Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Data Security in Cloud Computing using Cryptography

Keerthana G, Dr. Prabu S, Dr. Swarnalatha P
Department of CSE, VIT University, Vellore,
Tamilnadu, India

Abstract*— Cloud computing is Internet based computing where virtual shared servers give softwares and different assets and facilitating to clients on a pay-as-you-use premise. cloud storage is only the putting away information on third party cloud servers. Points of interest of cloud computing are unlimited storage and backup and recovery. Demerits of cloud computing are specialized issues, cost and absence of backing. In any case, fundamental drawback is security. As we store our information on third party cloud administration suppliers our information is not totally protected. It force an extraordinary danger. Numerous cloud servers are interested servers i.e., they attempt to peruse the information which is put away on it. We will probably fabricate an application for enhancing cloud security utilizing partition and encryption technique which will enhance the cloud security.In this first we take record from client and partition it into number of parts. After partition we encrypt the all record parts. At that point we send record parts to various cloud servers. At the point when client need that information back we take that information from cloud servers and decyrpt that information. After decrypting we merge that information and offer it to client. Our objective is that the application ought to have straight forward client interface for clients adaptability. The proficient method for giving security is the utilization of hybrid cryptography for more secured sending and receiving of information.

***Keywords*— Cloud, Security, partition, cryptography, merging**

I. INTRODUCTION

In this period of innovation, the Internet access gets to be accessible in the late years, Cloud computing is a web based innovation, being utilized generally these days to empower the end client to make and utilize softwares without thinking over the execution of the specialized data from anyplace whenever. Keeping in mind the end goal to store the huge volume of information, cloud storage frameworks use some little scale free storage frameworks. These frameworks together shape the whole cloud storage. To store the information utilizing cloud storage has various points of interest. Few of them are information storage information using an account that can be used every where. There are lot of repeated data found in the cloud servers [2]. Clients can utilize negligible measure of storage space by keeping away from the copies. The cloud computing has numerous elements to the clients like correspondence media, file storage and calculations, continue reflecting of exceedingly essential data, and so on., Basically, client information are put away in different storage areas like nearby servers and cloud.[2]

Information security is seen as basic issue inside cloud computing environment. The adaptability to access information anyplace on the planet as long the clients has the advances and approaches to get to it has raises genuine security concern put away utilizing a record can be adjusted in numerous gadgets utilizing the same record. There are part of clashing copies are accessible in cloud storage[2].

The basic types of security concern are confidentiality, Integrity and Availability .

Confidentiality, depicted as the certification that information is be kept mystery.

Integrity, which alludes to the powerlessness to adjust or decimate information coincidentally or wrong doing.

Availability, which is the capacity to get to that information at whatever point it is required Hence there is a requirement for a component to handle the security issues.

In this paper, a framework has been proposed by using cryptography encryption algorithm RSA and AES encrypted methods to ensure the security of users' data in the cloud.[3]

IBM Bluemix is the IBM open cloud organize that gives portable and web makers access to IBM programming for blend, security, trade, and other key limits, and programming from business associates. Bluemix similarly has cloud game plans that fit your needs. Whether you are a little business that plans to scale, or a boundless try that requires additional separation, you can make in a cloud without edges, where you can relate your submitted administrations to individuals by and large Bluemix administrations open from IBM and thier suppliers. All administrations cases are regulated by IBM. Bluemix in like manner gives middleware administrations to your applications to use. Bluemix catches up for the application's purpose when it obtainments new administrations cases, and after that binds those administrations to the application. Your application can perform its certifiable occupation, leaving the administrations of the administrations to the foundation. Generally speaking, you don't have to push over the working structure and foundation layers when running applications on Bluemix. Layers, for instance, root filesystems and middleware sections are fantastic with the objective that you can focus on your application code.

II. CLOUD COMPUTING SECURITY ISSUES [4]

A. Identification & Authentication:

Cloud processing, subordinate upon the kind of cloud and also the transmission model, indicated customers ought to firstly be secured and going with access necessities and assents might be yielded in like way. This technique is center at checking and thankful solitary cloud customers by use usernames and passwords affirmations' to their cloud profiles Authorization is a basic data security necessity in Cloud registering to guarantee referential uprightness is keep up. It takes after on in applying control and common freedoms over procedure streams inside Cloud figuring. Approval is kept up by cloud administration provider.

B. Confidentiality:

In Cloud processing, security has genuine impact especially in overseeing of cloud administration supplier control over affiliations' data masterminded crosswise over various appropriated databases. It empower necessity when using in Public in light of unequivocal quality nature. Proclaiming privacy of customers' blueprint and securing their data that is for reason got to considers information security traditions to be approved at various particular layers of cloud demand.

C. Integrity:

The genuineness prerequisite lies in applying the due mindfulness inside the cloud region, on a very basic level while getting to Information. In this manner atomicity, consistency, control are the properties of the cloud's data ought to be sure be effectively constrained over all Cloud enrolling pass on models

D. Non-repudiation:

Non-denial in Cloud enlisting may be procured by applying the customary e-exchange security traditions and token offices to data transmission inside cloud procurements, for instance, propelled marks, timestamps and statement receipts organizations.

III. LITERATURE SURVEY

V.Masthanamma, G.Lakshmi Preya [1] discuss about the utilization of cryptography ideas, to expand the security of encoded information which is sent by the client to cloud server. The primary objective is to encrypt and decrypt the information in a secured path with exhaustion of less time and less cost in both the encryption and decoding process. Numerous quantities of keys will be created and regular attacks will be noted. So by rehashing the procedure it helps you to keep the assaults to expand the security of decrypted information which is sent by the client to cloud server. The principle objective is to encrypt and decrypt the information in a secured route with exhaustion of less time and less cost in both the encryption and unscrambling process. Numerous quantities of keys will be created and basic assaults will be noted. So by rehashing the procedure it helps you to keep the attacks.

Mr. Akash Kanade et al [2], portrays that in the Partitioning Technique writing audit is done for information respectability checking, information storage mechanisms and encryption instrument. The dynamic information stockpiling with token pre-calculation and AES calculation how it is stored in cloud is broke down Integrity checking isused to identify and abstain from getting out of hand server considering information revision and confining blunders .Distributed plan is utilized to accomplish the availability, information quality, integrity of tried and true stockpiling administrations. The data capacity utilizing dynamic information operation technique is used to perform different operations. Security investigation is encode the information by RSA.

Kiruthika.R et al [5], describes the way that the ciphers and its converse use diverse parts for all intents and purposes wipes out the keys in AES, which is a current downside of DES. Likewise, nonlinearity of the key extension for all intents and purposes takes out the likelihood of proportionate keys in AES. An execution correlation amongst AES, DES and Triple DES for various microcontrollers demonstrates that AES has a PC expense of the same request as required for Triple DES . Another execution assessment uncovers that AES has favorable position over calculations 3DES, DES and RC2 as far as execution time (in milliseconds) with various bundle size and throughput (Megabyte/Sec) for encryption and also decryption. Likewise on account of changing information sort, for example, image rather than text, it has been found that AES has advantage over RC2, RC6 and Blowfish regarding time utilization.

Nasrin Khanezaei , Zurina Mohd Hanapi [3], that there are numerous studies and examines performed to enhance the security of cloud computing storage and environment utilizing encryption strategies and different techniques. Not withstanding, there has been a slight change in the consequences of these works contrasting and the quick development of cloud computing correspondences. Ordinarily, security models in cloud-based situations are separated to verification models, for example, , information assurance models, for example, , and access administration models, for example, . Utilizing a mix of cryptography encryption calculations, for example, RSA and AES is one of the conceivable assurance answers for securing distributed storage administrations.

IV. IBM BLUEMIX

The point of IBM BlueMix (Cloud Operating Environment or OE) is to bolster the objectives and desires of designers, empowering them to transform their thoughts into delivered items quick. By disposing of multifaceted nature, IBM Cloud Platform cuts application advancement and arrangement times from months to days and hours. Blue Mix is a far reaching, cloud-based application advancement and facilitating stage. It gives designers of present day web and versatile applications with: Tools to creator their web and portable applications, and instruments to make them ceaselessly

accessible on the cloud. A versatile, cloud-based base to send and control their applications—taking into account an assortment of various runtimes (Java-based application servers, Ruby, JavaScript, and the sky is the limit from there). A wide assortment of prepared to-use administrations, (for example, perseverance, informing, reserving, investigation, and the sky is the limit from there) uncovered through APIs and straightforwardly provisioned by the stage at run time. What's more, engineers can significantly diminish time-to-quality and associations can drastically decrease operational expenses.

Networking services:

The IBM® Network Security Groups administration in Bluemix concentrates on system security. Utilize the IBM Network Security Groups administration to arrange and oversee system approaches that control inbound and outbound movement between virtual servers. You can discover the administration in the Bluemix index under the Security classification and under the Network class. A security gathering is an arrangement of IP channel rules. Every IP guideline speaks to a system security principle. Every security bunch speaks to a system security arrangement. You can have up to 10 security bunches for every space of your Bluemix association. You can relegate various security gatherings to a solitary virtual server or to a virtual server bunch.

V. BLUEMIX ARCHITECTURE

The application developer deploys an application so that bluemix can setup the proper execution environment. The bluemix also supports the virtual machines in which it contains the application manager and where the applications are enclosed .

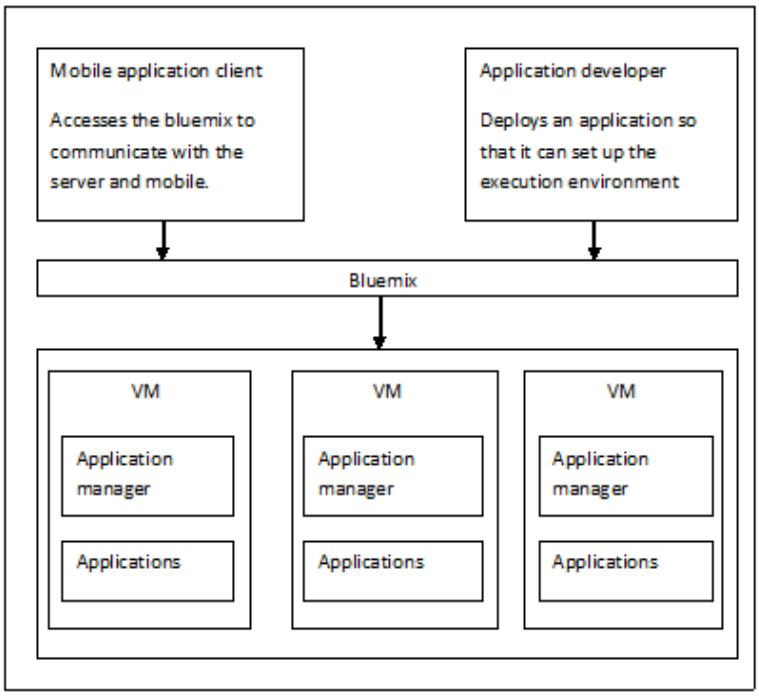

Fig-1 Blue mix working architecture

Here, the bluemix architecture working process is briefly explained. The mobile application client provides the accesses to the bluemix airfact to communicate with a server and also invokes the generic mobile and bluemix .net api's.

VI. ARCHITECTURE

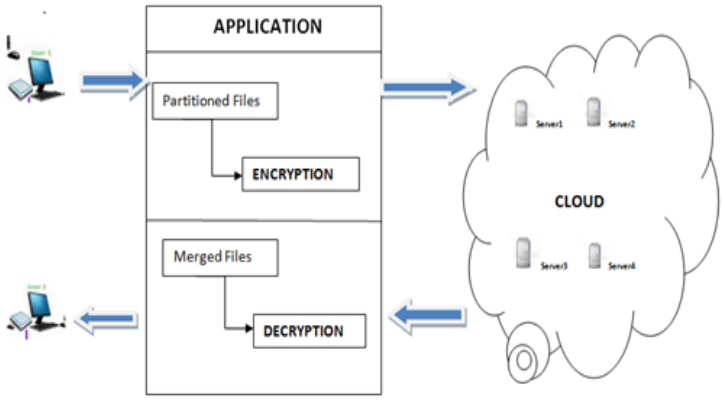

Fig-2 Architecture of the application

In Fig-2, it is explained about how the architecture works effectively for the secured transferring of data. Here the architecture includes client, Server and an application that is used to process the encryption and decryption techniques. Here the client sends the datas to the application where in the datas are partitioned and encrypted. Then it is sent to the cloud server. The datas from the cloud server are decrypted and then merged, which are again sent back to the client .This done with the efficient cryptographic techiniques i.e., the usage of symmetric and asymmetric algorithms together which provides more security. The Benefits

- Secure Transmission of file between users and cloud.
- Less chance of finding the symmetric secret key
- Using asymmetric encryption algorithm makes it difficult for attackers to read the files. Even if they have the PUBLIC KEY.
- Less time of transmission because of using symmetric algorithm.

VII. ENCRYPTION AND DECRYPTION TECHNIQUE

To build the security of encrypted information which is sent by the client to cloud server. The fundamental objective is to encrypt and decrypt the information in a secured path with less time and less cost in both the encryption and decryption process. Numerous quantities of keys will be produced and regular attacks will be noted. So this procedure it helps you to keep the attacks.

This algorithm is done in three steps:

Key generation
Encryption
Decryption

Encryption process:

In this process, a plaintext in series of numbers modulo n. This is too obain ciphertext from plain text M .It is formulated as C=M e mod n

Where C is cipher text

M is Message text

E is public key

D is private key

The file will be encrypted by an symmetric file encrypted key simultaneously asymmetric public key will generated, both will be combined and forms an encrypted with a header file.

Decryption process:

The reverse process of encryption will be decryption. It can be generated using the
m= e mod n.

Where C =cipher text
M=message text

E =public key; D =private key

Partition Algorithm

The input file and its sizes are loaded.
Size of the file is checked.

If size=invalid , declare as invalid size.
Else size= s

File is partitioned with indexed and extension value.

Return the files.

Merging Algorithm

Collect decrypted files pieces.
Check file status.

If file! Then missing

Else

Index value is taken
Merge files.

Return files.

AES Algorithm

It is a symmetric key cipher in which the block sizes are of 128 bits. The key can be 128, 192, 256 bits.
The steps involved are:
10 rounds for 128 bits

12 rounds for 192 bits
14 rounds for 256 bits

RSA Algorithm
It is an asymmetric public key used to support the encryption and digital signatures. The encrypting decrypting are confidentially done that is why the google mail, yahoo mail are using this to insure the services.

VIII. DESIGN AND IMPLEMENTATION

The module designs of application:

User Interface
In cloud technology, User browse the application through browsing interfaces. User interact with Application to perform the task. When an application reads a input from the user then it can connect to cloud Environment. Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations. An entity that is used to retrieve the data from cloud server.

Partition
User interact with Application to partition the data and store on to multiple servers. When file entered into the application it will partition. When an application reads a file, it divides and then contacts a cloud storage. After that file give requests and transfer to the desired resource in cloud.

Encryption
Here, the users are faciliated with the encryption process in order to provide security to the partitioned files.The partitioned files are encrypted with the hybrid cryptography methodology (i.e) usage of both the symmetric and asymmetric algorithms to provide more security.

Merging
The datas are merged from the servers and are sent for the next process . The networking concepts in bluemix are used here the merging process. Once if the datas are merged and done with the decryption the time taken will be reduced.

Decryption
Here, the users are faciliated with the decryption process in order to provide security to the merged files.The partitioned files are decrypted with the hybrid cryptography methodology (i.e) usage of both the symmetric and asymmetric algorithms to provide more security.

IX. DEMONSTRATION

The application process include the following steps:

1. **Create an application :**
   https://hub.jazz.net/docs/startproject/
2. **Editing code :**
   https://hub.jazz.net/docs/edit/
3. **Source control :**
   https://hub.jazz.net/docs/sourcecontrol/
4. **Build and deploy:**
   https://hub.jazz.net/docs/deploy/

Logint to the IBM bluemix:

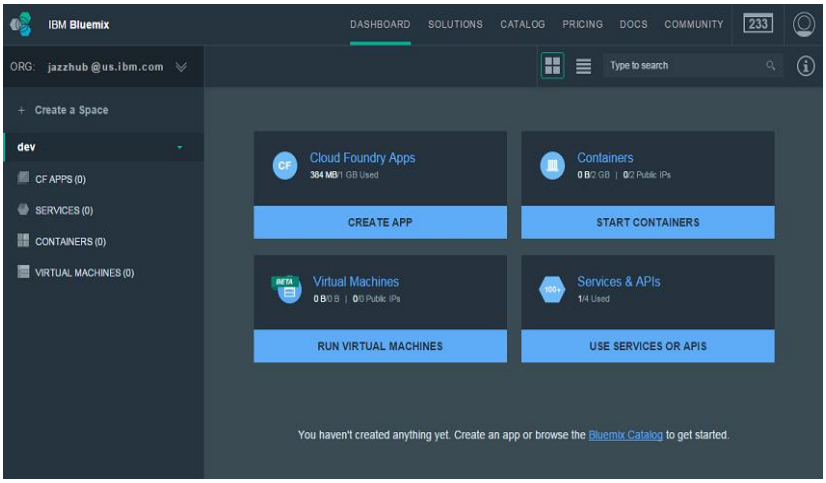

Fig- 3 Login to the Ibm bluemix

The login process requires the pre process of registration in the IBM bluemix. By loggin into the account we will find the dashboard in which the dashboard shows the Cloud foundary apps, conainers ,virtual machines and services.

Creating the application

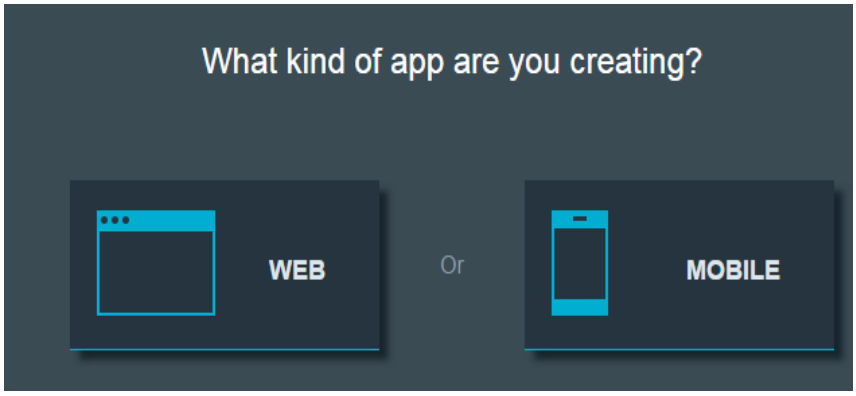

Fig- 4 Choosing the template

There are two kinds of application you can create and that can be selected while creating that is whether for web or mobile. The selection of languages like java, .Net or python is also available and then continue the process by naming the application .The renaming of application is also available.

Adding GIT Repository:

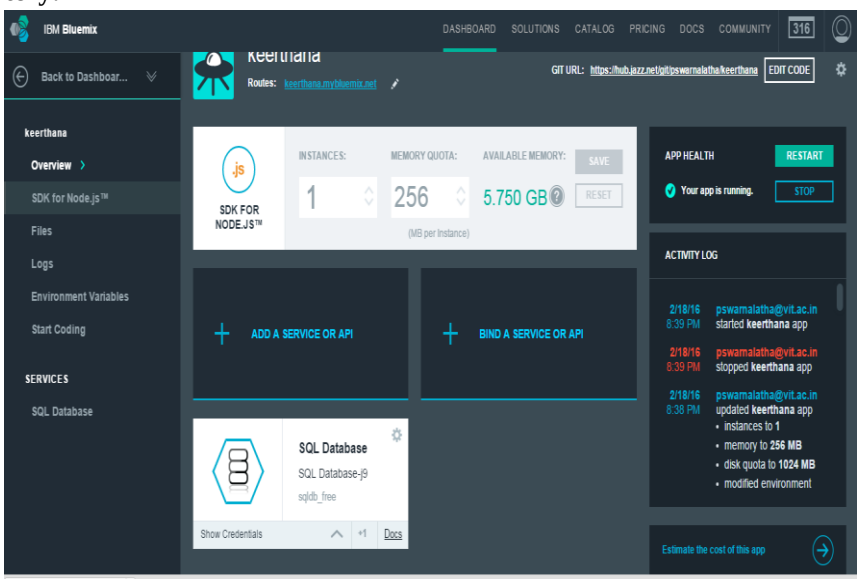

Fig-5 created application with edit code

Here , once if the GIT repository is added we can click on the EDIT code option that is available in the right side upper corner and we can start coding the application with the features what we needed .

X. CONCLUSION

A mix of asymmetric and symmetric encryption methods (i.e. RSA and AES encryption techniques) was proposed in this way to deal with accomplish the affirmations of cloud information security. The emphasis was on RSA encryption to give trouble to aggressors and lessening the season of data transmission by utilizing AES encryption strategy. The procedure of sending the documents to the cloud and recovering the records from the cloud was proficient by symmetric and hilter kilter encryption separately. The reason of utilizing symmetric encryption as a part of recovering the documents from the cloud was a result of the key circulation issue. Then again, it provides an ideal result in light of the fact that producing hilter kilter keys is a period expending. Thus, the encryption process turns out to be twofold and increasingly if there is augmentation of the document measure more than 254 byte. Another issue is the quantity of keys produced for every records. The quantity of keys will get to be triple times for every measure of documents put away in the cloud. Accordingly can be a major issue to handle for a substantial stockpiling framework. Additionally, the encryption and decoding handle that done twice for every documents cause framework overhead. By and by, contrasted with existing technique a cross breed strategy for encryption, for example, this is more secure to utilize. The specified disadvantages must be considered in future attempts to upgrade the security of distributed computing administrations.

REFERENCES

[1] V. Masthanamma, G. Lakshmi Preya," An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm", International Journal of Innovative Research in Science, Engineering and Technology,Vol.4,pp.1441- 1445,2015.

[2] Kanade, Mr Akash, et al. "Improving Cloud Security Using Data Partitioning And Encryption Technique" , International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015 ISSN 2091-2730

[3] Khanezaei, Nasrin, and Zurina Mohd Hanapi. "A framework based on RSA and AES encryption algorithms for cloud computing services." *Systems, Process and Control (ICSPC), 2014 IEEE Conference on*. IEEE, 2014.

[4] Kaur, Charanjeet, and Er Gurjit Singh Bhathal. "DATA SECURITY ALGORITHMS IN CLOUD COMPUTING: A." *International Journal For Technological Research In Engineering Volume 2, Issue 5, January-2015*

[5] Pancholi, Vishal R., and Bhadresh P. Patel. "Enhancement of Cloud Computing Security with Secure Data Storage using AES." *International Journal for Innovative Research in Science and Technology* 2.9 (2016):18-21.

