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

COPY RIGHT

Title: Advance Cryptographic Model for Secure Cloud Environment: A Review

Volume 07, Issue 04, Pages: 102 – 108.

Paper Authors

NIDHI RAGASE[1], ANGAD SINGH

NRI Institute of Information Science & Technology,Bhopal,Madhya Pradesh,India.

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

ADVANCE CRYPTOGRAPHIC MODEL FOR SECURE CLOUD ENVIRONMENT: A REVIEW

NIDHI RAGASE[1], ANGAD SINGH [2]

[1]Research Scholar, Dept of IT , NRI Institute of Information Science & Technology, MP,India.
[2]Associate Professor, Dept of IT, NRI Institute of Information Science & Technology, MP,India.

ABSTRACT: With the growth in information and concern of security, awareness among users are increasing about cloud computing and its security. Due to security concerns security algorithms are required for the processing of data systems. A brief review and survey has been made by many researchers in this area for the better performance of security algorithms, also comparisons are made in cryptographic algorithms using symmetric and asymmetric key on the basis of cloud environment. In this paper security is performed using symmetric key RC6 for the purpose of increasing confidentiality by creating keypool to form it into multi key RC6 and storing every chunk with its id in Map Index then encrypting it using ECC for strong encryption. Also, the chunk data is encrypted using ECC and than cipher text is stored in cloud environment. keypool is generated using multiple number of keys.

INTRODUCTION

Many of the cryptographic and encryption algorithms are required for the security and privacy of data. Where, RC6 which is the symmetric key algorithm replaces many of the traditional algorithms. Multi key RC6 which is the modified version helps in securing data which security implementation using criteria like:

- Performance of software and hardware
- Security purpose
- Resistance from different attacks and attack analysis
- Suitable with every environment

With the combination of security, capability, performance, implementation, flexibility and efficiency an appropriate selection of RC6 is

made. RC6 performs efficiently with hardware and works faster with software by its design. It also works even more faster in mobile devices like small devices, phone, smart cards etc. because of its larger block size and longer keys, RC6 provides better security. It uses the fixed block size of 128 bit and also works with 192 and 256 bits key size. Traditional algorithm is flexible to work with because of keys and block size of multiple key of 32 bits, with minimum of 128 bits and maximum of 256 bits.

According to NIST, 3DES is replaced by AES, which allows immediate transmission to AES algorithm. Also AES comes up with the advantages like higher speed and hardware implementation.

In this paper a symmetric key algorithm is used for the security consolidation of applications and services based on cloud environment. In cloud environment, cloud itself manages the complete infrastructure, architecture and data centers. With the concern of security an integrated model is recommended for security purpose and secure data storage is proposed using security mechanism. Data integrity is the issue which is implemented in cloud for the verification purpose of the third party. Integrity in dynamic data improves model of retrievability using some authentication scheme.

Many challenges are faced by cloud on the basis of security, reliability and privacy. With observing essential characteristics like storage and security in distributed system because of its distributed capabilities. Therefore, security is the important concern with the growing of cloud users.

Now talking about Cloud computing, this technology is a vital technology with the growth in the field of computer science. Cloud serves there user using public and private enterprises and for the group of organization or corporate world it also provides with community cloud. For the integrated purpose it have hybrid cloud and consumers get services using these deployment models of cloud. Security is required in all the ways of security aspects and privacy. This will form cloud security a much better. Cloud computing on the basis of service models like Infrastructure-as-a-service (IaaS), Software-as-a-service (SaaS) and Platform-as-a-service (PaaS) serves there user with network connectivity, administrative services, accessing services,

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

operating system, utility computing, virtual computing.

2. RELATED WORK

Khushbu Jakhotia et al. In[1] proposed an architecture for novel cloud storage. Issues regarding trusted third part is always there in cloud because of the security and availability of data.

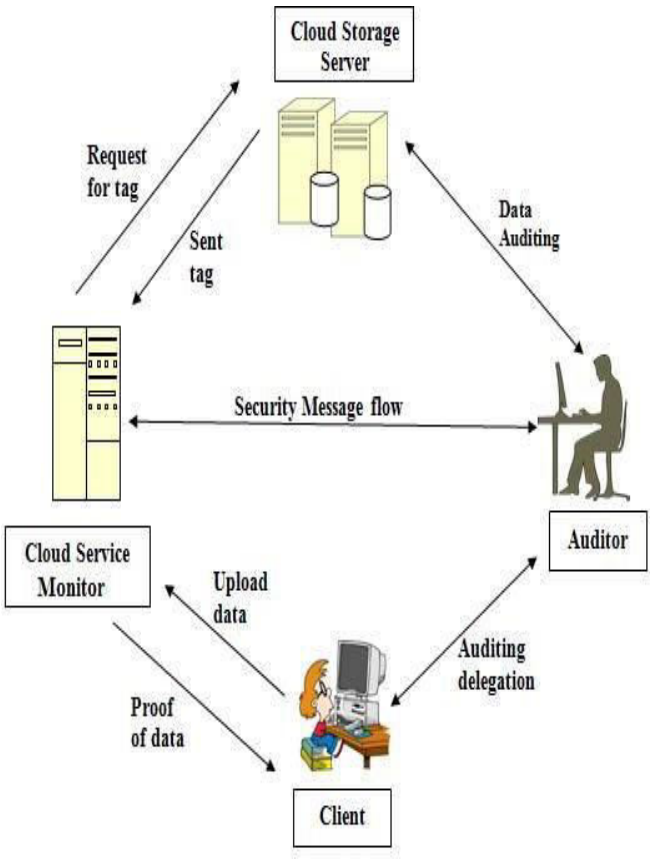

Figure 2: Existing Architecture

To get over from this issue an architecture which monitors cloud services are generated which verifies the original data, its availability and its retrievability for the proof of availability of original and accurate data for client at storage server. Third party auditor works as reducing the auditing of system. Thus, the model created reduces mistrust of the audit server and its dependency. For the security purpose data is encrypted using AES as a strong cryptographic algorithm and this algorithm is applied at the time of retrieving data and storing data on cloud server. At the time of downloading file more security is applied for making system more preventive and avoiding unnecessary downloads of file multiple time. In this way more security is provided by our model.

Babitha.M.P et al. In[2]proposed about various kinds of security issue in cloud environment with this, solution is also provided by author for using different services of securities such as authentication, confidentiality and authorization. AES is used by author for enhancement of confidentiality and data security. Data encrypted in this approach is using AES and then is uploaded on cloud. For avoidance of unauthorized access, short message service

is used. The proposed security approach uses a method for secure data in real time environment. Access control, confidentiality and authenticity is maintained using AES with 128 bit key. Performance of approach is studied by author, this analysis observe a delay with increased file size.

Teddy Mantoro et al. In[3] analyzed a comparison of speed time while encryption and decryption using algorithm RC4 and RSA, and than obtained outcome as RSA is 50 % faster when compared to RC4 algorithm in terms of encryption. It is faster because it immediately encrypt and decrypt the known value, whereas RC4 exchange the known key also. While comparing author address that RSA is shorter in key length then RC4 because result of RSA comes on the basis of length of plaintext.

Hyun-Suk Yu et al. In[4] worked on "Securing Data Storage in Cloud Computing". He explained about infrastructure of cloud and its management, where all the data storage, infrastructure and architecture is managed by cloud itself but concern on security which is recommended by author by consolidation security approaches with a secure mechanism for data storage.

3. PROBLEM STATEMENT

Existing system is facing issue of lacking in symmetric key because of using traditional AES technique, as Advanced Encryption Standard works on the basis of symmetric key algorithm, so only a single key is used for both encryption and decryption. This will rise the risk of key compromise and attackers can exclude cipher text and by attacking loose the originality of data.

By attacking data confidentiality may loose and integrity also breaks. Key compromising may lead to issue like Data confidentiality, Integrity and availability etc. and also data accuracy and originality is not maintained. If user access that data, might be possible, that data is modified or deleted.

Intruders involvement is also a biggest concern in loosing privacy, data accuracy can be reduced by unauthorized access, service denial attacks affect data availability.

4. PROPOSED SOLUTION

To overcome the issue of proposed problem a system implementation approach is proposed and this approach is the multi key RC6 technique with multiple key generation, works on the basis of key pool by storing the chunk_id and key_id in map

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

index and encrypting them using ECC and and calculating integrity through MD5 technique. The generated key_id is encrypted using ECC and the chunk_id which are stored in map index is encrypted using MD5 so as to generate integrity. Integrity maintains originality of data.

- Key pool solves the issue of key compromising
- MD5 helps in calculating integrity, where integrity maintains accuracy.
- ECC is used for Encrypting chunk_id which are stored in map index.
- Key pool also solve issue of lacking in symmetric key.

Flow of Complete Work:

Flow of complete work id described step by step below with the generation of key, encryption and decryption process. Step by step procedure is cited below:

step 1: Generation of Key:

- Take value from user
- Data is splitted into chunks
- For keypool, number of keys are generated.
- Keypool Kp = { K1, K2.....K6}
- Multiple keys are generated

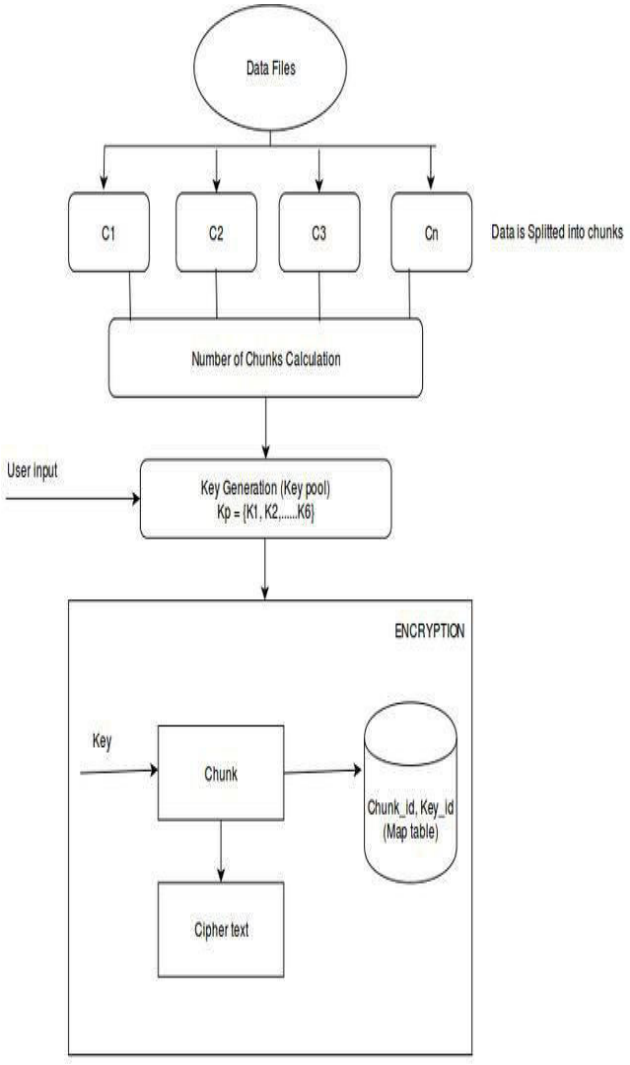

Figure 2: Flow of Proposed Work

Step 2. Encryption:

- Chunks are addressed with some chunk id.
- And these chunks are stored in Map Index.
- On the chunks the generated multiple keys are applied.
- These chunks are then encrypted using ECC.
- And, than cipher text is stored.
- The chunk_id that are stored in Map index are also encrypted using MD5.

Step 3. Decryption:

- Similar approach will be required to decrypt data.

5. CONCLUSION

Privacy and security are also important at the same time which need secure storage in cloud. This paper address secure data storage using multi key RC6 for increase in confidentiality and security by splitting data files into chunks and then calculating number of keys. The proposed model uses count to generate multiple number of keys after it encryption on data is performed.

6. 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.