ISSN: 0976-3104
SPECIAL ISSUE: Emerging trends in Computer Engineering and Research (ECER)

ARTICLE

AN EFFICIENT HYBRID CRYPTOGRAPHY FOR SECURED DATA IN PUBLIC CLOUD ENVIRONMENT

Prabu S*, Gopinath Ganapathy

Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamil Nadu, INDIA

ABSTRACT

Background: *Cloud Computing (CC) can be termed as the figuring which is based on Internet in which powerful apportioned servers are giving programming's including diverse belonging with encouraging for purchasers on a compensation as-you-utilize hypothesis. The archive in cloud is nothing but securing data on outsider cloud servers. The reasons for CC being huge are boundless capacity, reinforcement along with restoration. The CC's bad marks are specific concern, value including nonattendance of help. Regardless to say, reliability is the essential hitch. Since the capacity of data on outsider cloud servers' providers is concerned, one cannot say that it is fully secured. This constrains a sudden risk. Various servers in the cloud are concerned which means that they endeavor in order to examine the data secured on it.* ***Methods:*** *The paper is going to deliver software which helps to upgrade the reliability of cloud uses parcel along with an encoding approach that can intensify insurance of the cloud. Firstly, getting the purchaser's affirmation and then parceling that to various segments has been finished. Once the partition is done, encryption of each record segment.is considered.* ***Results:*** *By then, sending of affirmation parts to various cloud servers is given most extreme significance. And when customer requires that information back, recovery of information from cloud servers and decoding of that information is gone ahead. In the wake of unscrambling, mix of that information and offer it to buyer is considered.* ***Conclusion:*** *The concept is to have the software promptly remit customer incorporation for customer's suppleness. The system which is capable to assure is the usage of half and half cryptography in a method which is more secure to send and accept the data.*

KEY WORDS
Cloud Computing, Reliability Algorithm, Subdivision Algorithm, Cryptography, Converging Methodology

Received: 15 May 2017
Accepted: 15 July 2017
Published: 20 Sept 2017

***Corresponding Author**
Email:
sprabubdu@gmail.com

INTRODUCTION

In the current season comprising of improvement, the Internet persuades the chance to be open late years, Distributed figuring is a web progression, utilized overall now-a-days to draw in the ultimate user to produce and employ programming lacking a complete consideration of accomplishment of the specific information from wherever at whatever point. Recollecting the genuine target which is to save monstrous information, server structures apply a few stockpiling substructures which are free from scale. The entire cloud space is shaped by combining these substructures together. The server space comprises of diverse reasons for engrossment which supports the usage of data. The cloud servers have parts of repetitive information [1]. The consumers can use unimportant evaluation of repository volume by maintaining a strategic distance from the copies. The server space has different parts to the clients like correspondence, archive space, numbers, exceptionally central data continues to get reflected, and so forth. Essentially, the data of client are secured in various stockpiling locales as neighboring servers including cloud [1].

The reliability of data is perceived as fundamental predicament within server space condition. Its adaptability for utilizing data wherever on the planet as the customers has the advances , approaches for getting to it has good fashioned security concern set away using a record can be balanced in various contraptions using an equivalent record. There are a touch of conflicting duplicates are open in scattered limit. [1]

The groupings of security concern are:

- Privacy, depicted confirmation that information is be kept puzzle.
- Trustworthiness, proposes for weakness to alter or beat information fortuitously or malpractice.
- Openness, which is the ability to get to that data at whatever point it is required subsequently there, is a requirement for a segment to deal with the security issues.
- A count that usages particularly secured transmission of information is to store and recoup from the cloud space are used. [2]

IBM Blue mix is the IBM open cloud manage that gives invaluable and web producers access to IBM programming for mix, security, exchange, and other key motivations behind control, and programming from business associates. Blue mix moderately has cloud plans that fit your needs. Despite whether you are a little business that approaches to scale, or an unending attempt that requires extra section, you can make in a cloud without edges, where you can relate your submitted relationship to people all around Blue mix affiliations open from IBM and their providers. All affiliations cases are supervised by IBM. Blue mix in like way gives middleware relationship to your applications to utilize. Blue mix gets up to speed for the application's motivation when it acquisitions new affiliations cases, and after that ties those relationship to the application. Your application can play out its certifiable occupation, leaving the relationship of the relationship to the establishment. As a rule, you don't need to push over the working structure and establishment layers when running applications on Blue mix. Layers, for example, root file systems and middleware areas are exceptional with the target that you can concentrate on your application code.

IIOAB JOURNAL
ISSN: 0976-3104

RELATED WORK

Complications of reliability in cloud computing

Interdependence & Corroboration: Cloud taking care of, subordinate upon the kind of cloud and besides the transmission appear, exhibited customers should immediately be secured and running with get to necessities and assents might be yielded in like way. This system is focus at scrutinizing and appreciative single cloud clients by utilize usernames and passwords assertions' to their cloud profiles Dispensation is a fundamental information reliability need in Cloud enrolling to ensure remission integrity progresses at the same rate. It takes after on in pertaining ascendancy and normal flexibilities over methodology streams inside Cloud figuring. Endorsement is kept up by cloud organization supplier.

Privacy in Cloud handling, security has certifiable effect particularly in supervising of cloud organization provider control over affiliations' information planned transversely finished different appropriated databases. It engages need when utilizing as a part of open in light of incontrovertible supremacy identity. Broadcasting protection of clients' outline and making their data reliable got the chance which considers the reliability of data customs to be affirmed [3].

For the two originalities utilizing cloud conditions and cloud suppliers, to make the data reliable, a dubious limitation is encoding. Vormetric encoding offers an unsophisticated methods for security containing key administration, fine-grained get to controls, and imaginative security knowledge information to keep delicate information very still inside various cloud situations i.e. open, private, mixture mists [4]. By means of encoding the cloud to use for cloud applications, one can meet understanding goals for encryption, flight of duties, and get to controls for secure data, including PCI-DSS and Data crosswise over Borders [5].

The dangers likewise incorporate those displayed by the disclosure of customer information to cloud suppliers and of information is conclusion as of the normal, blended information stockpiling used to sustenance cloud conditions. Additionally, distributed computing encryption(s) offers crude security insight on information access to encryption monitor data; such knowledge bolsters a Safety Data and Event Organization (SIEO) answer for recognizing dynamic diligent dangers or vindictive insiders [6].

Encryption provides a solitary, available elucidation that can just scramble any document, database, or accommodation wherever they live on kept up powerful and record frameworks, without prior application institution and keeping in mind that going around primary controlling trouble. Besides, cloud encryption contains nonstop key administration inside the clarification and is completely certain to applications and shoppers, consequently allowing existing strategies and strategy to persevere without any alterations [7].

The paper proficiently guards any information inside cloud situations. Correspondingly, the proposition of the cloud arrangement systems for upkeeps far reaching, strategy based separating of obligations is to present a perplexing level of reliability. The managers of cloud and the chiefs of origin and structure framework try to acquire illegal automatic ingress so that they can measure information. This can be counteracted and reasonable purchaser-implementation use can also be permitted.

Vision and Malthus, a secured information supplier of cloud, expels a danger that outstands personal information as well as information stockpiling that a solitary juncture has. They similarly proposed elucidations that point in high information in mists for simple joining with SIEO arrangements and to give finish information on utilize and get to. Get to endeavors utilizing SIEO arrangements enable computations to decide dangers to applications, and even executives. As far as encoding in cloud situations, Malthus enables associations that can screen if their data are shielded from the unhindered; it has diverse implementations and is a crossover cloud; conventional data file assets likewise exist on start [8].

A solitary, halfway expert course of action over all circumstances encourages the administration of cloud information security and in addition information security for physical and compelling datacenter properties. Notwithstanding, providers of cloud administrations make high esteem offices that have intensified information security offices in personal mists: SaaS, PaaS, IaaS, SaaS obliging, and a few others. Contemplating this, current encoding of cloud is a model arrangement as it is multi-inhabitant readied and versatile, is completed securely, and incorporates APIs and interfaces that are fundamental keeping in mind the end goal to work in collaboration with existing framework.

In June 2013, Edward Snowden disclosed the principle unpretentious components of the perception procedures of the NSA to the correspondents. With this, the field specialists foreseen that Snowden's exposure would unfairly impact cloud game plan masterminds. In August 2013, the DTIF said that the openings cloud would realize that the providers of cloud in the US lose 10% to 20% of the business to remote contenders overseas. In 2016, the DTIF said that the cloud providers would lose around 35 billion dollars in prospective arrangements. The CSA got a response from the European associations as to fears that the U.S. government is going to have induction to their information. In any case, following six months, the effect is all in all less extraordinary than had been typical. Regardless of reports of moderate offers of

ISSN: 0976-3104

the organizations of cloud by the US venders to abroad associations, and masters await the discharges uncovered by Edward Snowden are going to have small-scale impact on long-368 term bargains.

Encoding of Data: The breaks by Snowden pulled in a great deal of consideration inside the area of encoding. Thus, real administration contributors, as Microsoft, Yahoo, and Google, have since other coding to end-to-end information facilitating and administration for buyers. The present Google Cloud Storage mechanically encodes entirely pristine information recorded to plate. Server-side coding can be be offered in the blink of an eye for late information keep in Google mists.

Since the holes, Microsoft broadcasted its expectation to expand bolster for coding differed administrations like Outlook.com, Office 365, SkyDrive, and Windows Azure. By 2014, Microsoft hopes that can finish an occasion of standards for coding data exchanged betwixt purchaser locales and server farms and information in travel betwixt its individual information datum. Practically like Google, Microsoft wants to deal with information in shifted cloud specialist co-ops' mists.

Drop-down, Sonic.net, and Spider Oak have broadcasted bolster for comparative projects, encoding, alternatives, subsequent confirmation encoded information, and 2048-piece keys for the "ideal forward mystery" procedure. In accordance with specialists, these measures square measure essential for protecting the development of information between the shopper partnerships and thusly the providers of cloud administrations. Characterized reports from the NSA demonstrate that they're making an endeavor to debilitate coding calculations used by the overall population. The tap fiber interfaces that associate datacenters and repair providers offer the driving force for these endeavors.

Key administration and learning possession: in accordance with the United States, all through its debate with Lava bit, a protected email administrations provider, cloud benefit companies should fork over their coding keys once inquired. Such explanations have focused on sizeable consideration on key administration and learning possession. Eric Chiu, the leader of Trust, a cloud foundation administration organization, affirmed that however coding endeavors by benefit contributors caper a noteworthy half in up the reliability of cloud, their adequacy is prohibited.

Respectability: The validity essential care inside the server area, on an exceptionally fundamental extent in which the user gets to the data. In this way equality, stability, supervision are should make sure be viably compelled over all Cloud enlisting pass on models.

The orders utilized as a part of the Transportation Layer Security (TLS)/Protected Sockets Layer (SSL) strategy are represented. When TLS/SSL segments of anticipated structure had been nearness controlled, we test the division which is not used properly with complex salaries on chaperon as well as customer sides which occasional estimation has given as an outcome along with correspondence hold-ups which follow if complex as well as division tasks at hand change. At a point when the stated framework as well as calculation belonging are not used properly, the TLS/SSL yield is upgraded by abusing use of stated assets.

Exerting a chose pressure procedure to a TLS/SSL affiliation is not going to be ideal if the affiliation as well as calculation work region unit very surprising and dynamic. On the off chance that over the top information territory unit stacked for a meager data transmission TLS/SSL affiliation, pressure instrument intelligent setting heterogeneousness have to be connected. Notwithstanding, contemplating that normal TLS/SSL instruments give an unchanged pressure manner, realignment ask for by an implementation ought to change pressure algorithmic control that has to be connected. Consequently, component which licenses TLS/SSL to recognize the difficult pressure strategy for TLS/SSL associations in an exceedingly auspicious and clear way ought to be connected though considering the viewpoints given.

To begin with, we have a tendency to present firmly coupled, rib TLS/SSL composing, with the objective of boosting calculation and correspondence usage once TLS/SSL information sections territory unit sent and got. In run of the mill TLS/SSL, calculation schedules, similar to pressure and encoding operations likewise in light of the fact that the TLS/SSL organize schedules range unit dead in an exceedingly 369 approximately coupled way. This kind of implementation prompts visit impedance as well as stand performances inside TLS/SSL strategy.

Non-disavowal: Non-foreswearing in Cloud enrolling might be acquired by appertaining standard e-trade reliability customs as well as indicative workplaces to information transferal within the cloud acquisitions, for example, moved imprints, timestamps as well as proclamation proceeds associations.

The use of encoding and interpreting thoughts, to extend the protection of encrypted data that the customer transferred to the cloud server is examined in V.Masthanamma, G.Lakshmi Preya[9], The essential goal is to scramble and unscramble the information in a private way along weariness of lessened cash in encoding and unraveling process. Various amounts of keys will be made. So by repeating the strategy, keeping the strikes to extend the reliability of decoded data which the customer has transferred to the server in cloud has been made. The guideline intent is to scramble as well as decode the data in a shielded course with weariness in encoded as well as altering procedure. Various amounts of

IIOAB JOURNAL
ISSN: 0976-3104

keys are made as well as fundamental strikes are brought down. So by reiterating method it is utilized once more.

The paper of Mr. Akash Kanade et al [1] depicts that in the Partitioning Technique composing review is accomplished for data reputability examining, data stockpiling systems as well as encoding utensil. Dispensed arrangement is used so that the accessibility, data standards, uprightness of time tested accumulated organizations. The information limit using effectual data implementation method is utilized to accomplish diverse activities. Reliability examination is to encrypt the data by RSA.

The paper of Kiruthika R et al [10], describes figures , speak utilize distinctive pieces eradicates the keys in AES, which is a present drawback of DES and in AES. An execution relationship among celebrated calculations for different micro controllers shows that Advanced encryption standard has a PC cost of an indistinguishable demand from required for Triple Data encryption standard.

Another execution appraisal reveals that Advanced Encryption Standard has ideal position over figuring's 3Data encryption standard, Data encryption standard to the extent implementation period with different package magnitude as well as yield for encoding as well as furthermore unscrambling. Moreover by virtue of changing information sort, for instance, picture as opposed to alternate calculations.

The paper of Nasrin Khanezaei, Zurina Mohd Hanapi [2] portrays that various analyzes using encryption systems, distinctive strategies. Despite with the adjustment in the outcomes differentiating and the brisk improvement of distributed computing correspondences is taken care. Normally, reliability prototypes which are based on the cloud circumstances are isolated to confirmation prototypes, for instance, data affirmation prototypes, for instance, as well as get to organization prototypes, for instance. Using a blend of steganography encoding estimations, for instance, propelled encryption standard is one of the possible confirmation answers for securing circulated capacity organizations.

The fast development of the distributed computing market has likewise raised numerous genuine concerns with respect to information security and information administration, and these are thought to be the real boundaries to more extensive reception of cloud computing [11].

A study on security issues in benefit conveyance models of distributed computing, which concentrate more on characteristic reliability complications which have emanated due to the idea because of which the managing transference prototypes of a dispensed computing system [12.]

The paper [13] gives the investigation of information security issues and security insurance issues identified with distributed computing by keeping information access from unapproved clients, overseeing delicate information, giving exactness and consistency of information stored.

Sabarish et al., [14] have tended to various security challenges identified with cloud specialist co-op. Computerized stockpiling of PC information is pushing toward distributed computing which is an arrangement of framework gives information stockpiling to associations and people. Due to this huge scale, in the event that an assault happens in the system of a cloud it would be a major test to explore the cloud. [3]

The shifted security parts of security issues have been investigated thus proposes a structure to alleviate security issues at the sum verification and capacity level in distributed computing. Temperate security components should be sent by recommends that of coding, validation, and approval or by another philosophy to ensure the protection of customer's information on cloud storage [15].

PROPOSED METHOD

Encoding and decoding techniques

In order to make the encoded data of the customer reliable to the server in cloud is considered. The principal intent is to encode as well as translate data in a private utilizing short period as well as cash inencoding along with deciphering procedure. Various amounts of keys are to be be delivered including general assaults that are to be observed. This strategy encourages the user to let the assaults remain.

The strategies included are:

- Key creation
- Encoding
- Decoding

Encoding procedure

In the encoding procedure, a normal fonts in continuation of numbered modulo n. Using this, cipher text can be applied from plain text M. This is given like D=F g mod n,
Here D, is cipher text

ISSN: 0976-3104

F is word font
g is known key
D is unknown key

Decoding procedure

The backward procedure of encoding and decoding is decoding.
That is given as:
F= e mod n.
Where D =cipher text
F=word font
g =known key; D =unknown key

Partition Algorithm

Step 1: The input program along with its expanse is stacked.
Step 2: The program's expanse is examined.
Step 3: If expanse=invalid, state as invalid expanse.
Else expanse= s
Step 4: The program is divided into recorded and augmentation value.
Step 5: Send back files.

Merging algorithm

Step 1: Gather the fragments of decoded documents.
Step 2: Examine data progress.
Step 3: If data! Then not found
Else
Step 4: Margin quantity is taken
Step 5: Combine files.
Step 6: Back files.

Advanced Encryption Standard (AES):

The AES is a uniform key code in which the expanses of pieces are of 128 bits. The value is of can be of various bits.

Steps involved are:

- Ten rounds for hundred and twenty eight bits.
- Twelve rounds for hundred and ninety two bits.
- Fourteen rounds of two hundred and fifty six bits.

Rivest shamir adleman algorithm

It's an unsymmetric public key which is utilized to assist the encoding passwords. The encoding and decoding are carried out privately, hence G-mail, y- mail.

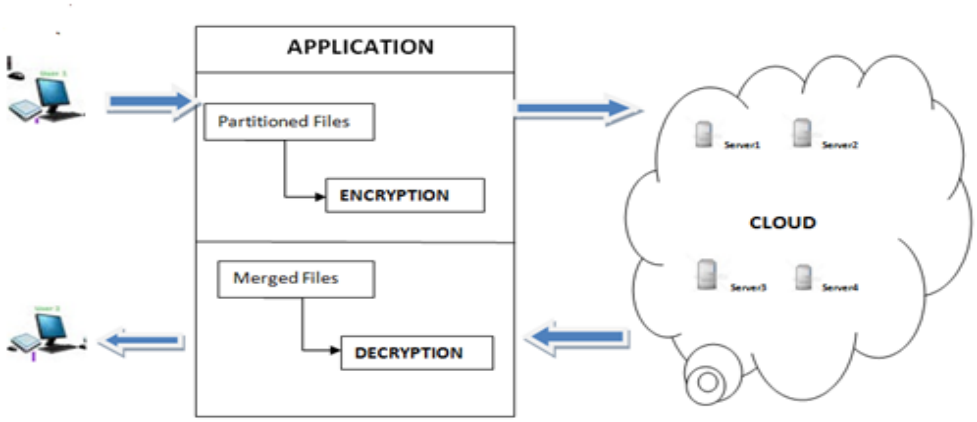

Fig. 1: Application architecture

The architecture of [Fig. 1] clarifies about how the engineering functions viably for the data to be exchanged in a protected way. In this context, the design incorporates customer, Server including software which is utilized to prepare the encoding as well as decoding procedures. In his context,

IIOAB JOURNAL
ISSN: 0976-3104

customer transfers the information's to the software in which the information is parceled as well as scrambled. At that point this information is transferred to the server in the cloud. This information is decoded, later combined, that are returned to the customer. It is finished along with proficient steganographic procedures in which utilization of uniform and lopsided calculations co-operatively that give greater reliability.

SYSTEM IMPLEMENTATION AND RESULTS

The plan of modules manages the accompanying:

Utilizer's Incorporation

In cloud innovation, the utilizer peruses the program by perusing interfaces. Client interfaces with this program to play out an errand. At the point, a program peruses a contribution from the client. After that, the program can interface with the environment in the cloud.

Partition

Client collaborates with program to parcel the information as well as save onto different servers. At the point at which the record went to the program that it is going to parcel. At the point at which a program peruses a document, it partitions as well as afterward connections distributed reserve. Later record gives demands as well as exchange to the coveted asset in the cloud.

Encoding

In this context, clients' encouraged to carry on the encoding procedure to give reliability divided records. The apportioned documents' are scrambled along with half breed steganography procedure use of uniform including hilter kilter calculations to give greater reliability.

Consolidation

The information is converged from servers which are later transferred to following procedure. The systems administration ideas in bluemix utilized here the combining procedure. Once the information is consolidated as well as finished along with decoding, the allotted period is going to be decreased.

Decoding

In this context, the clients' encouraged with the unscrambling procedure keeping in mind the end goal to give security to the combined records. The apportioned documents are decoded with the half and half cryptography system utilization of uniform as well as lopsided calculations which give greater reliability.

RESULTS

The application process includes creation of an application, edition of the code, source control and build and deployment. For this have to login to the IBM blue mix as given below:
a)

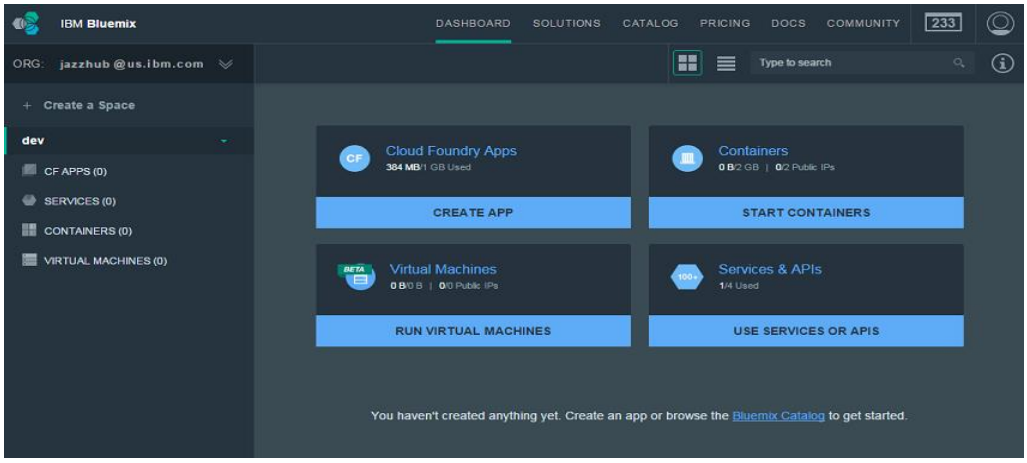

Fig. 2: Login to the blue mix page

The login procedure needs a pre-procedure of enrollment in the IBM blue mix. Through signing in the record, the dashboard in which the dashboard can be discovered that demonstrates the Cloud foundary applications, compartments, virtual machines and administrations.

b) Application can be created as shown below which deals with a couple of types of programs that could be created as well as picked when generating i.e., if for web or mobile application.

IIOAB JOURNAL
ISSN: 0976-3104

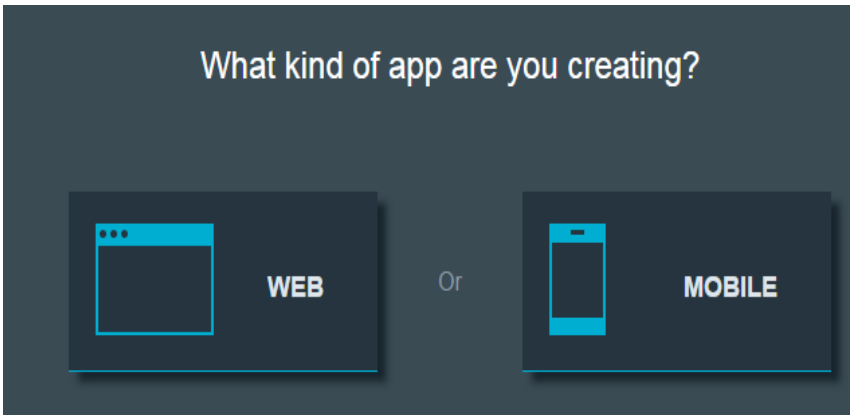

Fig. 3: Design of creating web or mobile application

c) Addition of GIT repository is made which is added and when EDIT code option is submitted to code the application with the functionalities that is required.

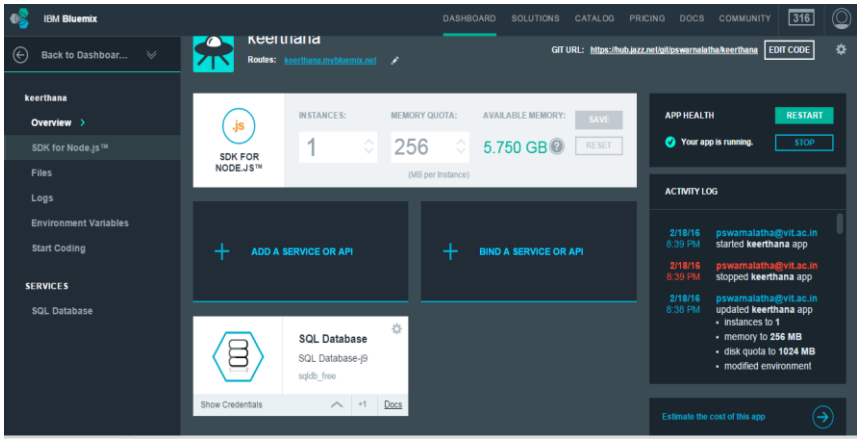

Fig. 4: Creation of an application with their operations created application with edit code.

CONCLUSION

A blend of shaky and adjusted encoding procedures (i.e. Rivert Shamir Adelman and Advanced Encryption typical systems) route for managing accomplish affirmation of cloud information separation. The significance was on Rivert Shamir Adleman encoding to offer inconvenience to aggressors and diminishment the period of information exchanging by using Advanced Encryption Standard encoding methodology. Methodology of transferring reports to server as well as recuperating documentations from cloud had been capable through uniform encoding independently. Using adjusted encoding technique, some portion will recoup the reports from the server which had been a consequence of the key dissemination problem. This problem gives a consummate out-turn in light of the way which is making different keys in a time span devouring. In like manner, the encryption technique winds up being twofold and dynamic, if there is extension of the report measure of two hundred and fifty six numbers. The measure of keys made for each record. The number finds the opportunity to be triple conditions for each estimation of reports set away in the cloud. As requirements could be an important problem that has to be managed for a liberal accumulated structure and moreover, the encoding as well as unraveling handle that done every two times each records structure overhead. A little while later, showed up contrastingly in connection to prevailing proficiency a hybrid approach for encoding, for example, it's more private to use. The specific shortcomings in future attempts will refresh the security of coursed taking care of associations.

CONFLICT OF INTEREST

There is no conflict of interest with any author regarding publication of this article

ISSN: 0976-3104

ACKNOWLEDGEMENTS

The authors of this paper express their gratitude to The Professor and Head, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirapalli Tamilnadu, India for providing guidance and support for this research work.

FINANCIAL DISCLOSURE

This research work was carried out without financial support from any organizations.

REFERENCES

[1] Kanade, Mr Akash, et al. [2015] Improving Cloud Security Using Data Partitioning And Encryption Technique, International Journal of Engineering Research and General Science. 3(1): ISSN 2091-2730.

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

[3] Sulabha Patil, Uzma Ali, Dharaskar R V. [2015] Design and Development of System for detection of security Breach in Cloud environment, International Journal of Advance Research in Computer Science and Management Studies. 3(9):221-227.

[4] Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. [2013] A survey on security issues and solutions at different layers of Cloud computing, J. Super comput. 63(2):561–592.

[5] Jensen M, Schwenk J, Gruschka N, Iacono LL. [2009] On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing. 109-116.

[6] Cloud Security Alliance. [2013] The Notorious Nine. Cloud Computing Top Threats in 2013, Security,1–14.

[7] Rodero-Merino L, Vaquero LM, Caron E, Muresan A, Desprez F. [2012] Building safe PaaS clouds: A survey on security in multitenant software platforms, Comput. Secur. 31(1):96–108.

[8] Jens-Matthias Bohli, Nils Gruschka, et al.[2013] Security and Privacy-Enhancing Multi cloud Architectures, IEEE Transactions on Dependable and Secure Computing. 10(4):212– 224.

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

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

[11] Sharanjit Singh Er, Rasneet Kaur Chauhan Er. [2015] Introduction to CryptoCloud in Cloud Computing (IJETCAS) ISSN (Print): 2279-0047, ISSN (Online): 2279- 0055.

[12] Subashini, Kavitha V. [2011] A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications. 34:1–11.

[13] Jeevitha B K, Thriveni J, Venugopal K R. [2016] Data Storage Security and Privacy in Cloud Computing:A Comprehensive Survey,International Journal of Computer Applications (0975 – 8887).156(12).

[14] Srinivas J, Venkata K., Reddy S. and Qyser A. M. [2012] Cloud Computing Basics", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 5, 2012,343-347.

[15] Deepika. [2017] Enhancement of Data Security for Cloud Environment Using Cryptography and Steganography Technique, International Journal of Innovative Research in Computer and Communication Engineering. 5(1):225-230.