International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 29th Jan 2019. Link :

http://www.ijiemr.org/main/index.php?vol=Volume-08&issue=ISSUE-01

Title: **HYBRID CRYPTOGRAPHIC MODEL TO ACCOMODATE STRONG SECURITY TO CLOUD ENVIRONMENT**

Volume 08, Issue 01, Pages: 247–252.

Paper Authors

NIDHI RAGASE ,ANGAD SINGH

NRI Institute of Information Science &Technology, Bhopal M.P,India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

HYBRID CRYPTOGRAPHIC MODEL TO ACCOMODATE STRONG SECURITY TO CLOUD ENVIRONMENT

[1]NIDHI RAGASE ,[2]ANGAD SINGH
[1]Research Scholar, Department of IT, NRI Institute of Information Science &Technology, Bhopal M.P,India
[2]Associate Professor, Department of IT, NRI Institute of InformationScience &Technology, Bhopal M.P ,India
[1]ragase.nidhi1410@gmail.com, [2]angada2007@gmail.com

ABSTRACT

The growth of internet makes it most promising and significant part of this world. The cloud computing technology helps to provide integrated approach for organizing and managing services, infrastructure and resources into strategic and proper way. Cloud applications provide convenient method for resource pooling, infrastructure sharing for public and private environment. Open nature and common environment makes public network vulnerable, which leads to make cloud prone for several security threats. Thus, work observes that security is primary requirement to maintain trust and authenticity of information and services. This research work observes the security gap in existing solution in terms of confidentiality, authentication and integrity with access control scheme and proposed improved security policy with advance cryptographic model. Proposed work presented that, symmetric key RC6 is used to maintain confidentiality with creating keypool, this form multikey RC6 and store chunks in Map Index with id. ECC is used then for the purpose of strong encryption and decryption.

Keywords: Keypool; chunk file; multi key RC6; MD5; ECC; BLOWFISH

1. INTRODUCTION

This work observes that cloud environment is good source to outsource data and integrate external provider with existing applications. In any application, data plays a key role, so data is very responsible and important element for cloud environment. Since geographical location plays very important role to expand the scalability of application, cloud providers interconnect multi located resources and applications with each other. Security is very important phenomena to keep data, resources and services private and inaccessible from unauthorized access. Researchers address that cloud user faces problem to use sensitive information in cloud environment, which is deployed using public infrastructure. Lots of effort has been invested to explore various algorithms to achieve security level in cloud applications. Furthermore, cloud hosting providers give lots of space and services to host cloud applications, they may be susceptible due to low security awareness. They required lots of security enhancement for cloud applications and platforms. The complete phenomena observe the need to enhance the level of security into cloud environment. It also address that a separate cloud model should be developed to provide a proper secure and safe environment for cloud applications. Hybrid cloud services must understand secure weak points of private cloud services and public cloud services. Moreover, they must support a way of resolving the security threats. They must provide a secure authentication system for hybrid cloud services. Therefore, hybrid cloud service provider must understand secure weak point for private and public cloud service and they must support suitable security services to hybrid cloud service users. The purpose of this research work is to explore the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

benefits and disadvantages of cloud. The research works explore the need of security into cloud communication and strongly address that privacy and authentication are major concern to establish trust on cloud application. The purpose of this research work is to establish strong faith of user along with reliable performance.Another way, security is not functional requirement in old days but it becomes very important to maintain privacy and trust of user on service providers. Cloud computing is mainly based on public infrastructure and internet services. Third party and unknown resources involvement make it vulnerable for various security threats, Opponents and attackers may use public infrastructure to compromise the communicated information or affect the performance by degrading the service level. All such susceptible situation creates huge motivation to develop an advance level security model to provide safe and secure communication environment

2. RELATED WORK

Khushbu Jakhotia et al. In[1] described about issue in maintaining trust with third party and this has been continued in cloud. Author proposed solution to get over from this kind of issue; an architecture is designed to monitor the generated cloud services because it verifies the originality of data. System auditing is reduced by third party auditor, so uncertainty of audit trust is reduced. AES is used to encrypt data and also to retrieve and store data on cloud server.

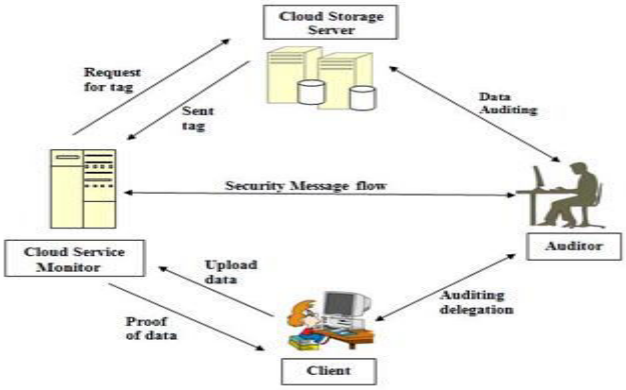


Figure 1: Existing Architecture [1]

TABLE 2.1 COMPARATIVE TABLE

AUTHOR	TITLE	SUMMARY
Babitha.M.P, K.R. Remesh Babu [2]	Secure Cloud Storage Using AES Encryption	Data encrypted in this approach used AES and then uploaded it on cloud. For avoidance of unauthorized access, short message service is used.
Teddy Mantoro, Yosep Lazuardi [3]	SMS Based Home Appliance Security Approach Using ROT 13, RC4 and RSA Algorithm	Analyzed comparison of speed time while encryption and decryption using algorithm RC4 and RSA, and obtained outcome as RSA is 50 % faster when compared to RC4 algorithm in terms of encryption.
Hyun-Suk Yu, Yvette E. Gelogo, K J Kim [4]	Securing Data Storage in Cloud Computing	Explained about infrastructure of cloud and its management, where all the data storage, infrastructure and architecture is managed by cloud

3. PROBLEM STATEMENT

Cloud computing establish their access through public networks, security issues like privacy, trust, authenticity , information security, authorization, access controls becomes essential challenges for developers. In order to overcome these challenges, various algorithms are implemented with cloud computing applications to get best approach. Today, security becomes indispensable concern and required separate attention for cloud computing environment. This research works consider this issue on primary mode and try

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

exploring algorithms and their limitations to observe and analyse security solutions and vulnerabilities for scope of improvement. This research work proposed advanced cryptographic model in terms of confidentiality, authentication and integrity with access control scheme.

Traditional AES is the issue identified in existing work, as AES works on symmetric key algorithm so only one key is shared for encryption and decryption process and key compromising issue raises, which invited attacker with removing cipher text and loosing originality of data. Key compromising issue centralize the problem of integrity, availability and confidentiality. The attacked data turns into modified, edited, or deleted data, which is harmful and is of no use for the user.

4. SYSTEM ARCHITECTURE

Issue of existing system is overcome in this approach with generating and implementing multi key RC6. Keypool is generated by storing chunks in Map index by naming as chunk_id and key_id with encrypting them using ECC. After it, MD5 technique is used to calculate integrity of data. ECC encrypt the stored key_id and MD5 encrypt chunk_id. Before this process, BLOWFISH algorithm is used, which encrypt the complete plain text.

Step by step description of complete architecture:

1. Encryption of Plain Text:
   The complete plain text is encrypted using BLOWFISH algorithm. After that, the encrypted data is divided into even and odd chunks.
2. Key generation:
   Take input from user. After that, it is divided into chunks and number of keys are generated for keypool, Kp = K1, K2…K6. This generates multiple key. Keypool resolves the issue of key compromising and also issues in traditional symmetric key.
3. Encryption Process:
   For encryption data is divided into chunks and these chunks are stored as chunk_id in Map Index. Multi keys, which are generated, are applied on these chunks. Using ECC and MD5, chunks are encrypted and then stored as cipher text. MD5 also calculates integrity of data to maintain its accuracy.
4. Decryption Process:
   For decryption process, similar approach will work.

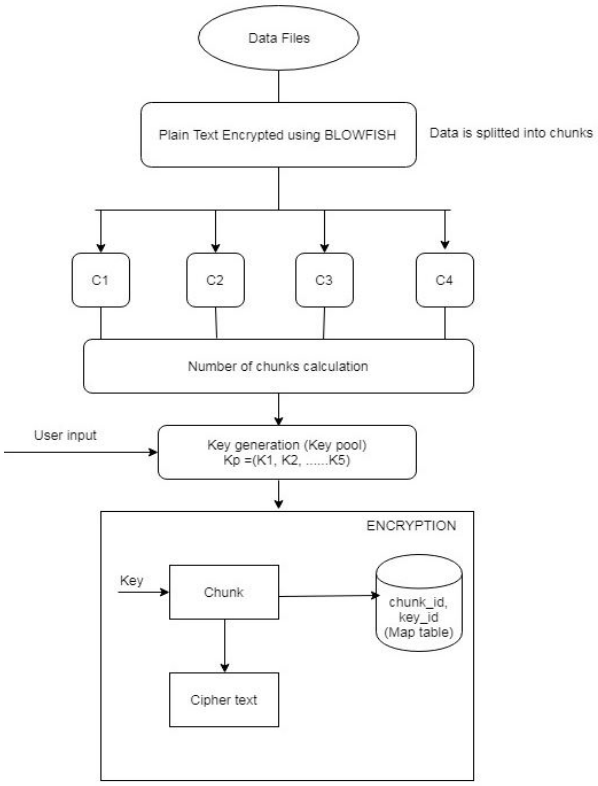


Figure 2: System Architecture

5. RESULT ANALYSIS

Result analysis of the complete work diagnose the mitigated issue of existing work by stimulating the problem with evaluating proper technique for it.The proposed system is an application that uploads the file and security is maintained by strong cryptographic algorithms like

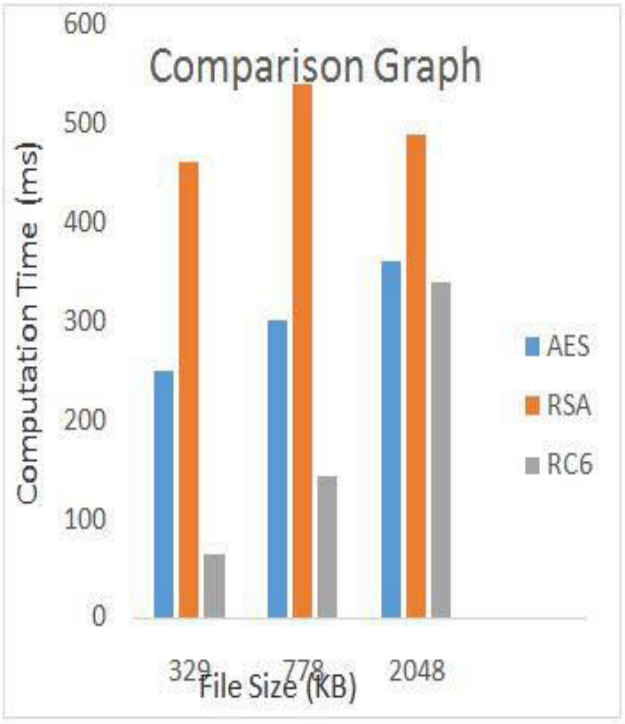
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

RC6,Blowfish and ECC different result tables and comparison graphs are used here to show the strong security of this cryptographic model.

File Size (KB)	AES (ms)	RSA (ms)	RC6 (ms)
329	250	462	64.964
778	300	541	142.9208
2048	360	488	340.228

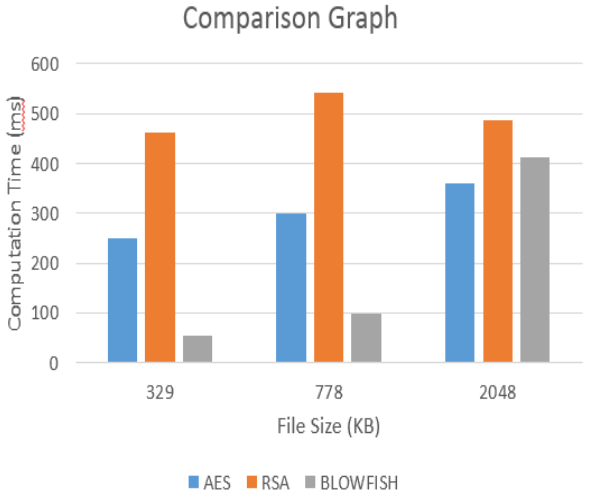
Table 5.1 Comparative result analysis between AES and RSA and RC6 encryption algorithm

Graph 1:comparison between AES and RSA and RC6 algorithm



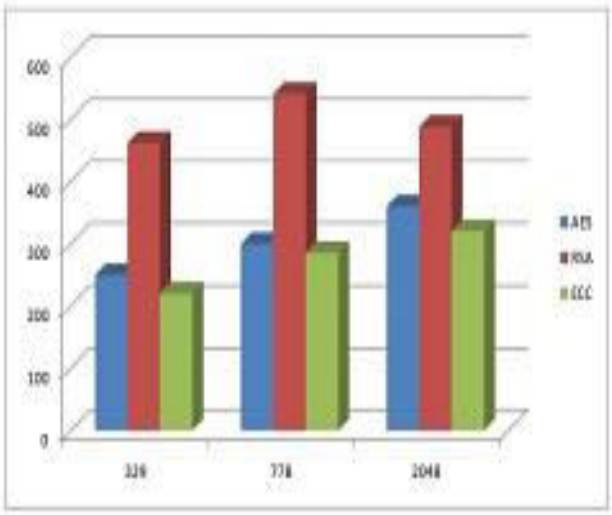
File Size (KB)	AES (ms)	RSA (ms)	BLOWFISH (ms)
329	250	462	52.940
778	300	541	98.248
2048	360	488	320.752

Table 5.2 shows the comparison between the values of AES and RSA and BLOWFISH encryption algorithm

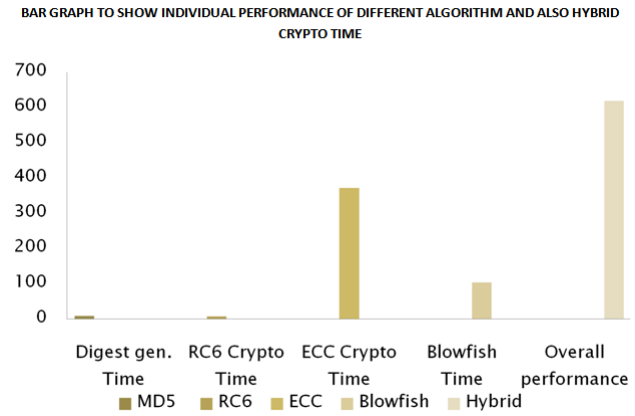


File Size (KB)	AES (ms)	RSA (ms)	ECC (ms)
329	250	462	8
778	300	541	18
2048	360	488	56

Table 5.3 shows the comparison between the values of AES and RSA and ECC encryption algorithm

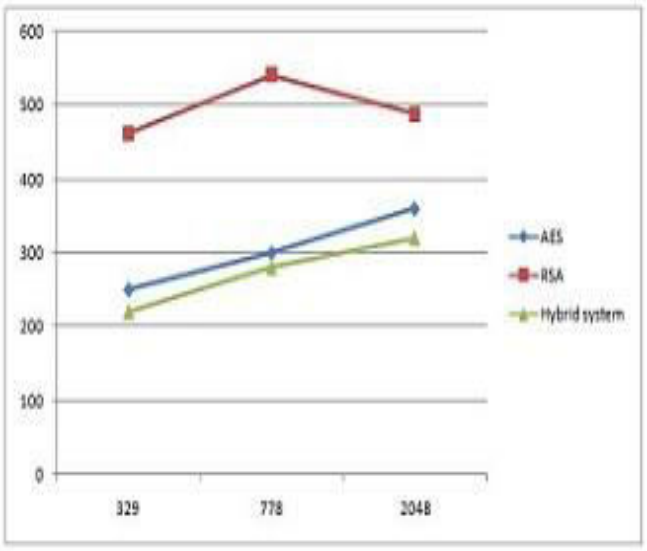


International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org



This Graph shows that firstly Blowfish encrypt the plain text then MD5 takes very less time to generate the digest value then Rc6 generates the keypool then ECC is used for strong encryption.

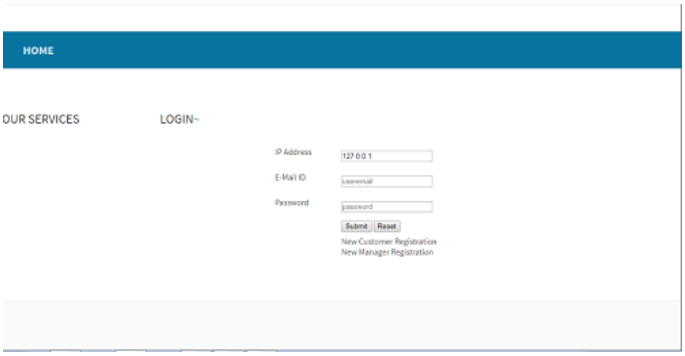
Final comparison graph for existing work and proposed work

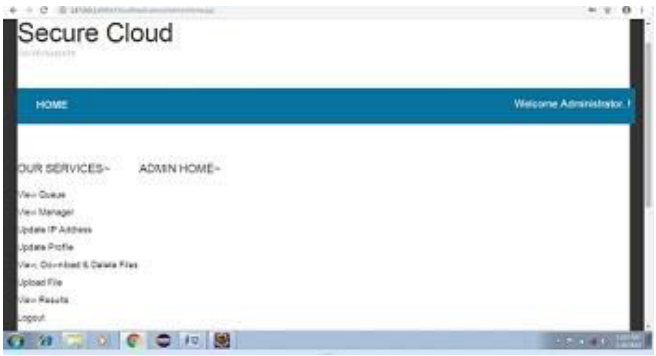


File Size	AES	RSA	Hybrid Crypto System
329	250	462	220
778	300	541	280
2048	360	488	320

1. IMPLIMANTATION ANALYSIS

Implimentation work of this project can be viewed in the snapshots that are given below:





7. CONCLUSION

Proposed work presented that, symmetric key RC6 is used to maintain confidentiality with creating keypool, this form multikey RC6 and store chunks in Map Index with id. ECC is used then for the purpose of strong encryption and decryption. BLOWFISH encrypt the complete plain text and after it the encrypted data is divided into chunks. The complete phenomena observe the need to enhance the level of security into cloud environment and proposed advance cryptographic model.

7. REFERENCES

[1] Khushbu Jakhotia, Rohini Bhosale, Dr. Chelpa Lingam, “Novel Architecture for Enabling Proof of Retrievability using AES Algorithm”.

Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[2] Babitha.M.P, K.R. Remesh Babu, "Secure Cloud Storage Using AES Encryption," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), IEEE.

[3] Teddy Mantoro, Yosep Lazuardi, "SMS Based Home Appliance Security Approach Using ROT 13, RC4 and RSA Algorithm. International conference on computing, engineer and design (ICCED). 2017 IEEE.

[4] Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, "Securing Data Storage in Cloud Computing", J. of Security Engineering, June 2012, pp.252-259.

[5] C.W. Hsu, C.W. Wang, Shiuhpyng Shieh, "Reliability and Security of Large Scale Data Storage in Cloud Computing", part of the Reliability Society Annual Technical Report 2010

[6] Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", IEEE Systems Journal, Vol.9, No.1, August 2015.

[7] P. Mell, Grance, "The NIST definition of cloud computing", Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145.

[8] Ashalatha R, Vaidehi M, "The Significance of Data Security in Cloud: A Survey on Challenges And Solutions on Data Security", International Journal of Internet Computing, Vol, 1, Iss. 3, 2012, pp.15-18.

[9] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, Iss. 1, Jan 2011, pp.1–11.

[10] Paul C. H., S Rao, C B. Silio, A Narayan, "System of Systems for Quality-of-Service Observation and Response inCloud Computing Environments", IEEE Systems Journal. Vol.9, No.1, March 2015, pp. 212-222.

[11] D Ardagna, G Casale, M Ciavotta, J F Perez, W Wang, "Quality-of-service in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications, 5:11, 2014, pp. 1-17.

[12] S.Lee, D.Tang, T.Chen, W.C.Chu, "A QoS assurance middleware model for enterprise cloud computing", IEEE 36 th Int. Conf. on Computer Software and Application Workshops, 2012, pp. 322-327.

[13] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", ACM Conference on Computer and Communication (CCS 2006), pp. 89-98.