International Journal of Engineering Sciences &Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

Chief Editor
Dr. J.B. Helonde

Executive Editor
Mr. Somil Mayur Shah

RESEARCHERID
THOMSON REUTERS

[Kaur, *et al.*, 8(11): November, 2019]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA MIGRATION FROM A PRIVATE CLOUD TO A PUBLIC CLOUD USING STEGNOGRAPHIC APPROACH

Gagandeep Kaur[*1] & Er. Chamkour Singh[2]
[*1]M.Tech. Student, Guru Kashi University, Talwandi Sabo
[2]Assistant Professor, Guru Kashi University, Talwandi Sabo

DOI: 10.5281/zenodo.3559494

ABSTRACT

Cloud computing has recently became a widely discussed topic in the IT industry. More and more organizations consider using the Cloud, because it enables an easy and cost efficient way of hosting applications, with dynamic scaling and geographical distribution possibilities. Still, it isnot clear how and when cloud computing should be used. Existing application are often written ina way that does not really fit a cloud environment well. Also, certain quality attributes (e.g. performance, security or portability) can be affected. More studies are needed on how existing systems should be plugged into the Cloud and what are the consequences of the migration. Data migration and application migration are one of popular technologies that enable computing and data storage management to be autonomic and self-managing. We examine important issues in designing and developing scalable architectures and techniques for efficient and effective data migration and application migration. The first contribution we have made is to investigate the opportunity of automated data migration across multi-tier storage systems.

In the proposed system we have developed a novel approach for migrating the data on the cloud environment with the help of stenographic approach. In the proposed system data is first entered into the system and then hidden in the image after performing the encryption to the data. After encryption and data hiding the image is then migrated to the cloud.

KEYWORDS: cloud computing, public cloud platform, migration, enterprise application.

1. INTRODUCTION

Distributed computing typically alludes to an utility-based provisioning of computational assets over the Internet. Generally utilized analogies to clarify distributed computing are power and water supply frameworks. Like the Cloud, they give brought together assets that are open for everybody. Also, in the Cloud you only pay for what you have used. Lastly, it is normally devoured by the individuals who experience issues to create important assets without anyone else's input or simply would prefer not to do that. Despite the description by analogy, it is difficult to give a unique and precise definition. One of the main ambiguities to define cloud computing is the fact that it is still evolving and taking its shape.

The definitions proposed in the cloud computing community are often focused on different perspectives and do not have common baselines. Breaking down existing sources so as to distinguish regular qualities, Vaquero et al [7] watched no unmistakable and complete definition in the writing. By and by, the creators proposed three highlights that most intently depict distributed computing: adaptability, pay-as-you-go utility model, and virtualization – and gave the accompanying definition:

"Mists are a huge pool of effectively usable and available virtualized assets, (for example, equipment, improvement stages and additionally benefits). These assets can be progressively reconfigured to acclimate to a variable burden (scale), permitting additionally for an ideal asset usage. This pool of assets is ordinarily abused by a compensation for each utilization model in which certifications are offered by the Infrastructure Provider by methods for modified SLAs"[1].

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

1.1 Cloud Computing characteristics:

1.1.1 Virtualization (abstracted infrastructure). Distributed computing ended up conceivable through another development of virtualization. Virtualization empowers dynamic foundation use, asset sharing, seclusion and security. In contrast to a standard model when processing takes place on specific hardware defined in advance, applications do not have any static computing place in a virtualized cloud environment. Resources are allocated dynamically depending on the demand. Therefore, clients don't have the foggiest idea about the definite spot and the kind of equipment their applications are running on. Cloud providers can only guarantee minimum performance or storage capacity for the customer [2].

1.1.2 A pay-per-use model. This is the key normal for distributed computing financial aspects. All assets in the Cloud are accessible on an utility premise, implying that clients are charged dependent on the amount devoured by them. This model permits entering the market with no forthright speculations into claim equipment framework.

1.1.3 On-request get to. On-request access implies that assets like CPU time or capacity can be provisioned naturally when required with no additional administration exertion [3].

1.1.4 Elastic scalability. Elastic scaling signifies that computational resources, used by the application, can be dynamically scaled up or down. In other words, virtualized hardware resources can be resized easily and rapidly on demand. It makes a utility model significantly progressively appealing, in light of the fact that shoppers utilize just what they truly need.

1.1.5 Resource pooling. Figuring assets of the supplier are shared over numerous clients. Different resources are pooled in a multi-tenant way so that they can be dynamically assigned and reassigned to serve consumers' needs.

1.1.6 Network access. Everything in the Cloud is connected via the network. End-clients access administrations by means of the Internet, engineers send and screen applications similarly, correspondence between various administrations in the Cloud happens through the system. Distributed computing stages more often than not give REST-based APIs to their administrations [5].

1.1.7 Usability. Typically cloud computing platforms provide a simple externally managed environment to hide deployment and operating details from the user. Distributed computing frameworks give APIs to communicate the earth, which streamlines the improvement. Many of these characteristics are well-known from service oriented architecture (SOA),distributed computing, peer-to-peer, etc [8].

1.2 Classifications of the Cloud

There are two widely used cloud computing classifications. The first depicts four cloud types relying upon the arrangement area:

1.2.1 Public mists. Open or outside mists are conventional mists where assets are powerfully provisioned by means of the Internet by the off-website outsider suppliers. These assets are publically accessible to everybody. Cloud buyers are charged relying upon the amount utilized. Examples are Microsoft Azure, Google App Engine, and Amazon Web Services.

1.2.2Private mists. Private mists normally allude to the copying of a distributed computing condition on private foundation. Since clients still need to purchase equipment and working hardware, private mists are frequently condemned. Numerous organizations attempt this sort of cloud to check their product locally before conveying it to open cloud.

1.2.3. Network mists. Network mists implies a cloud situation set up over a few associations. Such clouds can be managed by the organizations or third-parties and installed either on- or off-premise.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

1.2.4. Hybrid clouds. This term refers to a composition of two or more clouds, including private clouds and public clouds. This model can be used for different purposes. For example, archiving or replicating local data in the public cloud, or dealing with peak loads when the on-premise system uses the public cloud capacity only when needed [4].

2. CLOUD DATA MIGRATION

The basic IO changes of Solid State Disks (SSD) over customary rotational hard plates makes it an engaging method to manage join SSDs in layered limit systems for execution improvement. In any case, to organize SSD into multitiered limit system reasonably, motorized data development among SSD and HDD accept a fundamental part. In various genuine application circumstances like setting aside cash and economic situations, remaining task at hand and IO profile show fascinating characteristics and moreover bear the restriction of outstanding task at hand due date. Well ordered directions to totally release the vitality of data migration while guaranteeing the development due date is essential to boosting the execution of SSD enabled multi-layered limit system. To totally misuse the upsides of SSDs in a multi-layered limit system with SSDs filling in as the speediest dimension, it is fundamental to recognize the right subset of data that ought to be determined to this dimension given the confined furthest reaches of SSD level in light of amazing cost per gigabyte. Specifically, we have to lift general system execution by setting fundamental, IOPS (input/yield exercises each second) genuine and latency sensitive data on the snappy SSD level through two-way automated data migration among SSDs and HDDs. By working with a combination of huge business class amassing applications, we watch that various square dimension IO remaining tasks at hand demonstrate certain time-subordinate ordinariness to the extent get to precedents and temperature of degrees (hot or cold). For example, in keeping cash applications, IO outstanding tasks at hand for record access and credit check are conventionally heavier in the midst of explicit significant lots of multi day. Regardless, such precedents may change from day-time to night time, from ordinarily, from weekdays to finishes of the week or from working days to open events. Subsequently, square dimension IO profiling is the underlying advance for structure a motorized data migration system. The accompanying colossal test is to devise techniques[15].

In this work, we proposed a motorized look forward data development plan, called LAM, which intends to adaptively move data between different dimensions to keep pace with the IO outstanding task at hand assortments, to enhance the upsides of the speedy yet breaking point confined SSD level, and to improve the general structure execution to the extent response time and resource use, while obliging the impact of LAM on existing IO remaining burdens. Even more emphatically, in perspective on outstanding task at hand assortments and temperature of square dimension IO get to (e.g., hot or frosty degrees) learned through IO profiling, we envision moves in issue regions of square dimension degrees and proactively move those data degrees whose temperature is depended upon to climb in the accompanying remaining burden into the snappy SSD level in the midst of a look ahead period. A key test in the LAM setup is to understand and trade off various parts that effect the perfect look ahead development window[15].

3. LITERATURE SURVEY

[1] Issa Khalil, Cloud preparing organizations are winding up progressively standard. In any case, the high centralization of data and organizations on the fogs make them charming concentrations for various security attacks, including DoS, data burglary, and insurance strikes. In addition, cloud providers may disregard to comply with advantage level understanding similar to execution, openness, and security guarantees. Thusly, it is of important essentialness to have secure and viable instruments that enable customers to direct copy and move their data beginning with one provider then onto the following. In this paper, we explore the top tier between cloud movement methodology and recognize the potential security threats in the degree of Hadoop Distributed File System HDFS. We propose a between cloud data movement part that offers better security guarantees and snappier response time for moving significant scale data records in cloud database organization systems. The execution of the proposed methodology is endorsed by evaluating its impact on response time and throughput, and standing out the execution from that of various frameworks in the composition. The results exhibit that our methodology basically upgrades the execution of HDFS and outmaneuvers its accomplices.

[2] Ibrahim Ejdayid A. Mansour, Cloud providers offer their IaaS organizations in light of virtualization to enable multi-inhabitant and isolated conditions for cloud customers. At the present time, each provider has its

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

very own prohibitive virtual machine (VM) executive, called the hypervisor. This has realized tight coupling of VMs to their major gear blocking live development of VMs to different providers. Different customer driven approachs have been proposed from both academic network and industry to understand this issue. Regardless, these procedures persevere through confinements to the extent execution (migration personal time), versatility (decoupling VMs from fundamental gear) and security (secure live development). This paper proposes LivCloud to thrashing such obstructions. An open-source cloud orchestrator, a made transport show, overlay sort out and verified migration channel are essential pieces of LivCloud to achieve convincing live cloud development. Plus, a fundamental evaluation of LAN live migration in settled virtualization condition and between different hypervisors has been considered to exhibit the development influence on mastermind throughput, compose latency and CPU use. The appraisal has demonstrated the necessity for headway inside the LAN condition.

[3] Qingni Shen, with the improvement of disseminated registering, cloud security issues have starting late grabbed balance in the investigation arranges. Yet an extraordinary piece of the undertakings are based on verifying the errand system and virtual machine, or verifying data storing inside a cloud structure, this paper takes an elective perspective to cloud security—the security of data migration between different fogs. To begin with, we depict a couple of risks when we are doing data development. Second, we propose a security segment to deal with the security issues on data development beginning with one cloud then onto the following. Third, we diagram a model to give the instrument a short execution in perspective on HDFS (Hadoop Distributed File System) and we complete a movement of tests to survey our model. Here, the responses for verifying data development between fogs on a very basic level incorporate into SSL exchange, migration ticket diagram and square encryption in appropriated report structure and bundle parallel preparing.

[4] Sameera Dhuria, Distributed computing is another enlisting model in the domain of Information Technology that passes on advantages as utility over the Internet. It has a couple of central focuses when diverged from ordinary enlisting models like on-demand benefits, preparation, flexibility, diminished information development overhead for the end-customer, progressively unmistakable versatility, diminished expense, etc. The focal points and whole deal focal points of this new advancement move relationship to move their present applications to the cloud. In spite of the way that migrating to cloud gives various preferences, there are different challenges and security issues related to cloud, that square the system of its appointment by the affiliations. The present paper intends to analyze the genuine challenges related to development to Cloud Computing.

4. RESEARCH GAP

Cloud platform offers a plethora of services, concepts and applications such as storage, processing power, virtualization, connectivity and sharing. It allows users to have access to applications delivered as a service from the internet as well as the hardware and system software in the data centers that provide such services. No doubt, with so many benefits and plus points, cloud is here to stay and to grow even further in the coming time but as it happens with every good thing, there are issues with cloud too. The user's privacy and ensuring secure data migration of their most valuable data is one of the major challenges among the list of challenges being posed by the cloud platforms. Then, other issues like data integrity, data location and relocation, data availability and the issues related to storage, backup and recovery are also there which are no less than the major issue cited above.
A robust mechanism is required to migrate the data on the cloud based on stenographic approach to that messages can be sent to the cloud by hiding them in the images for the purpose of security.

Proposed Methodoloy

The proposed methodology works in the four phases in which are as follows:

4.1 Phase 1:

In the first phase client upload the data which is to be migrated to the cloud. An encryption is performed using arithmetic encryption algorithm to encrypt the data which is to be sent on the cloud. The encryption for the data is performed to provide the extra security layer for the client for data migration.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

4.2 Phase 2:
In the second phase function of steganography is performed to hide the encryption data to the cloud. A Enhanced 2-LSB Approach is used to hide the text data into the image which is then finally migrate to the cloud. After performing this step a stegno image is generated by the system in which data is hidden. This stegno image is then migrated to the cloud for storage.

4.3 Phase 3:
In this phase data is accessed from the cloud for the user for its personal use. In this phase stegno image can be downloaded from the cloud from which data is to be extracted using Inverse Enhanced 2-LSB approach. This data is in the encrypted form which is then sent to the next phase for decryption.

4.4 Phase 4
In this final phase data which is extracted from the stegno image is finally decrypted using inverse arithmetic coding to obtain the original message. The extracted message is then shown to the user.

The overall working of the proposed system can be described in the following steps:
STEP1: Client or Sender choose a CSP, subscribes to a plan offered by it and creates his account on their website.
STEP2: Client selects data to be uploaded on the CSP's website.
STEP3: The CSP server performs a three step process before finally uploading the data on its servers:
a. It performs data encryption, i.e. it converts the original data files of clients into a secret coded format using a strict encryption algorithm.
b. Now, this coded data is put behind a stego object and a stego image is created which hides the existence of anything sensitive travelling on the network. This double layered protected client's data now gets uploaded on CSP servers.
STEP 4: When client is required to use/access the data, the reverse process is performed. Firstly, the stego object is removed from the stego image and the data comes in the encrypted form.
STEP5 : Client use his credentials provided by the CSP to decrypt the data.
STEP6: Data is downloaded to the client.

The Proposed research use an improved steganography approach to hide the messages into image files which is Adaptive 2-LSB Method for color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks for the images to be stored on cloud. Images as well as text messages can be hide within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. It would be highly immune to any environmental disturbances like noise due to hybrid filtering.

5. RESULTS AND DISCUSSIONS

We have conducted several experiments to examine the effectiveness of proposed algorithm. We `choose the cover image of buildings, people and vehicles and hide various text in them. All the images are of different sizes and taken from real world data. Proposed system is tested on more than 50 images with different text data for data hiding. System is giving 94% accurate results.

The following table shows the statistics of the proposed system:

Table 3: Shows the statistics of the proposed system

Parameter	Value
Total Images Tested	50
Text Messages	50
System Accuracy	97%

PSNR(Peak Signal to Noise Ratio) of the obtained stego-image can be computed by

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

PSNR worst =20 × log10(255/MSE) dB (3.1)

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2.$$

The results are then compared with various steganography methods as shown in the following table. In current work more pixel values is change because the simple LSBre placement depends upon size of image. Comparative study of previous method and Adaptive LSB substitution method is shown below:

Table 4: Performance of Existing and Proposed system

Input Image	Existing	Proposed System
PSNR	38.98	49.32
Accuracy	88.62	96.02

comparison of the proposed system with the existing system is on the basis of PSNR values is shown as below :

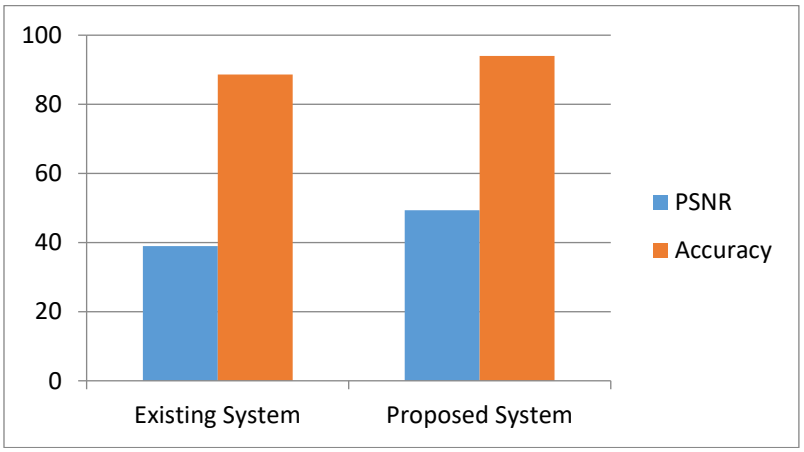

Figure 1.1: Show the accuracy and PSNR between existing and proposed system

6. CONCLUSION

In the proposed work, we proposed a novel approach to migrate data on cloud servers through the combined use of cryptography and steganography. In cryptography process, we make use of very robust approach which is Adaptive 2-Least Bit Significant (2-LSB) Technique to hide the text data into an image which is to be migrated to the cloud server. We hide the encrypted form of input data to provide more security. We use arithmetic coding technique to encrypt the input data which is to be hidden in the image. Proposed system works in four phases in which overall

working of the system is done. Performance of the proposed system is tested on the basis of two parameters which is PSNR and overall accuracy. Performance of the proposed system is compared with the performance of the existing on the same input data set and it is concluded that the results of the proposed system are better than that of existing system.

7. FUTURE SCOPE

In future performance of the proposed system can also be improved by providing the hybrid encryption algorithm which may be the combination of more than two encryption algorithms. Performance of the proposed system can also be monitored in future on the basis of cloud migration time as well as encryption time.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

REFERENCES

[1] Issa Khalil, Ismail Hababeh, Abdallah Khreishah, "Secure Inter Cloud Data Migration", International Conference on Information and Communication Systems(ICICS), 2016
[2] Ibrahim Ejdayid A. Mansour, Kendra Cooper, Hamid Bouchachia, "Effective Live Cloud Migration", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud.
[3] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "Sec DM: Securing Data Migration Between Cloud Storage Systems",2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.
[4] Sameera Dhuria, Anu Gupta, R. K. Singla, "Migrating Applications to the Cloud: Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 6, June 2015.
[5] Virendra Singh Kushwah, Aradhana Saxena," A Security approach for Data Migration in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.
[6] Wei Hao, I-Ling Yen and Bhavani Thuraisingham, "Dynamic Service and Data Migration in the Clouds", 2009 33rd Annual IEEE International Computer Software and Applications Conference.
[7] Rashmi Rao, Pawan Prakash, "Improving security for data migration in cloud computing using randomized encryption technique", July 2015 IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-8727Volume 11, Issue 6.
[8] Rajeshri Vaidya, and Prof. Sumedh Pundkar ,"Large Data migration within Cloud Environments using Compression and Encryption Technique", International Journal of Innovative and Emerging Research in Engineering, Volume 2, Issue 2, July 2015.
[9] Mohammad Manzurul Islam, Sarwar Morshed and Parijat Goswami," Cloud Computing: A Survey on its limitations and Potential Solutions", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013.
[10] Chetan M Bulla, Satish S Bhojannavar and Vishal M Danawade, "Cloud Computing: Research Activities and Challenges", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 5, September – October 2013.
[11] Nirav Shah, Sandip Chauhan" Survey Paper on Security Issues While Data Migration in Cloud Computing", July 2014 IJIRT | Volume 1 Issue 7 | ISSN: 2349-6002.
[12] Punit K Mendapara, Sandip S Chauhan," Survey Paper on Secure Live Data Migration in Cloud Computing by maintaining Integrity and Confidentiality", December 2015 | IJIRT | Volume 2 Issue 7 | ISSN: 2349-6002.
[13] Virendra Singh Kushwah, Aradhana Saxena,"A Security approach for Data Migration in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.
[14] Zohreh Sanaei, Abdullah Gani,"Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014.
[15] J. Priya Shanthi, Parsi Kalpana," Migration of Existing Applications to Cloud and Among Clouds", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
[16] Y. Ghebghoub, S. Oukid, and O. Boussaid," A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.
[17] Vijay.G.R , Dr. A. Rama Mohan Reddy, "Security Issue Analysis in Cloud Computing Environment", International Journal of Engineering Research and Applications (IJERA), 2016 ISSN: 2248-9622.
[18] Sh. Ajoudanian and M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing", IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, June 2012.
[19] Kangchan Lee," Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications, Vol. 6, No. 4, October, 2012.
[20] Vahid Ashktorab, Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2016

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.