International Journal of Future Generation Communication and Networking
Vol. 12, No. 5, (2019), pp. 301- 305

Asymmetric AES Algorithm for Cloud Security

Sampath Kumar Tallapally, Dr.B. Manjula
[1,2]*Assistant Professor,*
Dept of CSE,
[1]*S R Engineering College,*
[2]*Kakatiya University,*
Warangal, India.

Abstract**:** In the present day scenario one of the major challenge in the area of cloud computing industry is to gather the confidence of consumers' and gather the trust by imposing adequate privacy and security for the obtained sensitive consumer or end-user data by providing constructive suggestions for imparting regulatory reforms which can provide sensitive information in cloud computing environments and to remove regulatory constraints that limit the acceleration of this vivacious new industry [2]. Due to emerging shape of cloud computing the process of developing quality data both conceptually and in reality the characteristics required are legal or contractual in terms of economic or service quality or interoperability or security and privacy related issues that prevail with significant challenges imposed. In this paper we are proposing a new algorithm which uses the basics of AES by which we can have better security for data on the cloud [5].

Keywords: *Advanced Encryption Standard; API- Application programming interface; CSP-Cloud Service Provider; AS-Authentication Server.*

I. INTRODUCTION

In the present day scenario AES a technique for data encryption is implemented or handled mathematically in an efficient and elegant cryptographic algorithm whose major strength is considered to be the option for various key lengths. In AES algorithm it allows you to choose a 128-bit or 192-bit or 256-bit key length for making it exponentially stronger. *On the same hand* AES1[1] uses permutation-substitution technique that involves a series of substitution and permutation steps for generating the encrypted block.

AES is a "Block Cipher Algorithm" which takes plain text in blocks and generates cipher text which is secured one. It is used for a secured file transfer as the data in the file is divided into fixed blocks that converts cipher text and then transmit to the receiver through a secured channel. The key used in the AES algorithm is symmetric key that is the same key is used at both sender and receiver ends as shown in figure 1 as it explains the skeleton of AES [2].

According to the Cloud Security Alliance the rundown of the primary cloud security is considerably dangers incorporated by accompanying: 1. Data Leaks: "Data in the cloud is presented to impossible to tell apart dangers from predictable frameworks because of the enormous quantify of information foundation of cloud suppliers that become an appealing objective for aggressors by identifying various information holes that can be punctual a chain of lamentable occasion for IT organizations and framework as a help (IaaS) supplier that exist. 2. Compromising Accounts and Authentication Bypass:As the information spills often via as a result of missing of statistics through consideration concerning validation take a look at as the powerless passwords associated with bad management of encryption keys and endorsements are to be faulted because the issues can likewise appear while a customer takes every other role or leaves the organization because the report has rights to a bigger number of highlights than should be expected. The cloud situations are frequently willing to make use of extensive range of assaults over manage facts because the chance can also likewise originate from gift or preceding representatives as the insiders may also have numerous idea techniques that extends information robbery to straightforward retribution.

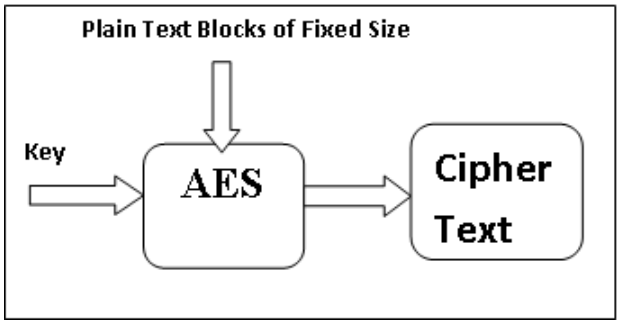

Fig. 1. Plain Text Blocks of Fixed Size

Distributed storage model is utilized in the model for PC information that performs stock piling where the advanced information is kept away in the form of legitimate pools. The physical stockpiling traverses in distinct servers as considered being once in a while in distinct areas based on the physical condition it is normally claimed and overseen by possible facilitating organization [3]. These distributed storage suppliers are responsible for keeping the information accessible and open the physical condition by ensuring and running where individual and association based purchase or rent stockpiling limits from the suppliers to store client along with association or application information.

Distributed storage administration is the major aspect that might be considered through allocated distributed computing administration as the web administration "Application Programming Interface (API)" or by the applications that utilize the API document. As an example every cloud work area or the stock pilings considered to be a distributed storage portal or the Web-based substance the board various frameworks [4].

The process of distributed storage completely depends on virtualized framework that resembles more extensive distributed computing aspect in regard of open interfaces as well as close moment flexibility and adaptability for obtaining multi-tenure and metered assets[13].

Distributed storage administrations are utilized by "off-premises administration (Amazon S3)" or conveyed "on-premises (ViON Capacity Services)". Cloud stockpiling normally comprises of article stockpiling administration where the term has expanded to incorporate various kinds of information that is stockpiled and is more often accessed by administrations.

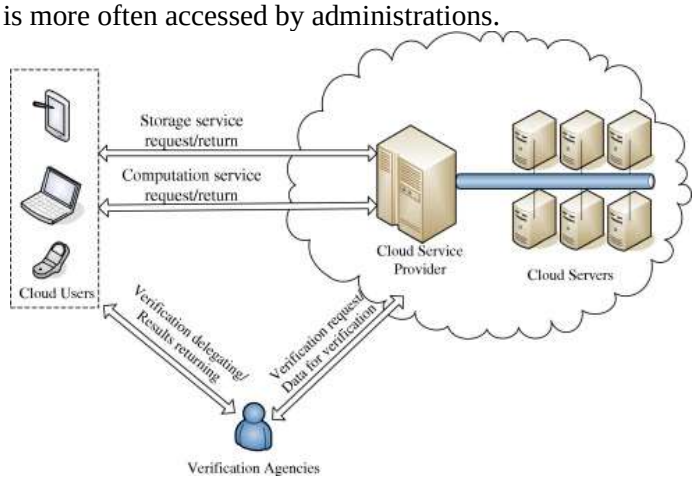

Fig. 2. Public API's for data and management

Article "stockpiling administrations like Amazon S3", "Oracle Cloud Storage and Microsoft Azure Storage", "object stockpiling programming like Openstack Swift", "object stockpiling frameworks like EMC Atmos" [5][8], "EMC ECS and Hitachi Content Platform" and disseminated stockpiling research ventures like OceanStore [6][11] and VISION Cloud are largely considered to be the instances of capacity that can be facilitated and conveyed with distributed storage attributes.

Distributed storage is:

- Made up of many conveyed assets at the same time that goes about as one or either in a united or a helpful stockpiling cloud design environment.
- Higher deficiency tolerant through repetition and conveyance of provided information.

- Highly sturdy through the production of formed duplicates or duplicate values.

Typically at the end predictable concerning information reproductions are attained.

II. DATA SECURITY

Re-appropriating information stockpiling builds the assault surface region

a) As and when information has been dispersed it is put away at more areas by perform expansion as the only danger of unapproved physical access to the information as the instance in cloud based engineering where the information is reproduced and moved every now and again so the danger of unapproved information is recovery increments significantly. For example on account of transfer of old hardware we can reuse of drives or reallocation of extra room. The way that information is repeated relies purely upon the administration level of a client picks and also based on the administration gave as a point when encryption is set up it can guarantee the aspect of classification and on the same hand Crypto-destroying can be utilized when discarding information in a circular form.

b) In order to access data or information on individual basis will be undermined that is paid off or constrained with possible increments significantly. In a stochastic organization comprises of a team of chairmen who hires skilled designers along with a team lead so called specialist in a distributed storage organization that comprises of numerous clients and a maximum number of servers. These servers require a lot bigger group of specialized staff with physical and electronic access as the majority of the information will tend to unscrambling keys. Separate keys are made available for administration users and a separate set of keys are generated for client. Instead of the specialist cooperation limit the entrance to information is considered to be specialist when compared with coworkers. The major concern is when it is related to different information grabbers with cloud. In an addition to this extensive number of keys must be disseminated to clients for providing secure channels for unscrambling and in addition to this it must be safely put away from clients in their gadgets which is a costly approach for attaining secure capacity for defeating the aspect of total key cryptosystem for utilizing it[10][12].

c) Quantity of systems can be constructed with possible set of information ventures with possible “neighborhood (LAN)“ or “capacity region arrange (SAN)” information that is kept away over possible clouds that requires a “WAN (wide region organize)” which is associated to both of them.

d) By offering stockpiling systems to numerous different clients or clients in workable form in different clients for obtaining the provided information. Due to the availability of inconsistent activities that is obtained due to flawed hardware or due to possible attainment of bug or due to any possible criminal aim the possible hazard applies to a wide range of capacity and not just over a distributed storage. The risk involved in having information perused or transmitted can be alleviated through encryption innovation scheme where the encryption secures information before transmitting to and from the cloud administration process. The process of encryption ensures information by specialist organization for encoding information in an on-premises cloud administration for obtaining entrance ramp framework which is provided in two sorts of encryption assurance.

A. Problem Statement

Basically AES is a Symmetric encryption algorithm ie same key is used by sender and receiver .Storing a file over a Cloud for maintaining and providing security to the file which doesn’t need and searching or indexing a file, we take the advantage of AES algorithm to convert the file data into cipher text and store it on to the cloud. But the problem is unauthorized persons or intruders who are closely watching the network can enter into the cloud download the cipher text and cryptanalysis can be done and key can be expected by brute force and the same key is used to decrypt the data into actual file which can make money for the intruders.

B. Solution

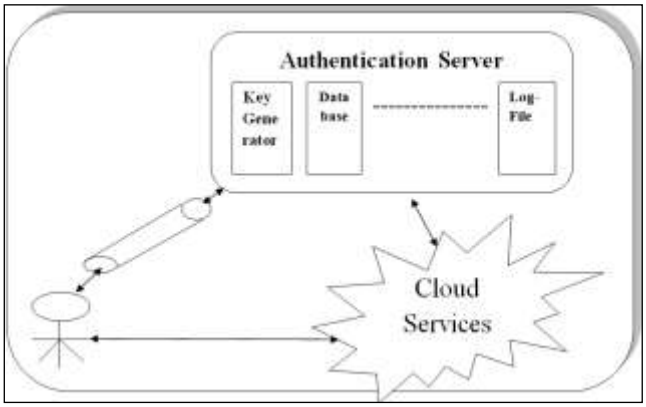

Fig. 3. Authentication server process for cloud services.

Once the data owner is authenticated by the server (a data owner is a person who wants t store the data on the cloud) the data owner performs the operations

a) Data Owner request AS for a key which will be supplied to the authenticated owner, AS creates two keys private key (pk) and public key(pu)

b) The public key generated by the server is sent to the owner and the private key for this particular owner is stored/ appended to a file.

c) Data Owner takes the public key.

d) The file which is to be stored into the cloud is divided into divisions or parts we intern have blocks in it, we use the public key to convert these divisions into cipher text.

e) This Cipher text is stored over the cloud.

f) These steps are repeated till the data in file is exhausted.

Role of Authenticating Server(AS):-It authenticates the data owner to store the data over the cloud and a special component which exist in the AS is key generator which generates the key in the manner of Producer and Consumer where new key is not generated till the old one is been used for the data encryption for every request.

C Result Analysis

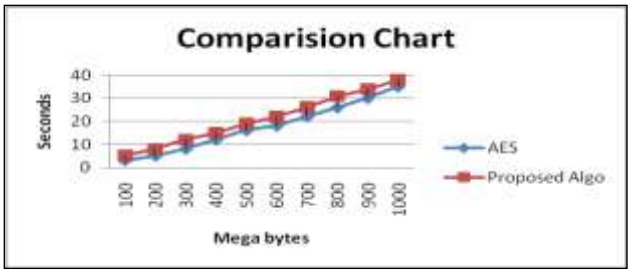

Fig. 4. Comparison chart of AES and proposed AES for memory utilization in megabytes for a span of seconds

In the above line chart y axis says about time taken to transmit the data and x axis defines the file size ,red line shows the time taken by the AES algorithm and the blue line defines the Asymmetric AES algorithm which was simulated on Java Platform. When security is concerned we can compromise with time after all we are dealing with sensitive data.

III. CONCLUSIONS

AES need only one key which can be generated by the intruder by making a bit analysis but where as in our proposed algorithm the file have different divisions and every divisions is encrypted with

a different public key .When a customer wants to download the file he should be authenticated by the AS and AS should supply the log file to the customer so that he can decrypt the file. The above scenario was applied only for the text sought of data in future we apply it to different files like pdf, docx, videos etc.

References

[1] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] A New Technique to Secure Data Over Cloud.
Jour of Adv Research in Dynamical & Control Systems, 11-Special Issue, July 2017
[3] Juels, A. and Kaliski Jr, B.S. PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM conference on Computer and communications security, 2007, 584-597
[4] He, J., Zhang, Y., Huang, G., Shi, Y. and Cao, J. Distributed data possession checking for securing multiple replicas in geographically-dispersed clouds. Journal of Computer and System Sciences 78 (5) (2012) 1345-1358.
[5] https://en.wikipedia.org/wiki/Producer%E2%80%93consumer_problem
[6] P. Praveen, B. Rama and T. Sampath Kumar, "An efficient clustering algorithm of minimum Spanning Tree," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2017, pp. 131-135.doi: 10.1109/AEEICB.2017.7972398
[7] Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud DataNing Cao, Member, IEEE, Cong Wang, Member, IEEE, Ming Li, Member, IEEE,Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE
[8] Data Privacy in “Cloud computing”Ahmed EL-Yahyaoui, Mohamed Dafir Ech-Chrif& EL Kettani
[9] Mohammed Ali Shaik, P.Praveen, Dr.R.Vijaya Prakash, "Novel Classification Scheme for Multi Agents", Asian Journal of Computer Science and Technology, ISSN: 2249-0701 Vol.8 No.S3, 2019, pp. 54-58.
[10] P.Praveen, B.Rama, “An Efficient Smart Search Using R Tree on Spatial Data”, Journal of Advanced Research in Dynamical and Control Systems, Issue 4,ISSN:1943-023x.
[11] Sallauddin Mohmmad,Dr.M.Sheshikala, Shabana,”Software Defined Security (SDSec):Reliable centralized security system to decentralized applications in SDN and their challenges”,Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (147-152).
[12] R. Ravi Kumar, M. Babu Reddy and P. Praveen, "A review of feature subset selection on unsupervised learning," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai,2017,pp.163-167.doi: 10.1109/AEEICB.2017.7972404.
[13] M. Sheshikala, D. Rajeswara Rao and R. Vijaya Prakash, Computation Analysis for Finding Co–Location Patterns using Map–Reduce Framework, Indian Journal of Science and Technology, Vol 10(8), DOI: 10.17485/ijst/2017/v10i8/106709, February 2017.