World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(11): 297-301
www.wwjmrd.com
*International Journal*
*Peer Reviewed Journal*
*Refereed Journal*
*Indexed Journal*
*UGC Approved Journal*
*Impact Factor MJIF: 4.25*
e-ISSN: 2454-6615

**Gurdeep Singh**
UCCA, Guru Kashi University,
Talwandi Sabo, India

**VijayLaxmi**
UCCA, Guru Kashi University,
Talwandi Sabo, India

**Correspondence**:
**Gurdeep Singh**
UCCA, Guru Kashi University,
Talwandi Sabo, India

# Data Migration Using Steganography and Cryptography in Public Cloud

**Gurdeep Singh, Vijay Laxmi**

## 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 is not clear how and when cloud computing should be used. 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.

## Introduction

Cloud computing usually refers to a utility-based provisioning of computational resources over the Internet. Widely used analogies to explain cloud computing are electricity and water supply systems. Like the Cloud, they provide centralized resources that are accessible for everyone. Also, in the Cloud you only pay for what you have used. And finally, it is usually consumed by those who have difficulties to produce necessary resources by themselves or just do not want 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.

## Major Challenges in Cloud Computing

### Security and privacy

Security and privacy are the most discussed issues of cloud computing. Even though security is improved through data centralization and security-oriented components, there is still a concern regarding sensitive information stored in the Cloud. Since users do not fully control their data, they have to trust cloud providers in securing it. Also, the risk of a data leakage on the way to the Cloud brings new challenges regarding secure transportation. VPN or encrypted data tunnelling between the local machine and a cloud environment are possible solutions. Private cloud installations were partly motivated by security and privacy concerns.

### Availability

Another cloud adoption issue is availability. Even though cloud providers offer a high level of availability through SLAs, outages do occur in cloud platforms. There are two types of outages: a permanent and a temporary outage. The first one means that the cloud provider goes out of business. A temporary outage means service unavailability during a relatively short period of time like several hours. The biggest cloud providers have experienced several serious outages for the past several years. There are some precautions that cloud consumes can take to mitigate the risk. For example, they can use the Cloud for non-critical systems, keep on premise backups, and set up a service level agreement. In general, large cloud providers are usually more reliable than small ones.

**Performance**

There are also some performance implications when adopting cloud computing. Virtualization and resource sharing lead to performance unpredictability, especially for I/O resources. Cloud platforms should guarantee a fair resource distribution across the applications running on the same machine. Unlike on premise systems that can keep their code and data in the same runtime environment, cloud components communicate via the network. Since users cannot control the exact deployment location, application components are usually spread across many servers. This results in higher latencies and bandwidth limitations. Performance can become a serious problem, especially when the number of requests and the amount of data increase. Cloud platforms often provide special caching mechanisms and CDN services that can partly compensate these issues.

**Compliance requirements**

Many enterprises, especially in the US, are regulated by government policies regarding data security and disclosure, like Sarbanes-Oxley Act for corporate accounting data and Health Insurance Portability and Accountability Act (HIPPA) for people’s healthcare insurance data. Most of these rules do not consider cloud services, so it is unclear whether or not cloud computing services violate the regulations. Such issues are not analyzed in our report. However, it should be taken into account when adopting the Cloud.

**Literature Survey**

1. Issa Khalil, Cloud computing services are becoming more and more popular. However, the high concentration of data and services on the clouds make them attractive targets for various security attacks, including DoS, data theft, and privacy attacks. Additionally, cloud providers may fail to comply with service level agreement in terms of performance, availability, and security guarantees. Therefore, it is of paramount importance to have secure and efficient mechanisms that enable users to transparently copy and move their data from one provider to another. In this paper, we explore the state-of-the-art inter-cloud migration techniques and identify the potential security threats in the scope of Hadoop Distributed File System HDFS. We propose an inter-cloud data migration mechanism that offers better security guarantee sand faster response time for migrating large scale data files in cloud database management systems. The performance of the proposed approach is validated by measuring its impact on response time and throughput, and comparing the performance to that of other techniques in the literature. The results show that our approach significantly improves the performance of HDFS and outperforms its counterparts.
2. Ibrahim Ejdayid A. Mansour, Cloud providers offer their IaaS services based on virtualization to enable multi-tenant and isolated environments for cloud users. Currently, each provider has its own proprietary virtual machine (VM) manager, called the hypervisor. This has resulted in tight coupling of VMs to their underlying hardware hindering live migration of VMs to different providers. A number of user-centric approaches have been proposed from both academia and industry to solve this issue. However, these approaches suffer limitations in terms of performance (migration downtime), flexibility (decoupling VMs from underlying hardware) and security (secure live migration). This paper proposes Liv Cloud to overcome such limitations. An open-source cloud orchestrator, a developed transport protocol, overlay network and secured migration channel are crucial parts of Liv Cloud to achieve effective live cloud migration. Moreover, an initial evaluation of LAN live migration in nested virtualization environment and between different hypervisors has been considered to show the migration impact on network throughput, network latency and CPU utilization. The evaluation has demonstrated the need for optimization within the LAN environment.
3. Qingni Shen, with the development of cloud computing, cloud security issues have recently gained traction in the research community. Although much of the efforts are focused on securing the operation system and virtual machine, or securing data storage inside a cloud system, this paper takes an alternative perspective to cloud security—the security of data migration between different clouds. First, we describe some threats when we are doing data migration. Second, we propose a security mechanism to deal with the security issues on data migration from one cloud to another. Third, we design a prototype to give the mechanism a brief implementation based on HDFS (Hadoop Distributed File System) and we do a series of tests to evaluate our prototype. Here, the

solutions to securing data migration between clouds mainly involve in SSL negotiation, migration ticket design and block encryption in distributed file system and cluster parallel computing.

4. Sameera Dhuria, Cloud Computing is a new computing model in the world of Information Technology that delivers services as utility over the Internet. It has several advantages as compared to traditional computing models like on-demand services, agility, scalability, reduced information technology overhead for the end-user, greater flexibility, reduced cost etc. The advantages and long term benefits of this new technology motivate organizations to migrate their existing applications to the cloud. Though migrating to cloud provides many benefits, there are a number of challenges and security issues related to cloud, that hinder the process of its adoption by the organizations. The present paper aims to discuss the major challenges related to migration to Cloud Computing.

## Proposed Methodology

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

**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.

**Phase 2:**

In the second phase function of steganography is performed to hide the encryption data to the cloud. An Enhanced 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.

**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 LSB approach. This data is in the encrypted form which is then sent to the next phase for decryption.

**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:

**STEP 1**: Client or Sender choose a CSP, subscribes to a plan offered by it and creates his account on their website.

**STEP 2:** Client selects data to be uploaded on the CSP's website.

**STEP 3:** 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 thenetwork. 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 stage object is removed from the stego image and the data comes in the encrypted form.

**STEP 5:** Client use his credentials provided by the CSP to decrypt the data.

**STEP 6:** Data is downloaded to the client.

The Proposed research use an improved steganography approach to hide the messages into image files which is Adaptive 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.

## Results and Discussion

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:

| Parameter | Value |
|---|---|
| Total Images Tested | 50 |
| Text Messages | 50 |
| System Accuracy | 94% |

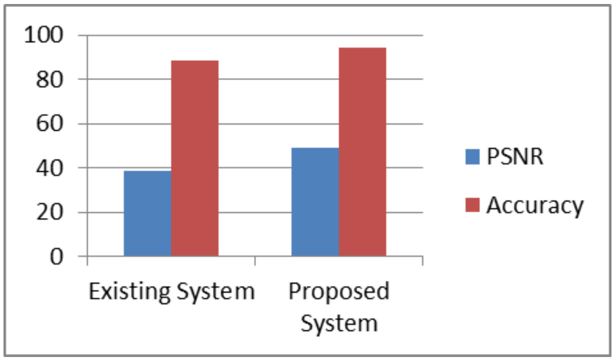
PSNR (Peak Signal to Noise Ratio) of the obtained stego-image can be computed by

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

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 LSB replacement depends upon size of image. Comparative study of previous method and Adaptive LSB substitution method is shown below:

| Input Image | Existing | Proposed System |
|---|---|---|
| PSNR | 38.98 | 49.32 |
| Accuracy | 88.62 | 94.02 |

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



## Conclusion and Future Scope

### 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 Least Bit Significant (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.

### 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.

### References

1. IssaKhalil,IsmailHababeh,AbdallahKhreishah,"Secure Inter Cloud Data Migration" ,International Conference on Information and Communication Systems(ICICS), 2016
2. Ibrahim EjdayidA.Mansour,Kendra Cooper, Hamid Bouchachia,"Effective Live Cloud Migration", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud.
3. QingniShen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM: 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, AradhanaSaxena,"A Security approach for Data Migration in Cloud Computing",International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.
6. Sultan Ullah,ZhengXuefeng, "Cloud Computing Research Challenges", 2013
7. Prashant Pant, SanjeevThakur,"Data Migration Across The Clouds", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-3, Issue-2, May 2013
8. Wei Hao, I-Ling Yen and BhavaniThuraisingham,"Dynamic Service and Data Migration in the Clouds", 2009 33rd Annual IEEE International Computer Software and Applications Conference
9. RashmiRao, PawanPrakash, "Improving security for data migration in cloud computing using randomized encryption technique", IOSR Journal

of Computer Engineering (IOSR-JCE), ISSN: 2278-8727Volume 11, Issue 6

10. 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, 2015
11. 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
12. 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
13. Nirav Shah, Sandip Chauhan,"Survey Paper on Security Issues While Data Migration in Cloud Computing", 2014 IJIRT | Volume 1 Issue 7 | ISSN: 2349-6002
14. 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
15. Virendra Singh Kushwah, AradhanaSaxena,"A Security approach for Data Migration in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013
16. Zohreh Sanaei, Abdullah Gani,"Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014
17. 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
18. 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.
19. Ashima Narang, Dr. Vijay LAXMI “Comparison of a New Approach of Balancing the Load Environment with the Existing Techniques” published in the INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, IN THE October, 2014