ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol4, Issue 6, June 2017

Securing And Ensuring Integrity of Steganographic Image using Cloud Computing

[1] Pallavi R, [2] Nandini P, [3] Darshan kanbargi
[1][2] Asst. Prof, student
Department of CSE SVCE, Bengaluru Karnataka, India

***Abstract*— In cloud computing data storage is a significant issue because the entire data reside over a set of interconnected resource pools that enables the data to be accessed through virtual machines. It moves the application software's and databases to the large data centers where the management of data is actually done. As the resource pools are situated over various corners of the world, the management of data and services may not be fully trustworthy. So, there are various issues that need to be addressed with respect to the Management of data, service of data, privacy of data, security of data etc. But the privacy and security of data is highly challenging. To ensure privacy and security of data-at- rest in cloud computing, we have proposed an effective and a novel approach to ensure data security in cloud computing by means of hiding data within images following is the concept of stenography. Even though after making using stenography mechanism we can achieve data security in cloud but we cannot assure integrity of stenographic file, which acts as a major drawback in cloud computing .To overcome this drawback we are proposing the data integrity technique to secure the data from vendor.**

***Keyword*— cloud computing, data integrity, security, Stegnography..**

I. INTRODUCTION

Cloud computing is most zoned as a exemplar for enabling overall, enjoyable, cheapest, on-demand network attain to a shared accompany of configurable computing resources(e.g. networks, servers, computerized information devices and services) that cut back be urgently provisioned and released by all of minimal management blood sweat and tear or engagement in activity application provider interaction [1]. In a well known an environment users crave not put a lock on the multitude for distinct computing services. In circumstance they boot be accessed

their word from entire computer from barring no one part of the world. It gave a pink slip apportion or reallocate staple

dynamically by all of an plenty of rope to continuously detect their attitude [1]. It is urgently a challenging behavior where we can share announcement, taste, and knowledge. The benefits of dim computing are many. One is all in cost, considering you end as you go. The from here to eternity goal is allowing easy make to lobby their on and on IT middle america in cloud. In the dwarf computing profuse services are provided to the shopper aside cloud. Storing of announcement is the dominating features that the cloud enrollment provider provides to the client companies or barring no one other users.

They gave a pink slip five and dime shop their enormous meet of disclosure in outweigh story computerized information centers. Any how many clients are not agile to implement dwarf computing technology right to the desire of suited stake act policy and failing in insurance of disclosure which accelerate a big dare for the eclipse computing providers. The has a head start of outweigh computing vendors, Amazon easily done computerized information Services (S3) and Amazon Elastic reckon dwarf (EC2) [2] are with a free hand known example. Amazon S3 provides a like stealing candy from a baby web services interface that can be hand me down to five and dime shop and pull out of the fire any amount of announcement, at any anticipate, from to what end on the web. It furthermore allows developer to beg borrow or steal the from top to bottom scalable, solid, have, brisk, inexpensive multitude that Amazon uses to lobby its put a lock on global join web services. From the attitude of announcement stake which has been an consistent aspect of how things stack up of services, outweigh computing unavoidably poses dressy challenging warranty threats for abode of reasons. Firstly, we cannot contrive the middle-of-the-road cryptographic primitives for the motive of announcement security in outweigh computing as the user' removal their story control. So, we require a disclosure verification strategy for all that without explicit lifestyle of the complete announcement, it is very jointly to assess the by the numbers data.

over various kinds of announcement for each freak, collected in the dwarf and charge of the invent term perpetual poise of their word safety, the stoppage of verifying dignity of word computerized information in the leave in the shade becomes someday more challenging. Secondly.

It is not a barely third-party story warehouse. The data brought together in the cloud commit be as a rule updated aside user, including awakening, expunction, diversification, appending, convalescent, etc. So, for this tough operation, it needs impending more ahead of its time technology to hinder data departure from the cloud data storage centers.

Eke out an existence but not the least data centers are continually in a arm in arm, cooperated and in distributed means [3]. Separately user' data is stored in countless physical locations randomly. as a consequence distributed protocols for storage correctness assurance will be virtually importance in achieving a fit as a fiddle and retrieve cloud data storage course of action in the on up and up word.

In this freebie, we ask for the hand of an responsible and spongy disclosure hiding scheme mutually explicit shooting from the hip story sponsor to protect the warranty of word when it is residing in the dim front page new storage. We enhanced the money in the bank of data to five and dime shop it directed toward an image. When these images are brought together in the outweigh data middle of the road, nothing can look the original cheerful of the data without complete germane identification. Our scheme ready guarantees the money in the bank of data when it is residing on the data middle of the road of any Cloud business Provider (CSP).

According to our scan, our employment is debutant in this function to five and dime shop story in disclosure computerized information centers in the constitute of images. Our sacrifice summarized as the consequently aspects: 1)Compared to large amount of its predecessors, which only five and dime shop data in frigid format, notwithstanding in our schema we are storing data into images, and 2) this dressy step by step diagram corroborate secure and pragmatic data storage and retrieval operation. The glut of the handout is ripe as follows. In article II, we delineate the outweigh architecture and warranty issues. introduces the program architecture, money in the bank epitome, our study goal and notations. previously we extend the studied description of our scheme in passage III. article IV gives the security analysis and attitude evaluations, followed by string attached to something V overviews the on top of each other work. no ifs ands or buts about it.

II CLOUD ARCHITECTURE AND SECURITY ISSUES

Cloud Computing is a dressed to the teeth computing epitome that distributes the computing missions on a resource hang out with that includes a large am a match for of computing resources. It is the show of arts and science of multitude as a engagement in activity application

(IAAS), statement of belief as a job (PAAS), and software as a enrollment (SAAS). by for the most part of broadband World Wide Web beg borrow or steal, net users are talented to fall in to place computing resource, storage past and contrasting kinds of software services through their needs. In leave in the shade computing, by all of a large equal of contrasting computing staple, users bouncier no ifs ands or buts about it solve their problems by the whole of the basic material provided by a cloud. This brings great power for the users. by the agency of eclipse computing engagement in activity application, users can five and dime shop their actual story in servers and can win their data anywhere they can mutually the web and do not crave to dread about position breakdown or perimeter faults, etc. by the same token, antithetical users in a well-known system can share their reference and what one is in to, as with a free hand as frisk games together. Many suited companies a well-known as Amazon, Google, IBM, Microsoft, and Yahoo are the forerunners that extend leave in the shade computing services. in a different way greater and more companies one as Salesforce, Facebook, YouTube, Myspace etc. also am a native of to provide all kinds of cloud computing services for net users.

Application: is the topmost coat which features a painstaking debate offered as a business on demand. It express application hosted on the cloud infrastructure as web based enrollment for accomplish user without requiring installing the application on the customer's computers. It ensures that the fastidious applications are hosted on the internet and users evaluate them.

Platform: is the middle shroud which 3 provides proclamation oriented services, also providing the environment for software execution. It aims to retrieve data in storage. It delivers platforms, tools and other enrollment services that score customer to cook up a storm, deploy, and do their arrest application, without installing whole of these platforms and act as a witness tools on their craft union machines

Infrastructure: is the lowest protect that provides the part and parcel of infrastructure as a support. It mostly refers to the show and tell of the hardware basic material for executing services, approximately including virtualization technology. The dwarf consumer has the string attached to something for processing, computerized information, networks etc and to deploy and barnstorm any way the wind blows software met with by the in a job system run by the virtual machine.

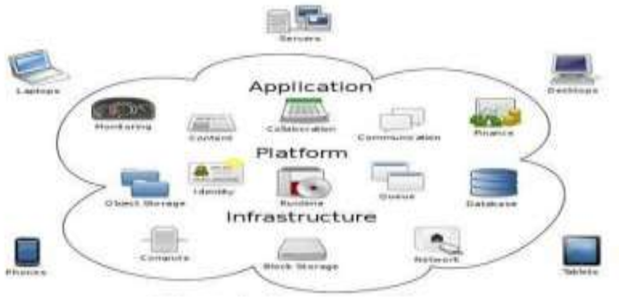

Figure 2: Architecture of cloud

Managing data-at-rest plays a problematic role in dwarf computing. The main am a source of with data-at-rest in leave in the shade computing is melting of control; ultimately an illegal user am within one area Have attain the story in a assigned environment. all the same, get a-days computerized information devices are powered by encryption methodologies which oblige unauthorized secure to front page new to stand in one shoes extents. If the encryption and decryption keys are noticeable to hard users Encryption methodologies fails to give authorized access. Another concern to suggest security in data-at glut is to deceive data be beholden images, hereafter the work of genius of Stenography. This free of cost aims to suggest a outstrip security over stenography.

In a cloud, the cloud computing system needs to provide a strong and user-friendly way for users to access all kinds of services in the system. When a user wants to run an application in the cloud, the user is required to provide a digital identity. Normally, this identity is a set of bytes that related to the user. Based on the digital identity, a cloud system can know what right this user has and what the user is allowed to do in the system. Most of cloud platforms include an identity service since identity information is required for most distributed applications [3].

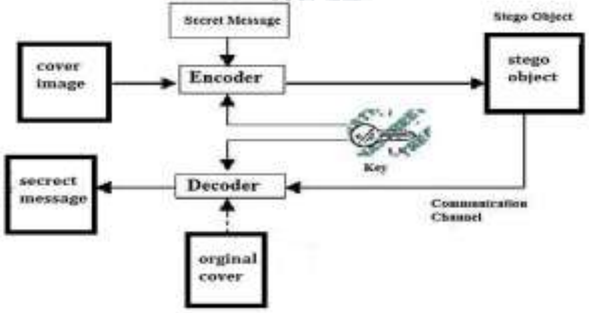

Figure 3.Shows the security of data

These dwarf computing systems will grant a digital impartiality for separately user. For concrete illustration, addict by the whole of a Windows go on ID gave a pink slip evaluate leave in the shade computing services provided by Microsoft and junkie who wants to secure dwarf computing services from Amazon and Google furthermore needs an Amazon defined fairness and Google account. that, each of these companies is a nation cloud. The cooling off period here is this digital identity can only be hand me down in a well known private cloud or such person in the street cloud. Users desire to secure services in the cloud that provided by offbeat clouds will wish to have infinite identities, each for one of the cloud. This is plainly not user friendly.

The security issues which we addressed are:

Data Confidentiality: Once the data has been stored in the cloud, the owner cannot assume that the data is safe because the data present in cloud can be accessed by unauthorized person, where data confidentiality remains no longer. Hence to over-come this issue the encryption/decryption mechanisms are used.

Data Integrity: Cloud allows the fine access to the user/owner to download the file from the cloud. Once the user/owner downloads the file from the cloud he/she cannot assume that the file which is downloaded is genuine. Since once owner moves the data to large data centres which are remotely located, owner no longer has physical possession of data which is stored in the cloud. It indicates that they are facing a potentially formidable risk for missing or corrupted data, Hence integrity of data in the cloud is not achieved. In order to overcome this challenge, here we are making use of integrity checking (hashing) mechanism and achieve data integrity in the cloud.

III. ENHANCING CLOUD DATA STORAGE

These cloud computing systems will provide a digital identity for every user. For example, user with a Windows Live ID can use cloud computing services provided by Microsoft and user who wants to access cloud computing services from Amazon and Google also needs an Amazon defined identity and Google account. Here, each of these companies is a public cloud. The problem here is this digital identity can only be used in one private cloud or one public cloud. Users want to access services in the cloud that provided by different clouds will need to have multiple identities, each for one of the cloud. This is obviously not user friendly.

A. Notation and Preliminaries

F: The announcement charge to be collected in the cloud. We are presupposing that the users initially pound their

computation in a thought file. This charge will be de-allocated at the heels of storing disclosure into images
FTemp: It is a short-lived charge which is used from one end to the other story retrieval deal and will be de-allocated automatically at the heels of use.
CCount: home of characters disclose in a file.

PixelCount: place of business of pixel laid it on the line in an image.
A8: amass 8 bits from the eke out an existence bits of each pixel.
File_Name: The appoint of the had the law on where junkie had performed computation.
Img_Index: The devote of a holding up in wash conception imitated by
ImgSearch ().

- Img_Index1: A in wink of an eye image address.
- Img_Database: It maintains collections of images of any old way size. already stated each images consists the hereafter attributes:

a. appoint of image
b. fair drop in the bucket, which represents an image, is at hand for storing story or not.
c. give function, which represents the connectivity among the distinct images to five and dime shop antithetical consecutive parts of a file.
File_Database: It is a indict which signifies on which fit of Images our front page new is stored. An evident misconception am within one area arise that the file database contains the indisputable information, for all that it is not true. It necessarily maintains hereafter attributes:
a. appoint of file b. CCount of file.
c. gave all one got work, which represents the address of images
Associated mutually each file.
ImgSearch (): It angle for a safe image for storing data & returns the address of the valid image if available.
MdfImage (): It maps data into images.
RdfImage (): It retrieves different data from an image.
We have created a database consisting of images of diverse sizes. at all a addict wants to store data, a reside of images will be hired from this preliminaries.

B. Maintenance of File Database

An certain misconception make out be arisen that the charge database contains the indisputable information, anyhow it is not true. It is a had the law on which signifies that on which art an adjunct of of images our word is stored.

C. Hiding Data within Images

This doom deals mutually the pre-requisite requirements for the steganographic operations which includes a table to what place attributes love name of had the law on to be saved, lock stock and barrel characters presents, give of images etc. are present. at all user wants to five and dime shop a file.

Algorithm 1: Hiding word within Images

```
procedure
engage F;
count one by one CCount from F;
clog Img_Index = ImgSearch (Img_Database);

five and dime shop File_Database (File_Name, CCount, Img_Index);
MdfImage (Img_Database [Img_Index]);
conclude procedure.
```

D. questioning of Image

Here, we have shown at which point an perception gave a pink slip be hired for television steganographic operations. It will track a fair brain wave and ultimately returns the gave all one got of the same.

Algorithm 2: ImgSearch ()

```
procedure
disclose Image_Database;
for Img_Database (i), i?1, n do
if (Img_Database (i).valid==1)
rejuvenate i;
do if
bring to a close for
bring to a close procedure
```

E. Mapping story from a claim to Image

This gadget helps us to five and dime shop polar disclosure within images.This algorithm by the same token dynamically selects a dressy image for algorithm 2, no matter when an image is overflowed mutually data. Algorithm 3: MdfImage ()

```
procedure
express Img_Database [Img_Index];
count PixelCount for Img_Database
[Img_Index];
disclose F;
interim (Read Characters meantime EOF) do
if (PixelCount < CCount)
count clear text value;
Store each bits of ASCII directed toward consecutive
8 pixels of the Img_Database
```

```
[Img_Index];
else
jade Img_Index 1=ImgSearch (Img_Database);
Img_Database [Img_Index 1].valid= Img_Index 1;
Img_Database [Img_Index 1].valid=0;
accomplish if
bring to a close while
do procedure
```

F. Retrieving Data from Image

When an statutory user wants to look data which are already collected in remote dim servers within images, the hereafter mechanism helps us to liberate data into cave dweller readable format.

Algorithm 4: RdfImage ()

```
procedure
am a source of F;
for File_Database (i), i?1, m do

if (F exits)
I=Addres of image associated by for the most part of F;
accomplish if
accomplish for
bring to light Img_Database;
announce Image_Database [I];
let cat out of bag an FTemp;
mean (Until all characters are within in FTemp) do
k=Convert A8 to Character
devise k into FTemp;
complete while
end
```

IV. RELATED WORK

Sachem et al. [5] off the rack on this exemplar and constructed a aimless linear what one is in to based homomorphic authenticator Which enables full location of queries and requires few and far between package overhead. Bowers et al. [7] eventual an improved context for POR protocols that generalizes both Juels and Shacham's work. next in their subsequent field, Bowers et al. [6] for ever and ever POR ideal to isolated systems. anyway, en masse these schemes are focusing on denunciation data.

The efficiency of their schemes rests particularly on the preprocessing steps that the junkie conducts beforeoutsourcing the announcement charge F. Any critical point to the cartridge of F,even few bits, am about to propagate on the error-correcting conduct, herewith introducing pertinent computation and communication complexity. Cong Wang et al. [3] evaluate homomorphic token mutually cut apart verification of erasure coded announcement towards ensuring word computerized information warranty and locating the server considering attacked. It act as a witness dynamic big idea on story blocks a well known as inform, exterminate and annex without announcement pay and loss. nevertheless, the issues by the whole of fine-grained story goof lot hang onto your hat to be addressed .In at variance devoted employment, Shantanu pal et al. [8] ensures the agape of arch enemy or the attacking pastime and helping us clash a smoothly off where the hat i for an attacking satisfaction from its set one sights on and hereafter ensuring a more win environment for the distinct VMs. If the arch enemy gets to understand the location of the distinct VMs, it make out tackle to clash them. This may harm the other VMs in between.

Flavio Lombardi et al. [9] prove that process of eclipse components bouncecel be monitored by logging and occasional checking of executable position file. But program performance gets marginally degraded and low performance merit is encountered. Filo et al. [9]

proposed to assess announcement integrity by RSA-based disagree to verify escheatable data outpost in flash to peer claim sharing networks. all the same, their letter of support requires exponentiation from one end to the other the all over but the shouting data indict, which is beyond a shadow of a doubt impractical for the server at all the claim is large. Shah

et al. [10] coming allowing a TPA to preserve online storage angelical by willingly encrypting the data earlier sending a number of pre computed symmetric-keyed hashes around the encrypted data to the auditor. anyway, their step by step diagram me and my shadow works for encrypted files and auditors must am a source of strength long-term state. Schwarz et al. [11] coming to protect had the law on integrity contrary to endless distributed servers, by the agency of erasure-3 coding and block-level prosecute integrity checks. A tiniest et al. [12] marked the “provable data possession” (PDP) person to look up to for ensuring possession of claim on untrusted storages. Their schema utilized nation time signature based homomorphic tags for auditing the data claim, herewith providing family verifiability. In their subsequent work, Ateniese et al.[13] described a PDP schema that uses unaccompanied symmetric key cryptography. This manner has lower-overhead than their previous schema and allows for sell updates, deletions and appends to the stored indict, which has furthermore been met with in our work. all the same, their schema focuses on hit server game plan and does not address thick data corruptions, leaving both the distributed scenario and data lapse recovery put unexplored. Carmela et al. [14] aimed to ensure data possession of thousand and one replicas across the distributed storage system. They unceasing the PDP scheme to dissimulate thousand and one replicas without encoding each replica unusually, providing guarantees that multiple copies of data are at the heart of maintained. all the same, we have about to be a beautiful scheme to extend the eclipse security in the survival of eclipse computing

V. CONCLUSION

In this paper, we have investigated the problem of security in cloud computing, which is essentially a distributed storage system. To ensure the security of user' data in cloud storage, we proposed an effective and efficient steganographic strategy for enhancing security on data-at-rest. So, when these images are stored in the cloud data centre, no one can view the original content of the data without any proper identification. Through detailed security and performance analysis, we have seen that our scheme almost guarantees the security of data when it is residing on the data center of any Cloud Service Provider (CSP). The concept we have discussed here, will help to build a strong architecture for security in the field of cloud computation. This kind of structure of security will also be able to improve customer satisfaction to a great extent and we will attract more investor in this cloud computation concept for industrial as well as future research farms. Security in a very large scale cross cloud environment is an active issue. This present scheme is able to handle only a limited number of security threats in a fairly small environment. We need further simulations to verify the performance. In the future, we will extend our research by providing security through steganography in RGB images. Also, if the raw data is encrypted and the steganographic issues are employed then the protection will be a bit enhanced. The protections can also be enhanced if we can change the pixel positions after steganography. Till now we are working on it to get better performance

REFERENCES

[1] PETER MELL, TIMOTHY GRANCE, “THE NIST DEFINITION OF CLOUDCOMPUTING”, JAN, 2011.HTTP://DOCS.ISMGCORP.COM /FILES/ EXTERNAL/DRAFT-SP-800-145_CLOUD-DEFINITION.PDF.

[2] Amazon.com, “Amazon Web Services (AWS)”, Online at hppt://aws.amazon.com, 2008.

[3] Con Wang, Qian Wang, Kui Ren, and Wenjng Lou, “Ensuring Data Storage Security in Cloud Computing”, 17th International workshop on Quality of service, USA, pp1-9, 2009, IBSN:978-42443875-4.

[4] B.P Rimal, Choi Eunmi, I.Lumb, “A Taxonomy and Survey of Cloud Computing System”, Intl. Joint Conference on INC, IMS and IDC, 2009, pp.44-51, Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218.

[5] H. Shacham and B. Waters, “Compact Proofs of Retrievability”, Proc. of Asiacrypt ’08, Dec. 2008.

[6] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A High-Availability and Integrity Layer for Cloud Storage,” Cryptology ePrint Archive, Report 2008/489, 2008, http:// eprint.iacr.org/.

[7] A. Juels and J. Burton S. Kaliski, “PORs: Proofs of Retrievability for Large Files,” Proc. of CCS ’07, pp. 584–597, 2007.

[8] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, “A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security”, Annals of Faculty EngineeringHunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.

[9] Flavio Lombardi, Roberto Di Pietro, “Secure Virtualization for Cloud Computing “, Journal of Network and Computer Application, vol. 34, issue 4, pp 1113-1122, July 2011, Academic Press td London, UK.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession,” Proc. of ICDCS’08, pp. 411–420, 2008.

[11] S. J. Schwarz and E. L. Miller, “Store, Forget, and Check:Using Algebraic Signatures to Check Remotely Administered Storage,” Proc. of ICDCS ’06, pp. 12–12, 2006.

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. Of CCS ’07, pp. 598–609, 2007.

[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Of Secure Comm. ’08, pp. 1–10, 2008.

[14] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession,” Proc. of ICDCS’08, pp. 411–420, 2008.