International Journal of Engineering & Technology, 7 (2.8) (2018) 230-234

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper



Data migration in cloud computing using honey encryption

K.Ravindranadh[1], Mallarapu Sai Kiran[2], B Durga Sai Pavan Kumar[3], D Priyanka[4]

[1]Associate Professor, Deparment of CSE,Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502
[2,3,4]Student, Department of CSE,Koneru Lakshmaiah Education Foundation Vaddeswaram, Guntur, Andhra Pradesh,India-522502
**Corresponding author E-mail: [1]ravindra_ist@kluniversity.in*

Abstract

Cloud computing provides various kinds of services for storing data, load balancing between clouds and provides an infrastructure for developing applications and managing them. Due to various attractive services provided by various cloud service providers, users migrating their data from their storage system to cloud service provider. While migrating data to a cloud service provider there will be security and privacy protection concerns arises. By considering these concerns we are proposing a secure privacy protection migration using honey-encryption cryptographic algorithm for data which is outsourced data to cloud and we are using migration protocol while migrating data from existing server storage system to cloud server storage system which ensures data integrity and data confidentiality.

Keywords: *Cloud Computing, Data Migration, Honey Encryption, Data Confidentiality***.**

1. Introduction

With the enhancement in network technology and the vast requirement for computing resources, many industries have been initiated to outsource their data storage and computing needs, regarding to the ever cheaper hardware resources provided by cloud providers. The increasing requirement of outsourcing data and computing will require a migration of applications to the cloud, and migration of data to the cloud.
Cloud computing is a process of delivering computable resources over internet. Cloud computing provides various kinds of services such as Infrastructure as a service (Iaas), Software as a service (Saas), Platform as a service (Paas).
Infrastructure as a service (Iaas):- Iaas provides unlimited storage and network requirements without the needs of maintaining.
Software as a service (Saas):- Saas provides software applications running over the provider's infrastructure.
Platform as a service (Paas):- Paas provides a platform based environment for developing application with provider resources to users.
A cloud deployment model is classified into private cloud, public cloud, hybrid cloud, community cloud.
Private cloud: - It is a type of cloud which is exclusively used by single organization and it is maintained by organization or a trusted third party. This type of clouds will provides security as a major service due to its use by authorized people only.
Public cloud: - It is a type of cloud which is used by general people this type of cloud is a pay per used basis .in this cloud it provides vast no. of storage capacity but the main disadvantage is security concerns arises.
Hybrid cloud:- It is the combination of two or more clouds. this type of cloud provides scalability, data security due to combining both advantages of private and public or community cloud.
Community cloud:- It shares the cloud resources across several organizations to support specific community having common concerns .

2. Literature Survey

In [1] author proposed a technique of migrating data using randomized encryption technique for migrating data in encrypted format, but randomized encryption technique is not much will be suited from brute force attackers. In [2] author proposed a security approach of data migration based on prediction based encryption by picking an attribute in text and encrypting text with attribute selected but these encryption does not effectively handles the attacks on migrated or migrating encrypted data. In [3] author proposed a secure and reliable virtual machine migration in personal cloud in this paper author proposes secure migration of virtual machine from host. In [4] author proposed a technique secure instance migration it is based on introducing a new module in nova application programming interface which is secure instance . In[5] author proposes a framework for improving trust in migration to cloud this technique is mainly focuses on customer concerns and migrate according to it but if the customer wants to migrate entire data at a time this technique needs to be parallel done migration by considering customer concerns. In[6] author proposed a technique enabling dynamic and indirect mutual trust on storage systems this technique allows to outsource sensitive data to cloud service provider by ensuring that it allows only to authorized users though this technique is effective by allowing authorized users if some unauthorized user enters due to some

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

authorization hacked problem malicious user may steal the data and modify or read or copy the information.
In[7] author proposes a secure architecture for inter cloud vm migration by using local authentication server and shared key generation using elliptic curve for vm data transfer. In [8] author proposes technique to achieve security based on classifying data elements based on its value of usage and type of access control. Author proposes a technique of securely outsourcing data with verification in cloud storage by encrypting data blocks before uploading them to cloud by improved bcp encryption.
Author [9] proposes a novel cryptographic steganographic where we can encode data for migrating to cloud servers on a secure manner. Author [10] proposes a technique of migration this type of protocol ensures integrity problem by migrating data between storage systems but if data is sensitive integrity alone is not sufficient to ensure that data is confidential because even a passive attack is also looses confidentiality. Hence we are proposing a technique in which sensitive data is encrypted and outsourced to cloud storage system and if then user decided to migrate from existing cloud storage system to another cloud storage system we use migration protocol which is done by author[10].

3. Problem Statement

Cloud migration is the process of moving data from one cloud environment to another cloud environment (or) moving organization data from on premises database behind the firewall to cloud. Data migration in cloud is done due to various reasons such as cheaper cost for usage of cloud i.e pay per usage. Due to security (or) not having trust on cloud provider , suppose if the cloud provider is stopping services and user needs to transfer data to another cloud storage provider it requires data migration where security issues arises in migration.
Data migration in several aspects such as form direct cloud to cloud (or) downloading data from one cloud and upload to new cloud, but downloading and uploading requires a lot of work to be done by user, so direct migration form one cloud to another cloud is the best one for migrating purposes. As well as Outsourcing data from onsite server to cloud server also occurs some security concerns. In data migration there are several factors which can influence to improper migration and most influencing factor is security.
Data migration need to be securely transfer for maintaining confidentiality such that migration can strongly (or) effectively done even some active attacks are occurred . So data migration should be effectively done using some encryption techniques which can securely transfer the data with no data loss of control even when some severe active attacks are happened.

4. Existing System

According to author khalil [10] proposed work is about secure data migration among the clouds by considering parameter integrity which helps the user to ensure that data transfer is received same as sent data. This system consists of three main elements which is user, source cloud and destination cloud .user initiates migration process by logining to both cloud storage system accounts. user generates a random key and encrypt both cloud storage systems account password with it and send the encrypted password to both clouds. In this cloud storages is assumed as Hadoop distributed file system (hdfs) and data present in source hdfs is sent to target hdfs by encrypting block access tokens for authentication and transferring data present in data node with message digest for checking data integrity.

5. Proposed System

Our proposed work is intended to ensure that it satisfies authentication, data integrity, data confidentiality in cloud data migration. In this data migration there are some elements which are used for developing migration process they are source server, target cloud server, user admin name for storing admin files under his directory, upload the files, migrate the files. Our proposed work starts with selecting data migration should be done using honey encryption mode in source server where computation of encryption is done and after we have to create account name for user in source with admin name. Admin name indicates admin account where admin store his files.
After creating admin account ,we have to upload files into source server with some specified key at source server for encrypting data such that it cannot be seen by other user i.e it satisfies authentication for accessing the file, same key is used for authentication check for obtaining file access .After uploading the files to source server .Next step of our proposed work migration is to create an aws account for obtaining virtual cloud server to migrate from onsite server to virtual server.
After creation of aws account we have to create an ec2 instance for virtual cloud server then after we can obtain an public key and ip address for transmitting to cloud server and also we can create key pair for showing authentication to access the cloud server.

5.1 Migration process from onsite server to cloud server

1. Do the computation of honey encryption in onsite datacenter server and store the encrypted files data and database information of encrypted files such as key, admin name, date, file size in onsite datacenter server.
2. Create aws account for creating an ec2 instance for virtual server and obtain an ip address and key value pair for authentication to access virtual server.
3. Use winscp tool for migrating data from onsite datacenter to virtual server.
4. In winscp tool we use address of virtual server and key value pair for authentication of virtual server and after authentication we transfer the files from onsite server to cloud server.

Honey encryption is one of the cryptographic algorithm which is intended to create a plausible text for a encrypted text which creates a confusion to brute force attacker to find whether it is a correct text or wrong text.it will be helpful to user in some aspects i.e, if some of files are is some empty the brute force attacker may confuse whether there is a text or not there. Honey encryption is mainly used for restricting brute force attacks by creating a confusing that plausible text is correct or wrong.
This will be more effectively if user changes his encryption keys regularly so that the attacker will get into some confusion that decrypted text is valid or invalid. This type of encryption is used in source server such that the control of data relies in hands of authenticated users only such that data confidentiality is obtained.

6. Results and analysis

To simulate our proposed work we have used net beans 8.0.2 and mysql tools in source server for computation of encryption. In this proposed work, we have started with creating a database for uploads, logging records and content records for source server. We have used an AWS account for obtaining virtual server. And also we have used winscp for authentication and graphical user interface for migration between source servers to virtual cloud server. And our intended proposed work is also done with ssh client with cmd prompt for command line interface authentication and migration between source and cloud virtual server. We have shown the results for proposed system and also performance analysis of migration time from onsite to virtual cloud server.

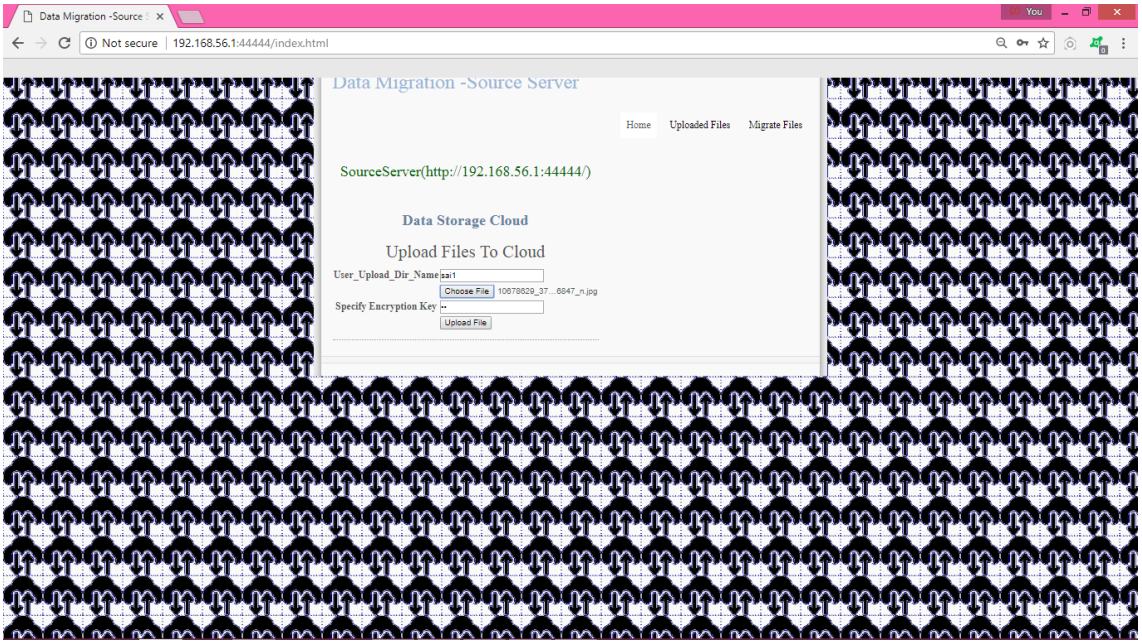


Fig.1: Uploading Data with honey encryption to onsite server

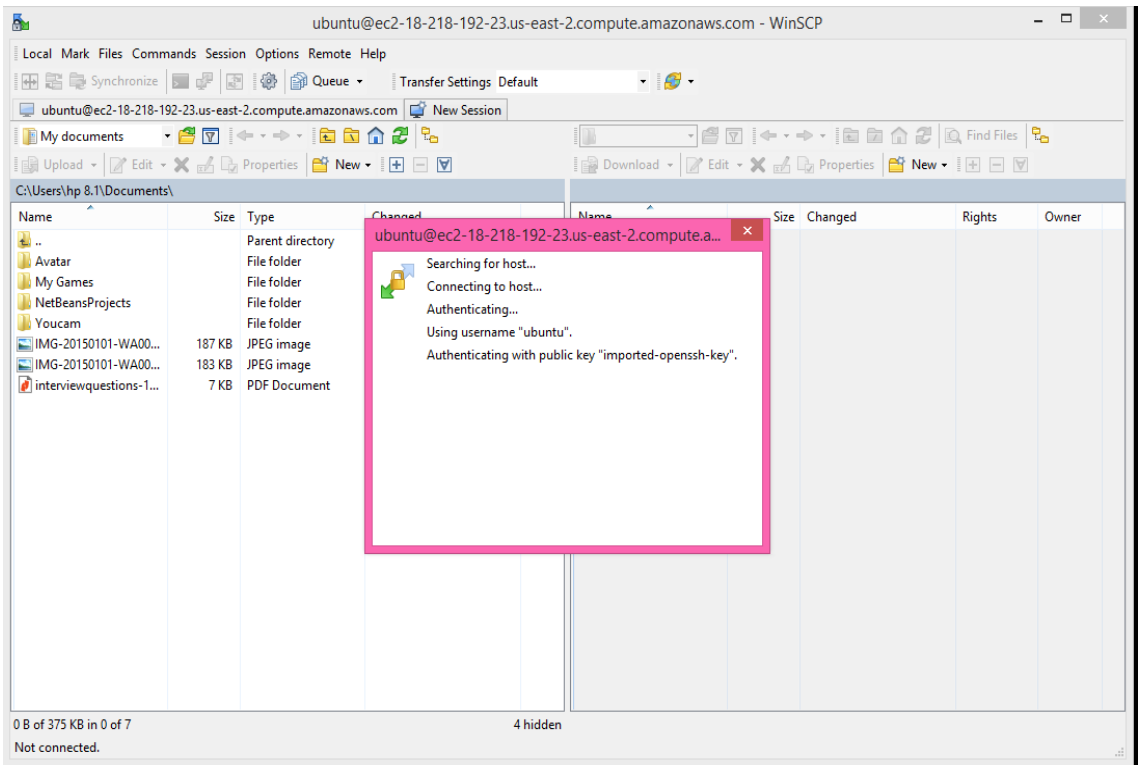


Fig.2: Authentication is established between onsite server and AWS server

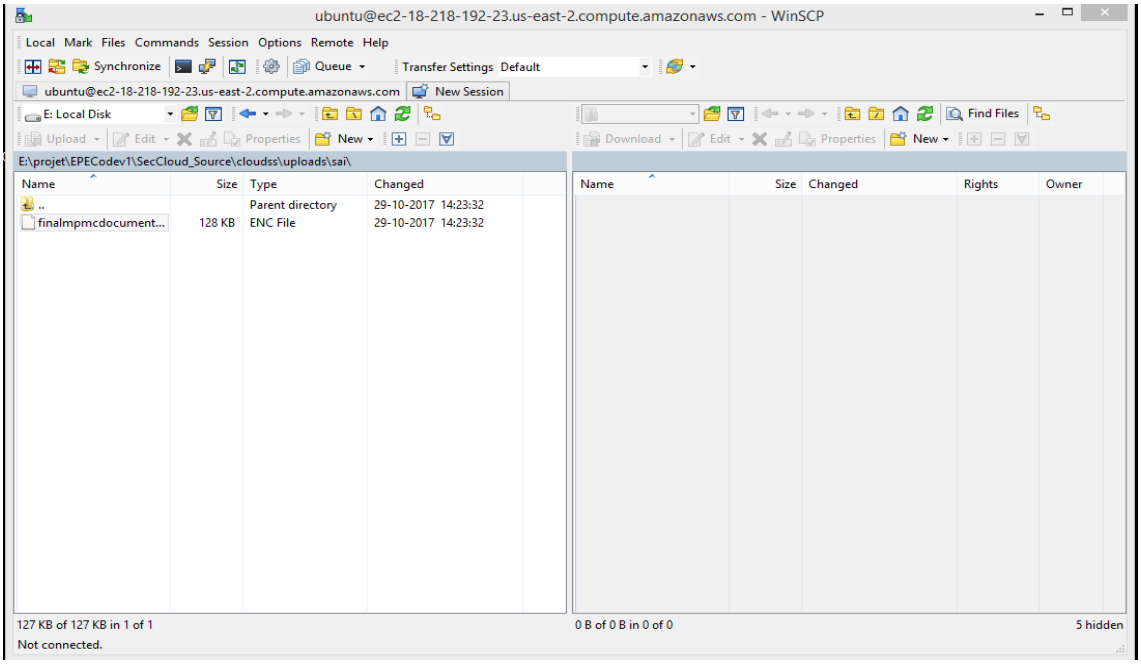


Fig.3: Migrating data from onsite server to Aws cloud server

6.1 Time analysis with respect to encryption algorithms

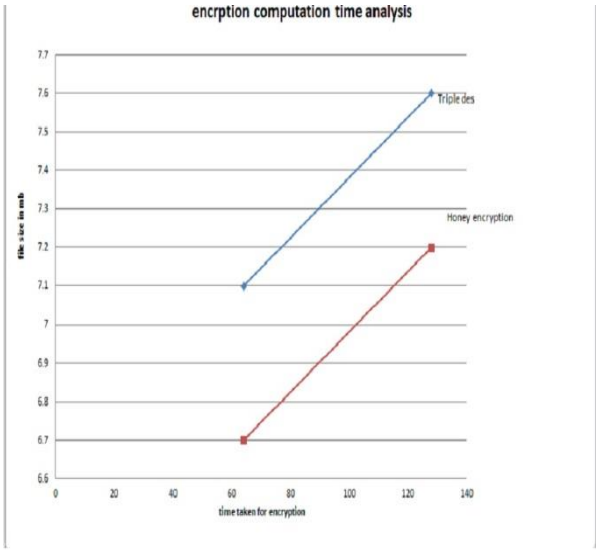


Fig.4: Comparison of time taken to encrypt between encryption algorithms for encrypting data.

7. Conclusions

Our proposed work is intended to secure privacy data during cloud data migration by ensuring authentication, data integrity, and data confidentiality. we have used honey encryption in our migration for securely transfer the data, this encryption mechanism is used mainly for restricting the brute force attacks by creating plausible text for unspecified key. In our migration concept we used same key at both source and target clouds it indicates authentication parameter is satisfied, we use some file size and we store content i.e message digest and migrate to required cloud for integrity parameter checking and logging records for integrity checking. We are using honey encryption for data confidentiality that is when some invalid key is specified we are generating some plausible text and for authenticated users with specified key only we are showing correct text. So in our proposed work we have achieved authentication, data integrity, data confidentiality during cloud data migration process.

References

[1] Rashmi rao," Improving security for data migration in cloud computing using randomized encryption technique", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), pp 39-42.

[2] 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 1 ISSN 2250-3153.

[3] Weiwang,Ya Zhang,Ben Lin."Secured and reliable VM migration in personal cloud", Computer Engineering and Technology (ICCET), 2010 2nd International Conference.

[4] Toqeer alisyed,Shahrulniza Musa,Abdur Rahman ."Towards secure instance migration in cloud", CloudComputing (ICCC), 2015 International Conference.

[5] Sara saadat,Hamid Reza Shahriari ,"Towards a process-oriented framework for improving trust and security in migration to cloud", Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference.

[6] Ayad barsowm,AAnwar Hasan ," Enabling dynamic data and indirect mutual trust for cloud computing storage systems", IEEE Transactions on Parallel andDistributed Systems (Volume: 24, Issue: 12, Dec. 2013).

[7] Tayyaba Zeb,Awais Shibli ,Muhammad Yousaf," A secure architecture for inter cloud vm migration ",10 International ICST conference SecureComm 2014, Part I, LNICST 152, pp. 24–35, 2015.

[8] Shaikh rizwana,M Sasi Kumar ." Data classification for achieving security in cloud computing", Procedia Computer Science Volume 45, 2015, Pages 493-498.

[9] Ankit Dhamija,Vijay Dhaka, " A novel cryptographic and steganographic approach for secure cloud data migration", Green Computing and Internet of Things (ICGCIoT), 2015 International Conference.

[10] Issa Khalil, Ismail Hababeh,Abdallah Khreishah,"Secure inter cloud data migration"Information and Communication Systems (ICICS), 2016 7th International Conference.

[11] Ari juels,"honey encryption beyond brute force barrier",IEEE Security&privacy (volume:12,issue:4,2014).

[12] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[13] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[14] P Bala Gopal, K Hari Kishore, R.R Kalyan Venkatesh, P Harinath Mandalapu “An FPGA Implementation of On Chip UART Testing with BIST Techniques”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015
[15] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.
[16] Mahesh Mudavath, K Hari Kishore, D Venkat Reddy "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs” Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.
[17] N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.
[18] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.
[19] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.
[20] N Bala Dastagiri,, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.
[21] Harikishore Kakarla, Madhavi Latha M and Habibulla Khan, “Transition Optimization in Fault Free Memory Application Using Bus-Align Mode”, European Journal of Scientific Research, Vol.112, No.2, pp.237-245, ISSN: 1450-216x135/1450-202x, October 2013.
[22] T. Padmapriya and V. Saminadan, “Improving Throughput for Downlink Multi user MIMO-LTE Advanced Networks using SINR approximation and Hierarchical CSI feedback”, International Journal of Mobile Design Network and Innovation- Inderscience Publisher, ISSN : 1744-2850 vol. 6, no.1, pp. 14-23, May 2015.
[23] S.V.Manikanthan and K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27Feb.2015, Publisher: IEEE-DOI:10.1109, /ECS.2015.7124833.