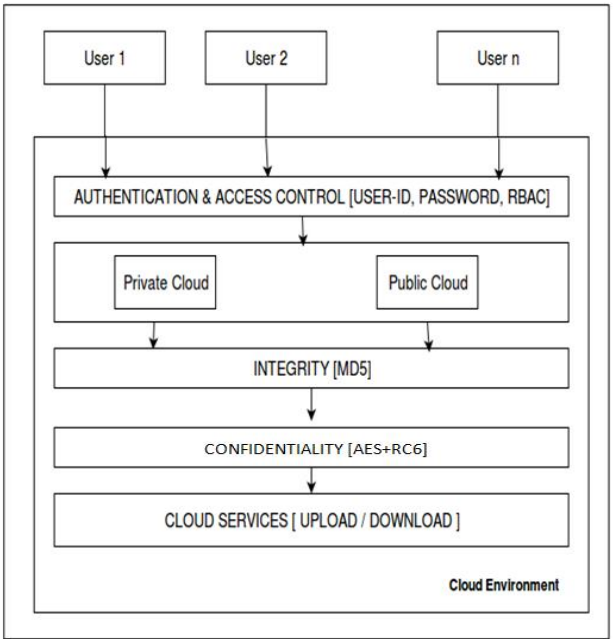

Fig. 3. Proposed Architecture

VI. RESULT

Result of the complete work describes achieving confidentiality of work using hybrid system, which is the combination of RC6 and AES. Comparison of the proposed work with the existing work is accomplished in this section.

Existing work is explained in below table:

Table 3. Existing Work

Packet Size (KB)	RSA	IRSA	AES
150	7.0	2.8	1.5
190	8.1	2.9	1.6
310	7.5	2.8	1.7

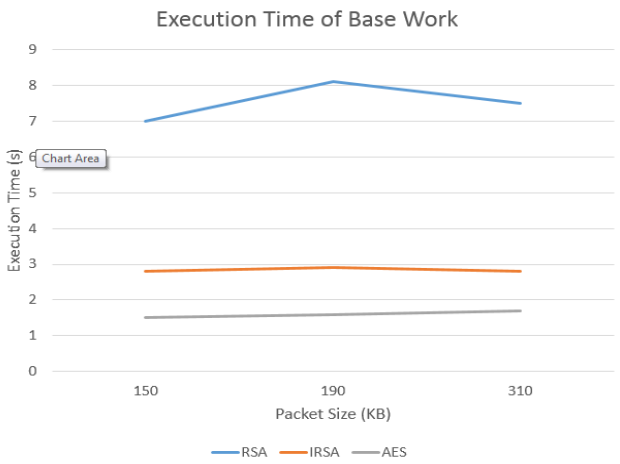

Fig.4. Existing Work

Table 4. Proposed Work

Packet Size (KB)	RC6 + AES
150	1.3
190	1.5
310	1.6

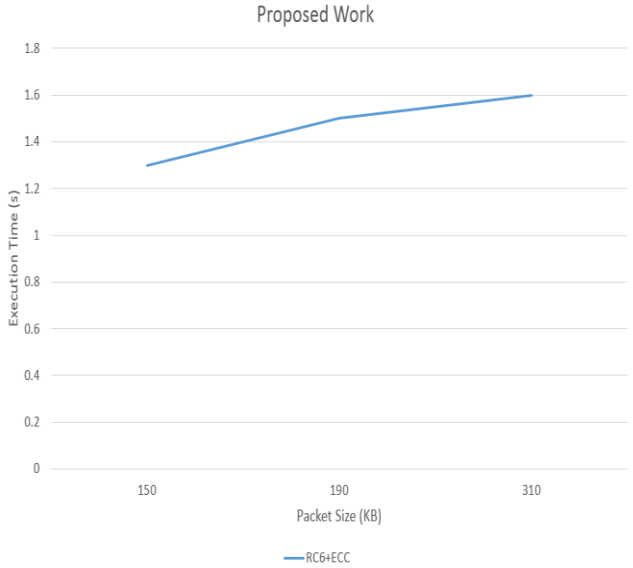

Fig.5.Proposed Work

Table 5: Comparison of Work

Packet Size (KB)	RSA	IRSA	AES	RC 6 + AES
150	7.0	2.8	1.5	1.3
190	8.1	2.9	1.6	1.5
310	7.5	2.8	1.7	1.6

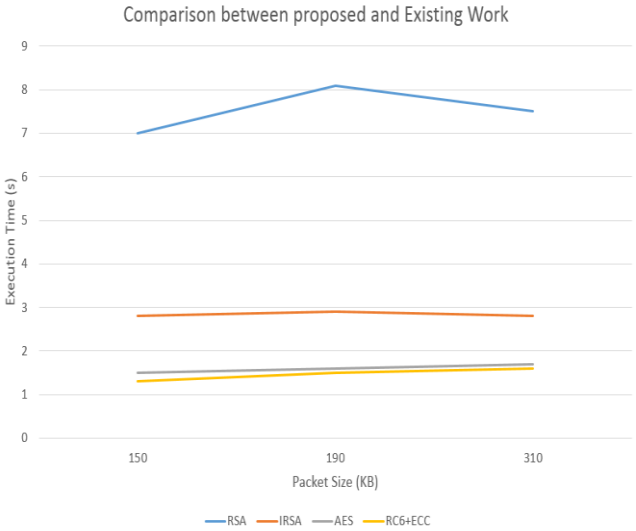

Fig.6. Comparison of Existing work and Proposed Work

VII. CONCLUSION

In proposed work security is a big demand because of achieving features like access control, authentication, confidentiality, integrity and privacy. It is performed using hybrid system which is the combination of RC6 and AES. MD5 is used for file uploading and downloading service by checking integrity. Existing work only deals with confidentiality and integrity. Study analysis is done based on key features.

Results of the proposed work in theoretical way show the upload and download of file in a secure way.

REFERENCES

[1] 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), pp. **1-7**, **2016**

[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**.

[3] B. Shereek, "Improve Cloud Computing Security Using RSA Encryption WithFermats Little Theorem", IOSR Journal of Engineering, vol. **4**, no. **2**, pp. **01-08**, **2014**.

[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] 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] ChorB,GilboaN,Naor M, "Private Information Retrieval by Keywords", Report 98-03, Theory of Cryptography Library, 1998.

[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] Wang, Cong, "Privacy-preserving public auditing for secure cloud storage", Computers, IEEE Transactions on Vol **62**.2, pp **362-375**, **2013**.

[9] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Elsevier Journal of Future Generation Computer Systems, vol. **28**, pp. **583-592**, **2012**.

[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**.

AUTHORS PROFILE

Miss Rupal Yadav received the B.E. degree in Computer Science and Engineering from Truba institute of Engineering and Information Technology, Bhopal, India, in 2015 and she is currently pursuing the M.E. degree in Computer Science and Engineering from Truba institute of Engineering and Information Technology, Bhopal, India. Her research interest includes cloud security, cyber security.

Mr.Kaptan Singh received the B.E. degree in Computer Science and Engineering from University Institute of Technology, Barkatullah University, Bhopal, India, in 2005 and the M.E. degree in Computer Science and Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, in 2012. He is currently pursuing the Ph. D.

degree in Computer Science and Engineering from Maulana Azad National Institute of Technology, Bhopal, India. He is an assistant Professor at department of Computer Science and Engineering in Truba institute of Engineering and Information Technology, Bhopal, India. He published 06 research paper in various international journal. His research interest includes the cyber forensic, e-mail forensic, Security in Internet of Things, Cyber Security.

Mr. Amit Saxena received the B.E. in Computer Science and Engineering in 2002 from UIT, GGU, Bilaspur and Master of Technology in Information Technology in 2006 from SOIT, RGPV, Bhopal with First Division. Currently, he is pursuing Ph. D. in Computer Science and Engineering. He is working as Head in the Department of Computer Science and Engineering Truba institute of Engineering and Information Technology, Bhopal, India. .His Domain of Research includes Machine Learning, Cloud Computing, Computer Networking and Wireless Communication. In recent times, he had taught subjects like Operating Systems, Software Engineering and Project Management, Computer Networks, Network Security and Advanced Computer Networking at both UG and PG levels. He had published more than 65 research papers in various international and national Journals and Conferences of high repute.

