IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA MIGRATION FROM PRIVATE CLOUD TO PUBLIC CLOUD USING ENCRYPTION AND STEGNOGRAPHY TECHNIQUE

Harjot Kaur*[1] & Prof. Dinesh Kumar[2]
*[1]M.Tech (CSE), Giani Zail Singh Campus College of Engg & Technology Bathinda
[2]Assistant Professor, Giani Zail Singh Campus College of Engg & Technology Bathinda

DOI: 10.5281/zenodo.1165928

ABSTRACT

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. Proposed system is used to migrate the data from private cloud to public cloud using encryption and stegnography technique.

Keywords: *Cloud Computing, Stenography, Cloud Security, Encryption, Data Migration*.

I. 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.

The definitions proposed in the cloud computing community are often focused on different perspectives and do not have common baselines. Analyzing existing sources in order to identify common characteristics, Vaquero et al [7] observed no clear and complete definition in the literature. Nevertheless, the authors proposed three features that most closely describe cloud computing: scalability, pay-as-you-go utility model, and virtualization – and gave the following definition:

"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be activelly reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs."

II. CLASSIFICATIONS OF THE CLOUD

There are two widely used cloud computing classifications. The first one describes four cloud types depending on the deployment location:

1.2.1 Public clouds. Public or external clouds are traditional clouds where resources are dynamically provisioned via the Internet by the off-site third-party providers. These resources are publically available to everyone. Cloud consumers are charged depending on the quantity used. Examples are Microsoft Azure, Google App Engine, and Amazon Web Services.

1.2.2 Private clouds. Private clouds usually refer to the emulation of a cloud computing environment on private infrastructure. Since users still have to buy hardware and operating equipment, private clouds are often criticized. Many companies try this type of cloud to verify their software locally before deploying it to public cloud.

1.2.3. Community clouds. Community clouds means a cloud environment established across several organizations. Such clouds can be managed by the organizations or third-parties and installed either on- or off-premise.

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.

III. DATA MIGRATION

The substantial IO improvements of Solid State Disks (SSD) through the conventional rotational hard disks makes it an attractive approach to integrate SSDs in tiered storage systems for performance enhancement. However, to integrate SSD into multi layred storage system effectively, automated data migration between SSD and HDD plays a critical role. In many real world application scenarios like banking and supermarket environments, workload and IO profile present interesting characteristics and also bear the constraint of workload deadline. How to fully release the power of data migration while guaranteeing the migration deadline is critical to maximizing the performance of SSD enabled multi-tiered storage system. In order to fully capitalize on the benefits of SSDs in a multi-tiered storage system with SSDs working as the fastest tier, it is important to identify the right subset of data that needs to be placed on this tier given the limited capacity of SSD tier due to high cost per gigabyte. Specifically, we want to maximize overall system performance by placing critical, IOPS (input/output operations per second) intensive and latency-sensitive data on the fast SSD tier through two-way automated data migration between SSDs and HDDs. By working with a variety of enterprise class storage applications, we observe that many block-level IO workloads exhibit certain time-dependent regularity in terms of access patterns and temperature of extents (hot or cold). For example, in banking applications, IO workloads for account access and credit verification are typically heavier during certain hours of a day. However, such patterns may change from day-time to night-time, from day to day, from weekdays to weekends or from working days to public holidays. Thus, block-level IO profiling is the first step for building an automated data migration system. The next big challenge is to devise strategies

In this work, we proposed an automated look ahead data migration scheme, called LAM, which aims to adaptively migrate data between different tiers to keep pace with the IO workload variations, to maximize the benefits of the fast but capacity-limited SSD tier, and to optimize the overall system performance in terms of response time and resource utilization, while limiting the impact of LAM on existing IO workloads. More concretely, based on workload variations and temperature of block level IO access (e.g., hot or cold extents) learned through IO profiling, we predict shifts in hot-spots of block-level extents and proactively migrate those data extents whose temperature is expected to rise in the next workload into the fast SSD tier during a look ahead period. A key challenge in the LAM design is to understand and trade off multiple factors that influence the optimal look ahead migration window.

The main contributions of this work are two lap. First, we propose the need and the impact of automated deadline aware data migration through observation and analysis of IO workload scenarios from real world storage system practice. By introducing basic data migration model in an SSD authorised multi-tiered storage system, we study the characteristics and impacts of several factors, including IO pro- files, IO block level bandwidth, and the capacity of SSD tier, on improving overall performance of the tiered storage systems. Second, we present a look ahead migration framework as an effective solution for performing deadline aware, automated data migration, by carefully managing the performance impact of data migration on existing runtime application workloads and maximizing the gains of look ahead migration. A greedy algorithm is designed to illustrate the importance of determining a near optimal look ahead window length on the overall system performance and a number of important factors, such as block level IO bandwidth, the size of SSD tier, the workload characteristics, and IO profiles. Our experiments are conducted using both the IO trace collected from benchmarks on a commercial enterprise storage system and the simulation over the real trace. The experimental study demonstrates that the greedy algorithm based look ahead migration scheme not only enhances the overall storage system performance but also provides significantly better IO performance as compared to both basic data migration.

The efficiency of greedy algorithm based look ahead data migration is restricted by the incremental granularity and lacks flexibility. Thus an adaptive migration algorithm, which can pace with the changes of the environment of the system, is demanded. In this work, we proposed an adaptive deadline aware look ahead data migration scheme, called ADLAM, which adaptively decides the window length of look ahead based on the system parameters.

The main contributions of the data migration work are two fold. First we build a formal model to analyze the benefits of basic data migration across different phases on system response time improvements and integrate the benefits in each phase into the benefits across all the phases. Second, we present our data migration optimization process which evolves from learning phase reduction, to constant look ahead data migration and to adaptive look ahead data migration scheme. The system utility measure is proposed to compare the performance gains in each data migration model. We propose an adaptive look ahead migration approach, which works as an effective solution for performing deadline aware data migration by carefully trading off the performance gains achieved by look ahead migration on the next workload and the potential impacts on existing workloads. This approach centers around a formal model which computes the optimal look ahead length by considering a number of important factors, such as block level IO bandwidth, the size of SSD tier, the workload characteristics, and IO profiles. Our experiments confirm the effectiveness of the proposed adaptive data migration scheme by testing the IO traces collected from benchmark and commercial applications running on an enterprise multi-tiered storage server. The experiments show that ADLAM not only improves the overall storage performance, but also outperforms the basic data migration model and constant look ahead migration strategies significantly in terms of system response time improvements.

IV. 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 the paper, we show 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 guarantees and 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 owners offer their some 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 LivCloud to overcome such limitations. An open-source cloud orchestrator, a developed transport protocol, overlay network and secured migration channel are crucial parts of LivCloud 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.

[5] Virendra Singh Kushwah,Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. The acceptance of Cloud computing has been increasing for some time and the maturity of the market is steadily growing. Security is the question most consistently raised as consumers look to move their data and applications to the cloud. I explain the importance and motivation of security in the migration of legacy systems and I carry out an approach related to security in migration processes to cloud with the aim of finding the needs, concerns, requirements, aspects, opportunities and benefits of security in the migration process of legacy systems.

[6] S. Ullah ,In recent times cloud computing has appeared as a new model for hosting and conveying services over the Internet. This model is striking to business vendors as it eradicates the requirement for users to plan in advance, and it permits the organization to start from low level and then add more resources only if there is an increase in the service demand. Even though cloud computing presents greater opportunities not only to information technology industry, but every organization involved in utilizing the computing in one way or the other, it is still in infancy with many problems to be fixed. The paper discusses research challenges in cloud computing.

V. 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. A 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 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.

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

STEP 6: Data is downloaded to the client.

VI. RESULTS AND DISCUSSIONS

In the proposed work LSB arithmetic algorithm had been implemented using JAVA platform. 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%

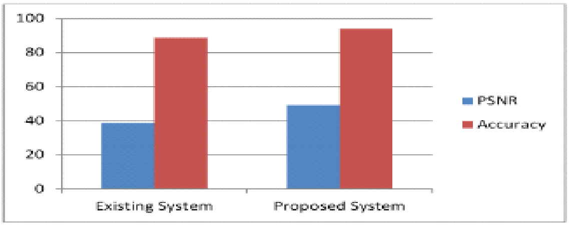
PSNR(Peak Signal to Noise Ratio) of the obtained stego-image can be computed by
PSNR worst =20 × log10 (255/MSE) dB (3.1)

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:

Table 4: Performance of Existing and Proposed system

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:



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.

VII. 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

VIII. REFERENCES

[1] 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.

[2] Qingni Shen, 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.

[3] Rabi Prasad Padhy, Manas Ranjan Patra,Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) ,Vol. 1, No. 2, December 2011.

[4] 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.

[5] Rajesh Piplode, Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.

[6] Kangchan Lee,"Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications, Vol. 6, No. 4, October, 2012.

[7] 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.

[8] Prashant Pant, Sanjeev Thakur,"Data Migration Across The Clouds", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[9] 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.

[10] 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.

[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] Sultan Ullah,Zheng Xuefeng, "Cloud Computing Research Challenges", Dec 2013.

[14] 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.

[15] Noor Ibrahim Hussein, Mervat Hashem,"Security Migration Requirements: From Legacy System to Cloud and from Cloud to Cloud", 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013).

[16] Monjur Ahmed and Mohammad Ashraf Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[17] Zohreh Sanaei, Abdullah Gani,"Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014.

[18] Osama Harfoushi, Bader Alfawwaz, Nazeeh A. Ghatasheh , "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review", Communications and Network, May 2014.

[19] 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.

[20] Neetu Kishore and Seema Sharma,"Secured Data Migration from Enterprise to Cloud Storage – Analytical Survey",BIJIT -BVICAM's International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM),May 2015 New Delhi (INDIA).

[21] Shyamli Dewan, Devendra Kumar, Sandeep Gonnade,"Secure Data Migration across Cloud System Using Third Party Auditor (TPA)", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June 2015

CITE AN ARTICLE

Kaur, H., & Kumar, D., Prof. (n.d.). DATA MIGRATION FROM PRIVATE CLOUD TO PUBLIC CLOUD USING ENCRYPTION AND STEGNOGRAPHY TECHNIQUE. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(2), 220-226.