IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

An Effective approach of Data Migration from Private to Public cloud using E-LSB with Improvisation Technique

Pallavi[1*], Dinesh Kumar[2]

[1,2]Department of Computer Science, GZSCET, Bathinda, India

Corresponding Author: thakral.pallavi@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i6.10121015 | Available online at: www.ijcseonline.org

Accepted: 10/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Cloud computing has recently became a most important and mainly discussed topic in the Technological industry. Almost all organizations use the Cloud, because it provides an easy and cost efficient way of using applications,which provides scalability for various systems. Still, it is not clear upto now how and when cloud computing should be used and where actually to be implemented. Existing applications are often written in such a way that it actually does not really fit a cloud environment well. Also, certain quality attributes like performance, security or portability integrity scalability network issues can be affected. Much more studies are actually needed on how existing systems should be used into the Cloud so that it can be transferred and it is checked what are the consequences of the migration. So in the proposed system we have developed an approach for enhancing the security of the data while migrating data on the cloud environment with the help of Cryptography and Stegnographic approach. In this mechanism, data is first entered or uploaded into the system and migrated on cloud.

***Keywords*—** cloud computing, public cloud platform, migration.

I. INTRODUCTION

Cloud is a type of Internet related computing service that provides shared processing resources and data to systems and other devices on request [1]. It is a model that enables on-demand access to various resources computer networks, servers, storage, applications and services, which can be quickly provided with minimum management effort [2][3]. Fundamentally, Cloud computing enables the users and enterprises with different capabilities to store and process their data in one or two privately owned cloud, or on a third-party server to enable data access in an easy manner and reliable way. Data centers which are located far from the user scope from across an area to all across the world [4]. This type of computing relies on sharing of resources to attain flexibility and economy of scale, like the power grid over an electricity network.

Experts claim that cloud enables enterprises to avoid infrastructure costs such as sales and purchasing servers, storage space etc. Similarly, it enables many organizations and firms to concentrate mainly on their core businesses instead of spending their time and money on computer infrastructure. Promoters also claim that cloud computing allows enterprises to get their applications running, with high efficiency and less maintenance, less cost and enables information technology (IT) teams to quickly adjust their data and resources to meet unpredictable changing demands.

Cloud providers typically use a "pay as you Use" model. This will lead to unexpectedly more charges if administrators do not adapt to the cloud pricing model.

A. Characteristics of Cloud

Using cloud storage has more benefits than traditional one. A firm can save money, time and data with cloud computing. The cloud has some of the unique properties such as it reduces infrastructure costs, set up cost, increases capacity and scalability, easily refresh aging infrastructure, supports new business opportunities, helps in business continuity
Business for enterprises may be elaborated and enhanced, as cloud computing may speed up and accelerate users' flexibility by providing re-provisioning, adding, or expanding technological infrastructure and resources.

Reductions in expenses are maintained by cloud service providers. A public-cloud delivery model converts primary rates and expenditures (e.g., buying servers) to operational costs. This supposedly reduces barriers such as third party to enter and increase cost and and need not be purchased for one-time or infrequent computing tasks and operations. As well, less IT skills are required for implementation of projects that use cloud computing.

Device and location independence helps users in accessing systems using any web application or a browser regardless of their location or what device they operate (e.g., PC, mobile

phone). As infrastructure is off-site (typically provided by a third-party) and easily accessed and can be retrieved via the Internet, users can connect to it from any location. Easy Maintenance can be done because of its remote accessibility. Productivity may be increased when multiple users can work on the same data side by side , instead of waiting for it to be saved and emailed. Time can be saved as information does not need to be re-entered ,it can be directly matched if needed , nor do users need to install application software and it can be upgraded to their systems.

B. Cloud Data Migration

The method of transferring data or resources of different formats between various storage devices or computers is referred as data migration. To achieve an automated migration, it must be done programmatically and in appropriate pattern. Migration is termed as moving the data from source to destination. Migration requires the coordination of host computer for the relocation of the files from source to destination through relocation scheme. We had to set up a management and implementation or a backup, while still sticking to the essential performance parameters such as security, scalability and efficiency.

II. RELATED WORK

Mr. Shrikant D. Bhopale [1], Cloud computing is one of the emerging fields in the computer world these days. Cloud computing is attracting everyone with its benefits. Now companies are shifting their focus onto cloud computing. But to be a part of cloud computing environment and to take advantages of cloud computing, legacy applications need to be migrated to cloud. Cloud migration is the process of transitioning all or part of a company's data, applications and services from onsite computers behind the firewall to the cloud or moving them from one cloud environment to another. After migrating to the cloud, the information will be available on the internet so that more people can have access to it as needed.

N. Kishore[2], Everything in Cloud is an emerging concept, with work in multiple areas right from the Infrastructure, to middleware, to applications and to data security. Every domain has its own flavor of Cloud. Technologies and techniques for Cloud has come a long way and is still evolving. Organizations are fast recognizing the value of migrating to Cloud but the biggest concern is around data security. The migration of sensitive data to a public cloud domain has risks associated with data loss, information theft, confidentiality and other vulnerabilities. There are security measures deployed at multiple points but the question of secured end to end data transmission still remains unanswered. Objective is to understand the security parameters that can help build a framework for secured data transmission. With reference to many research papers and reviews, the analysis is to focus on the security of data in transit. Pragmatic observation is that the data at rest in the Enterprise and the Cloud have fairly good security measures, but the data in transit is vulnerable. There is a future scope to build a security framework for the transit data. This paper will highlight few of the security aspects of Cloud that have been developed and the gap around the security of data being migrated from Enterprise storage to Cloud Storage.

Rabi Prasad Padhy[3], Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

S. Dewan[4],Cloud Computing is evolving as future generation architecture for computing. Usually cloud computing is defined as a grouping of computing recourses accessible via internet services. Traditionally the client/user store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. The client/user has less control over the stored data on the cloud, since the data is stored anywhere across the globe. It is the responsibility of cloud service providers to protect the client/user data from unauthorized access & disclosure and be faithful for the development of cloud computing. A third party auditor (TPA) can be used to provide security services over the cloud and ensures client/user that his/her data is secure from unwanted and suspicious activity. The TPA would not store any kind of data at its end, and it is only confined to providing security service between cloud service

provider and the user. During migration of data from one cloud to other cloud, the application framework will provide data integrity verification by using hashing algorithm like SHA-1 and provide encryption/decryption using symmetric algorithm like AES.

III. METHODOLOGY

In this proposed system, data from private cloud is being migrated to the public cloud with the help of two level security. These two levels of security are given below:

A. Data Encryption

In our system we are using ASCII values of text data and a random key of 4 characters to encrypt the data for communication purpose. 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. It provides extra security while migrating the data.

B. Stegnography

In the second phase function of steganography is performed to hide the encrypted data to the cloud. An improved E-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. In this step, two LSB's are used to hide the data than to use 1 bit data hiding technique as being used in the existing systems. The major advantage of using 2 bits for data hiding technique is that the capacity to hide the data into an image increases as proposed system uses 2 bits to hide data instead of using single bit for hiding the data.

The proposed algorithm for hiding the encrypted text data into an image is as below:

Step 1: Input the text data to be migrate for cloud.
Step 2: Encrypt the input data using ASCII data encryption.
Step 3: Input the cover image in which the encrypted data is to be hide.
Step 4: Convert the encrypted text data into the binary equivalent data.
Step 5: Calculate the total number of pixels of the cover image.
Step 6: For every input pixel of the cover image, generate a random number and calculate the mod 3of that random number.
Step 7: if the result of the step 6 is 0 then Overlap the i^{th} text data bit with the LSB of Red color of the i^{th} bit of input image. And If result of step 6 is 1 then use green color instead of Red color and if the result of step 6 is 2 then use blue color instead of red color to hide the text data.
Step 7: Regenerate the image from these updated pixels values.
Step 8: Send Updated image containing data to the cloud.
Step 9: End.

IV. 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 96.02% accurate results. The result comparison of the proposed system with the existing system is given as below in the table.

Table 4: Performance of Existing and Proposed system

Input Image	Existing	Proposed System
PSNR	49.32	54.67
Accuracy	94	96.02

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

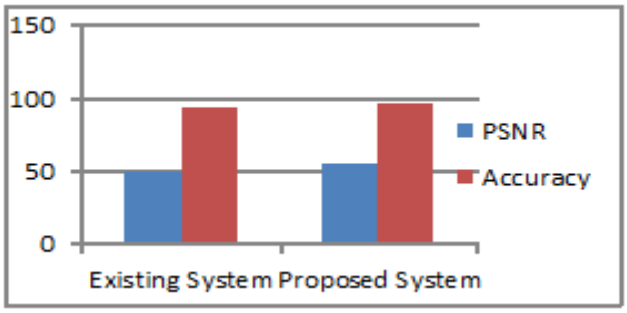

Fig. 1

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

The proposed system is developed to migrate the data from private cloud to public cloud along with two levels of security. In the first level, proposed system performs data encryption to the input text data using arithmetic encryption technique whereas in the second step proposed system performs the data hiding using two LSBs along with random number generation technique. This technique provide more security to the data as they are very hard to guess so the possibility of theft will be very less and by use of two bit LSBs the capacity to hide the data is also improved. The proposed system shows the accuracy of 96.02% which is the further improvement on the existing system.

B. Future Scope

In future, stegnogtyaphy technique to hide the data can be improved by hiding the encrypted data into edges only. Canny edge detection technique can be used to detect the edges and then data can be hidden in these pixels along with random number technique. Also data encryption algorithms can be

used to encrypt the text data that can also be improved to provide more security to the proposed system..

REFERENCES

[1] Mr. Shrikant D. Bhopale,"Cloud Migration Benefits and Its Challenges Issue", IOSR Journal of Computer Engineering (IOSR-JCE) ISSN : 2278-0661, ISBN : 2278-8727, PP : 40-45

[2] 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), New Delhi (INDIA)

[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] 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

[5] 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)

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

[7] 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

[8] 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

[9] Rashmi Rao, Pawan Prakash, "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

