International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 4 Issue: 2 March-April 2018 p-ISSN: 2394-8280

IMPROVED AES ALGORITHM FOR SECURE COMMUNICATION IN CLOUD

Abhipray Bajpai, Dr. D. K. Mishra

MTECH-Research Scholar, Sri Aurobindo Institute of Technology, Indore,
abhipraybajpai@gmail.com
Professor, Sri Aurobindo Institute of Technology, Indore, drdurgeshmishra@gmail.com

ABSTRACT

Cloud Computing provides the facility of shared environment due it its distributed resource nature and open environment. Thus, access of resource is easy from anywhere. Privacy and security are also important at the same time. Computing resources are another demand which makes outsourcing of data by the organizations, which need secure storage in cloud. This paper address secure data storage using AES (Advance Encryption Standard) for increase in confidentiality and security by splitting data files into chunks and then calculating number of keys. In the proposed approach chunk file is formed which generate key and then encryption on chunk file is performed. The proposed model uses count to generate multiple number of keys

Keywords: Key generation; AES; chunk file; encryption; decryption; count

1. INTRODUCTION

According to NIST, cloud is defined as the model which is convenient to serve with on-demand services and resources with decreased cost and easy to access service. Cloud environment is fully configured but require internet connection for accessing resources and services.

Cloud is a pool of resources which is the combination of distributed and shared computing offering beneficial aspects of software and hardware services. It is a cost effective service which is integrated with service model and has the ability to cope with the change in trend. Cloud computing serves with storage, server, network and a complete infrastructure to access applications and software easily.

Cloud computing is based on the service model and deployment model for the best performance and fulfilling demand of users. Deployment model and service models of cloud are cited below:

1. Deployment model:

   - Private Cloud: Private cloud is owned by a single organization and its complete management has to be taken care by the specific organization.
   - Public Cloud: Public cloud referred as inside and outside access, and popularly known as pay per use model.
   - Hybrid Cloud: It is the combination of both private and public cloud

- Community Cloud: It is cost effective and owned among organizations.

2. Service Model:

- Infrastructure-as-a-service: provides service like network connectivity, utility computing and administrative services.
- Platform-as-a-service: provides service for accessing libraries, tools and operating system.
- Software-as-a-service: provides service for accessing multiple software and application in beneficial way.

With the deployment and service models, cloud provides the feature and characteristics like:

- Scalability: It is scalable because its performance does not decrease with increase in user.
- Accessibility: provides easy and flexible accessibility with the use of browser.
- Shared resources:
- Elasticity: It is elastic because resources are used as per need.
- Pay-per-use: User only have to pay for the resources which he/she is using.

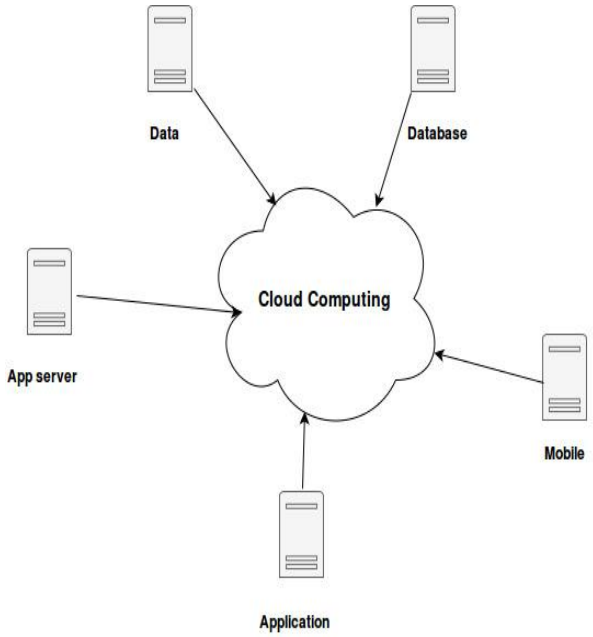

Figure 1: Cloud Computing

2. RELATED WORK

Babitha.M.P et al. In[1] proposed about security issues in cloud and a method for securing data using AES algorithm, which is the symmetric key algorithm used for encryption of data by providing security concern like authenticity, confidentiality and access control. Existing approach is based on delay with the increase in file size. But faces the issue of key compromising. It has been observed that for future extension an intelligent approch is used for the secure data storage.

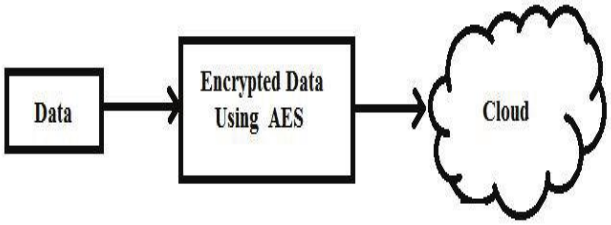

Figure 2: Existing work by Babitha.M.P[1]

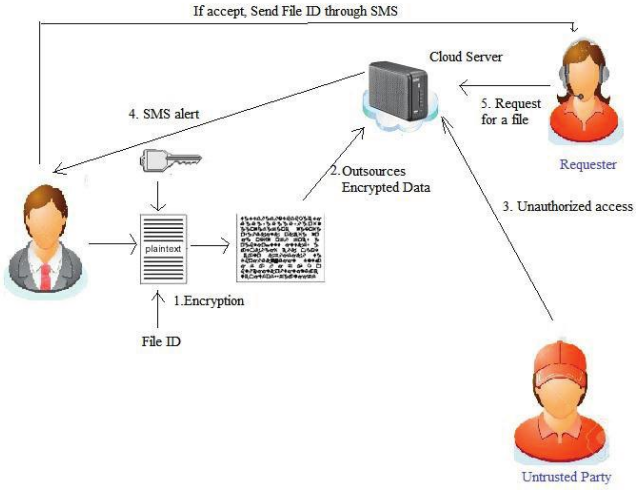

Figure 3: System architecture of existing work[1]

Hyun-Suk Yu et al. In[2] concluded about cloud infrastructure, where cloud itself manage its architecture, infrastructure and data storage. Here, security is the major concern. Author also recommended an integrated model for security in cloud infrastructure. Also proposed a security mechanism for secure data storage

C.W. Hsu et al. In[3] discussed about new challenges in cloud depending on security and reliability. Observe the important characteristics like distributed capabilities for storage and security using CAP theorem. Thus, security is the important concern because of the increase in number of cloud users.

Qian Wang et al. In[4] implemented the issue of data integrity in cloud computing. A third party auditor is used for the verification of integrity in dynamic data hich improves the retrievability model using hash tree for authentication.

3. PROBLEM STATEMENT

Existing system used AES fot the encryption od data in cloud. Data stored in cloud is firstly encrypted using Advanced Encryption Standard, but issue arises in existing system is the symmetric key. AES is a symmetric key algorithm which arises key compromising issue and this issue leads to access of data by intruders and attackers. Attackers by attacking may loss data confidentiality and privacy and results in modification or deletion of original data.

Key compromising may lead to:

1. Data confidentiality: Data confidentiality and privacy may loss due to attack.
2. Integrity: unauthorized access reduce accuracy of data.
3. Availability: Data availability may be affected lead to denial of services

Involvement of intruder is a big issue.

4. PROPOSED SOLUTION

To address the above problem proposed system will be implemented, which is also working on the AES technique but improved this technique using multi key generation. Data is encrypted using AES technique and the generated key by converting data into cipher text. N is the number of keys are calculated using count which solves the issue of key compromising. In the proposed approach chunk file is formed which generate key and then encryption on chunk file is performed. The proposed model uses count to generate multiple number of keys.

4.1 System Architecture:

Step bt step working procedure where firstly key is generated then data is encrypted and decrypted. Procedure is explained below:

1. Key Generation:
    - Take value of B(from user)
    - Split data into chunks
    - Find total number of chunks Tc.
    - Maximum number of keys to be generated for key pool.
    - Kp = { K1, K2, K3.....Kn }
    - n = Tc mod B
    - Generates multiple key n count.

2. Encryption:

- On the chunk file generated key are applied
- Key and chunk id are mapped in a table
- And then data is encrypted by converting into cipher text.

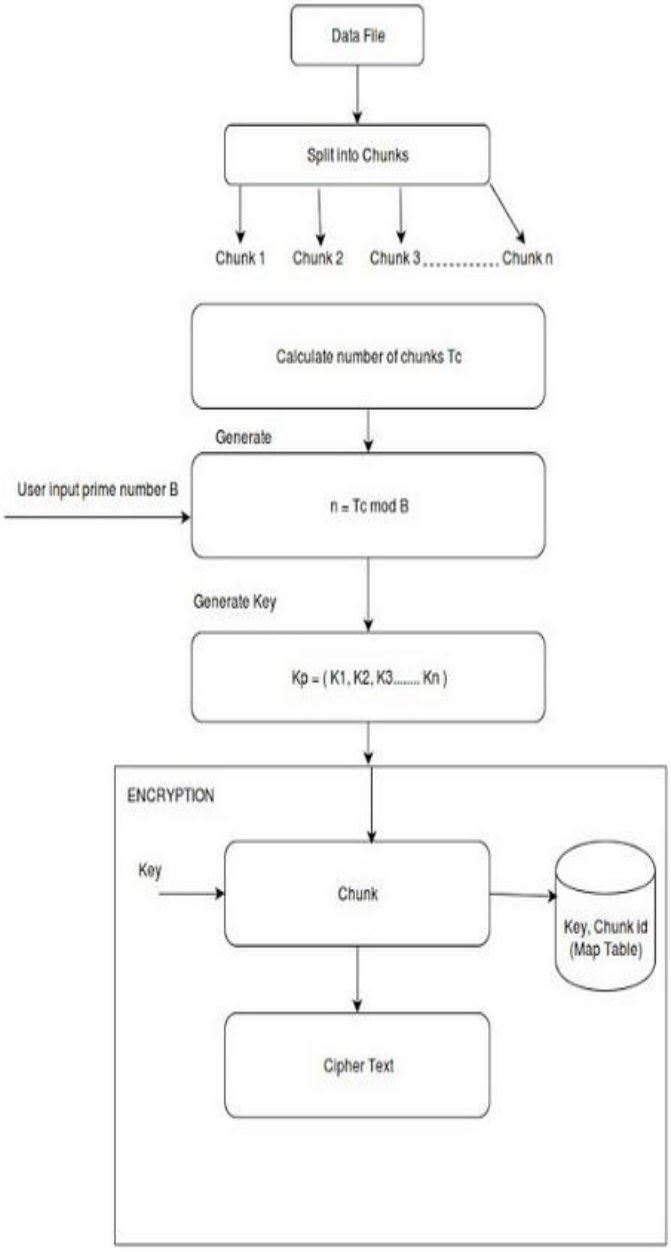

Figure 4: System Architecture for encryption

3. Decryption:

- User want to access the data and data is in encrypted form.
- Than, data is decrypted into plain text for further use
- Below diagram shows the decryption of data

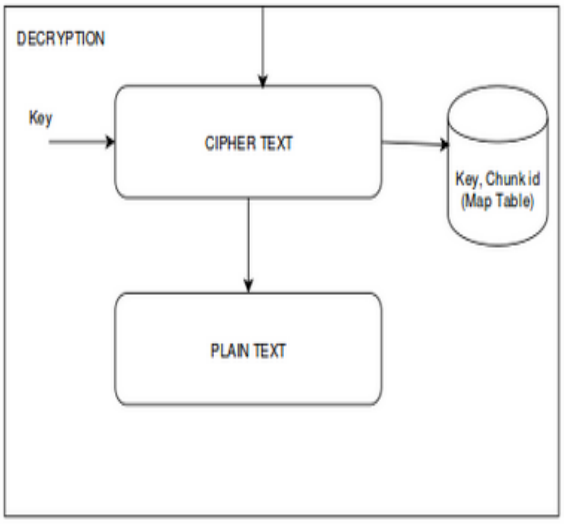

Figure 5: System Architecture for decryption

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 AES (Advance Encryption Standard) 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.

REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.