AN APPROCH TO ENSURE DATA STORAGE SECURING IN CLOUD COMPUTING

[1]Shreya Bhatt, [2] Prof. Dhiren Prajapati
[1]PG Student, [2]Professor
[1]Computer Engineering
[1]Merchant Engineering College, Basna, Visnagar – Mehsana Highway, Gujarat, India

Abstract: In spite of offering numerous benefits such as convenience, ubiquitous accessibility and scalability, Cloud storage security is one of the top concerns for organizations' security sections. As the data reside outside the physical possession of the owner, sensitive and confidential data needs to be safeguarded by taking supplementary measures to secure Cloud data storage. In this dissertation, we aim to address the issue of Cloud storage security. Particularly, we wish to address the concerns of data integrity and confidentiality by making use of the public key cryptography and hash functions.

Keywords: Cloud computing, Security, Confidentiality, Integrity.

I. INTRODUCTION

Cloud computing can be defined as a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g. server, network, storage, application, and services) that can be rapidly provisioned and released with minimal management effort from the user side and minimal service provider interaction. Cloud Computing Model on basis of deployment divided into four categories. Public Cloud the cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options. It is "cloud made available in a pay-as you-go manner to general public". It is also known as internet. Private Cloud the cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises. It is also known as intranet. Community Cloud it is "shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations)". Hybrid Cloud the cloud infrastructure consists of many clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and the need to offer services in the cloud. It takes shape when a private cloud is supplemented with computing capacity from public clouds the approach of temporarily renting capacity to handle spikes in load is known as "cloud-bursting".In this paper, a secure cloud computing deals with security issues in data storage. One Central Concern in cloud computing is privacy, integrity and confidentiality of data process in cloud. Cloud Security is security principles applied to protect data, applications and infrastructure associated within Cloud Computing Technology. Creating secure and reliable Data Storage and access benefits over remote service provider is big challenge. In Cloud Computing Storage data is stored on multiple third party servers, rather than on the dedicated servers used in traditional networked data storage users sees virtual server when storing data. Data Stored over cloud is cared by cloud service provider(CSP). In Cloud Security Data between application and database can protect data as encrypted package and decrypted when access is granted. For Secure data various techniques and algorithms use like RSA, Hashed Message authentications code (HMAC), Cryptographic Techniques etc. Security fall into two categories.
1.Cloud Service Provider (CSP) or Infrastructure-as-a service(IAAS).
2.Security issued faced by users or customers.

Confidentiality
Once the user host data to the cloud there should be some guarantee that data accessibility will be given only to authorized user. For achieving confidentiality there are two types of encryption algorithm used. Symmetric key cryptography and asymmetric key cryptography used. Same key is used for encryption and decryption in **symmetric key** cryptography examples are DES, AES, Blowfish, IDEA, RC4,3DES. One key for encryption and other key for decryption in **asymmetric key** cryptography RSA, ECC, Diffie-Hellman.

Integrity
Integrity is guarantee that the data stored in cloud is the data retrieved without altering intentionally or unintentionally. It can apply to a stream of messages a single message or selected fields within a message modification causes loss of message integrity. For achieving integrity Hash, SHA, MD5, MAC algorithms are used.

Authentication

Authentication is the process of determine whether someone or something is actual truth. It is a process for confirming the identity. Digital signature is the example of authentication; in digital signature the hash value of message is encrypted with user's private key. Anyone who knows the user's public key is encrypted with user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature.

II.RELATED WORK

Akshita Bhandari et al. [2016] [1] specify for getting faster access of data in massive storage security and gap problem determine for user and cloud service provider. Purposed framework can save data for sharing, transferring and storing in data centers while applying classification of data, Hashed message authentication codes and index building, the data is separated into three-part, user is authentication which he/she prepared digital signature validated by cloud directory. User can build on encrypted data with the help of index search.

M sulochana et al. [2015] [2] identify that the secure outsourcing of sensitive as well as business critical data and process which focus on privacy and integrity of data process in cloud. Author purposed integrity and confidentiality application logic and data logic divide into two cloud public and private. Admin located in private cloud which permit authenticated user for access the storage. admin executes data to provide data confidentiality. Through this it reduces data leakage risk in application logic make sure security and integrity data save in system.

Arjun Kumar et al. [2012] [3] describe a cloud storage service in this data saved in many third-party servers except one dedicated server in traditional network data storage. Not even user to know where actual data located, only this knowledge known by cloud service provider stated to keep safe data and store in plaintext format is security threat. Cloud service provider breaks the rule, all data is encrypted and protected using ECC encryption algorithm it accessed by only user. Authors explain that in time to come group sharing data problem also solved only group member can access stored data over shared data section.

Swapnali more et al. [2016] [4] identify that stored user's data can be changed or attacked by outside attacker.so user focusing on integrity of data. A new method for achieving integrity with confidentiality is Third Party Auditor (TPA) for auditing data. This secure method provide privacy preserving, public auditing with the help of three major entities data owner, TPA and cloud server. Authors claim that while using this method it executes activities to generating hash value for encrypted block received from cloud server sequencing them to generate signature on it. After sometimes differentiate signatures whether cloud stored data is tempered or not using AES, RSA, SHA-2 algorithm. Authors will plan to be in future, data dynamic operation such as insertion, updating and deletion of data.

Mrinal kanti Sarkar et al. [2016] [5] identify that latest computational framework associate with software as service, hardware on demand and computational infrastructure has power to reduce cost of IT related service .user can store their data into storage as per requirement. Many data stored in some interconnect resource pool, but pool is placed in some another place in world. Using virtual machine another unauthorized user can use data which create insecure medium. Authors proposed hybrid encryption schemes for encryption and retrieve data efficiently. Result of this search or analysis architecture are feasible, efficient and scalable.

PENG Young et al. [2012] [6] identify that users concerns more and more about security and privacy issues involved in these techniques. From industrial and academic viewpoints cryptography is considered as a key technology to solve security and privacy problems. In this paper they analyze and indicate what type of cryptographic techniques is mainly adopted in relationship between secure cloud storage and cryptographic techniques, they gave review on secure cloud storages, sub-offering within IaaS of cloud computing, in future it is believed that more cryptographic techniques can be applied to cloud computing and more secure cloud storage system proposed.

III.PROPOSED WORK

There are four types of entities **Cloud Data owner** have right control of set of element. **Cloud service provider(CSP)** are describe companies that offers new services, infrastructure or business application in cloud. **Cloud data user** who use services from CSP.**Key Distribution Center (KDC)** where each user has a single key shared with a KDC.The session key management and authentication is done by KDC.For achieving confidentiality in storage security two types of encryption used. Symmetric encryption also known as secret key encryption. The sender and receiver must share the algorithm and the key. Same key is used for encryption and decryption algorithm DES and AES algorithm used. Asymmetric algorithm one key for encryption and other key for decryption.it is also called public key encryption. The sender and receiver must each have one of the matched pair of keys.RSA and Diffie –Hellman algorithm used. For checking integrity MD5 and SHA algorithm used.

There are five functions which are performed for achieving storage security.

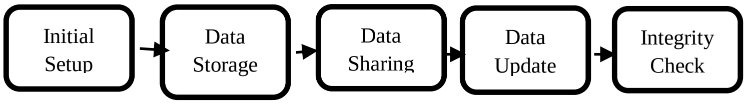
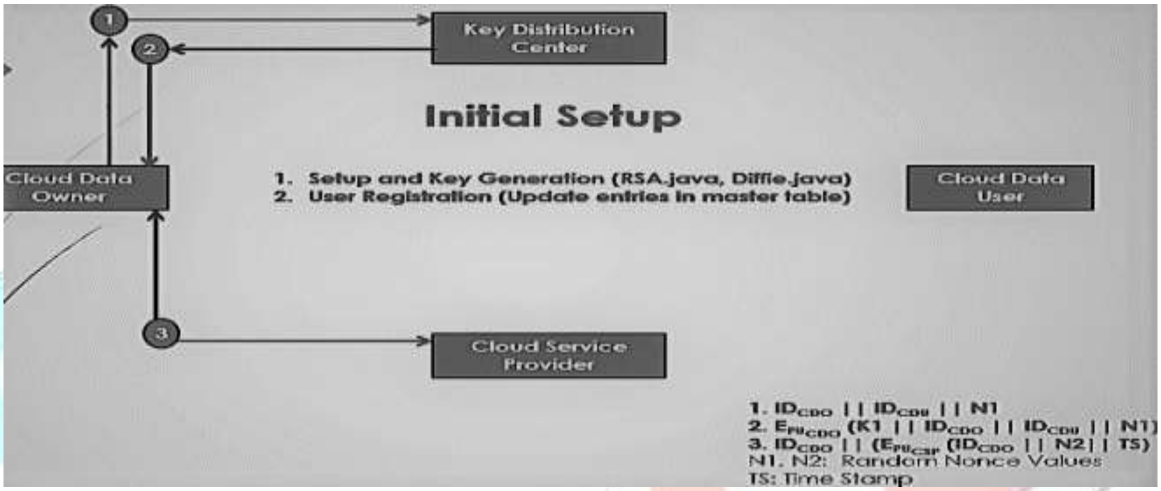


Fig. 1. Function for achieving security

A. Initial Setup

There are following two types of function performed in initial setup. Setup and key generation and User registration.



Initial Setup

1. Setup and Key Generation (RSA.java, Diffie.java)
2. User Registration (Update entries in master table)

1. ID_{CDO} | | ID_{CDU} | | N1
2. $E_{PU_{CDO}}$ (K1 | | ID_{CDO} | | ID_{CDU} | | N1)
3. ID_{CDO} | | ($E_{PU_{CSP}}$ (ID_{CDO} | | N2| | TS)

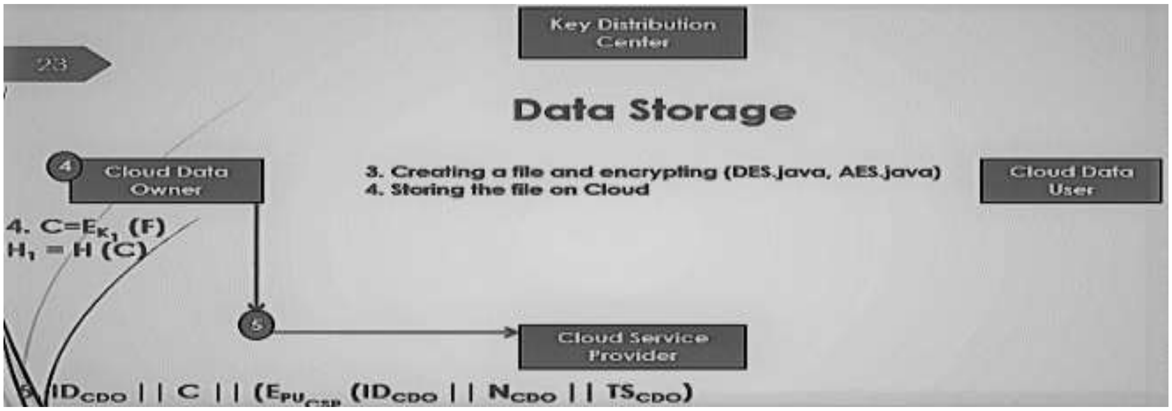
N1. N2: Random Nonce Values
TS: Time Stamp

Fig. 2. Initial Setup

Cloud Data Owner(CDO) request for key to the key distribution center (KDC) to protect logical connection. It includes with identity of cloud data owner and cloud data user (CSU). KDC generate key and encrypt with CDO public key send it to the Cloud Data Owner. CDO decrypt with its private key and gets key, ID of CDO, ID of CDU and random nonce N1. If KDC send many keys to same cloud data owner so for verify key used Time stamp. Nonce is value which is different in time duration.
CDO gets key and for registration purpose key will be encrypted by CDO with another random nonce and send it to CSP.It will be store in cloud. Cloud data owner ID, time stamp and nonce value decrypted by CSP private key. In future CSP acknowledgement to CDO for successful registration.

B. Data Storage

Cloud Data Owner (CDO) create the file apply unique key K1 to the file encrypt it and generate cipher text. hash function can be applied in given file cipher text and calculate hash function value using SHA algorithm. CDO have ID of CDO, Time stamp of CDO, Nonce and given cipher text encrypted with public key of CSP store in cloud.



Data Storage

3. Creating a file and encrypting (DES.java, AES.java)
4. Storing the file on Cloud

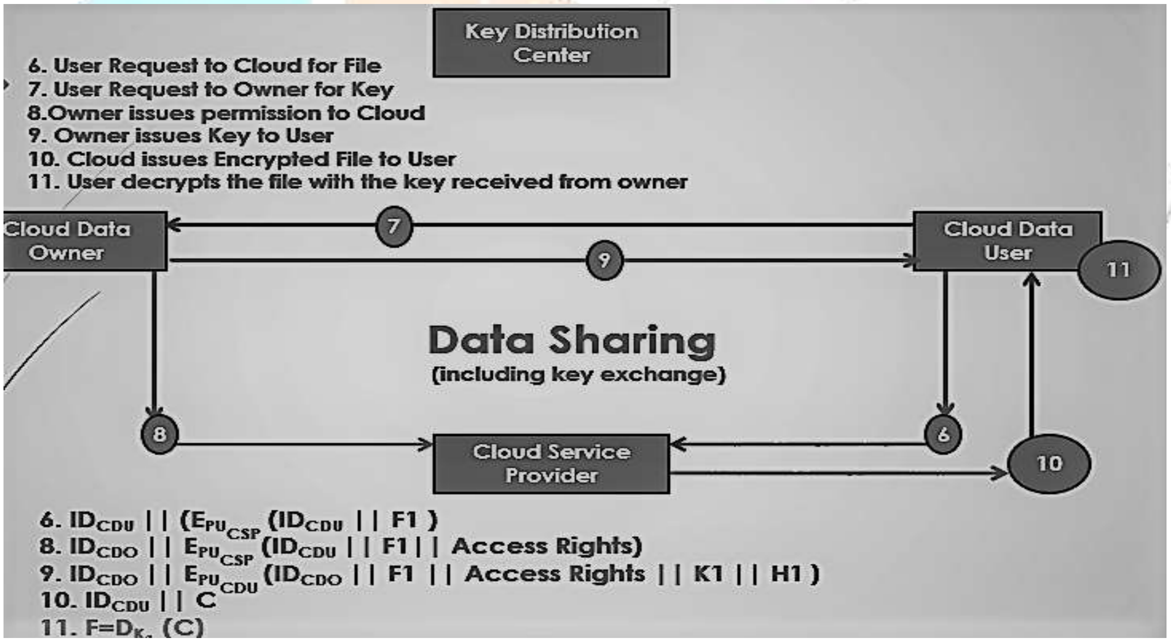
4. $C=E_{K_1}(F)$
$H_1 = H(C)$

5. $ID_{CDO} \mid\mid C \mid\mid (E_{PU_{CSP}} (ID_{CDO} \mid\mid N_{CDO} \mid\mid TS_{CDO})$

Fig. 3. Data Storage

C. Data Sharing

User request to cloud for file F. Cloud (CSP) encrypted ID of Cloud Data User (CDU) and file, send it to Cloud Data User. User request to owner for key. Owner issues permission to cloud. cloud gives access right to CDO.owner issues key to user. Cloud issues encrypted file to user. User decrypts the file with the key received from owner.



6. User Request to Cloud for File
7. User Request to Owner for Key
8.Owner issues permission to Cloud
9. Owner issues Key to User
10. Cloud issues Encrypted File to User
11. User decrypts the file with the key received from owner

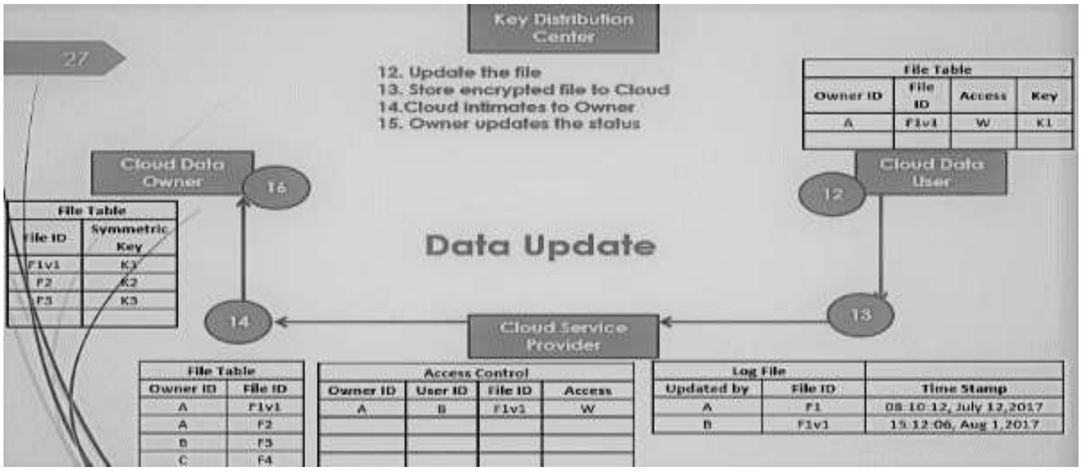
Data Sharing
(including key exchange)

6. $ID_{CDU} \mid\mid (E_{PU_{CSP}} (ID_{CDU} \mid\mid F1)$
8. $ID_{CDO} \mid\mid E_{PU_{CSP}} (ID_{CDU} \mid\mid F1 \mid\mid$ Access Rights)
9. $ID_{CDO} \mid\mid E_{PU_{CDU}} (ID_{CDO} \mid\mid F1 \mid\mid$ Access Rights $\mid\mid K1 \mid\mid H1)$
10. $ID_{CDU} \mid\mid C$
11. $F=D_{K_1}(C)$

Fig. 4. Data Sharing

D. Data Update

Cloud Data user (CDU) wants to update the file which are stored in cloud. If owner gives access for write so user gets chance to update the file. when user access file and updated with own steps cloud intimate to owner that this user changed something in file.CDO gives access to CDU so it will be stored as a new updated version.



12. Update the file
13. Store encrypted file to Cloud
14.Cloud intimates to Owner
15. Owner updates the status

File Table	
File ID	Symmetric Key
F1v1	K1
F2	K2
F3	K3

File Table			
Owner ID	File ID	Access	Key
A	F1v1	W	K1

File Table	
Owner ID	File ID
A	F1v1
A	F2
B	F3
C	F4

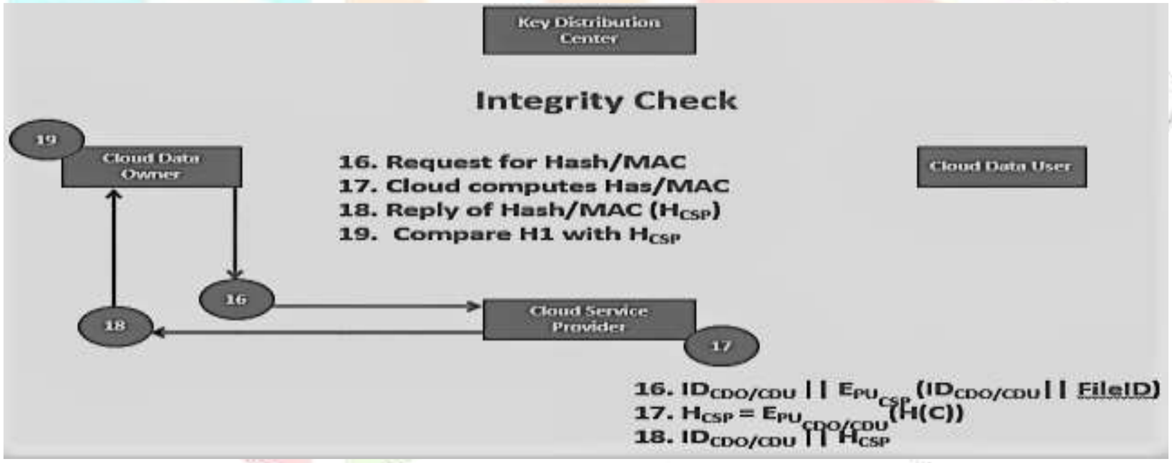
Access Control			
Owner ID	User ID	File ID	Access
A	B	F1v1	W

Log File		
Updated by	File ID	Time Stamp
A	F1	08:10:12, July 12,2017
B	F1v1	15:12:06, Aug 1,2017

Fig. 5. Data Update

E. Integrity Check

For check whether file is modified or not cloud data owner (CDO) request Hash/Mac to the Cloud Service Provider (CSP). CSP calculate and send H1’ to CDO. CDO match its calculated H1 and H1’. If match, then integrity protected otherwise not protected.



16. Request for Hash/MAC
17. Cloud computes Has/MAC
18. Reply of Hash/MAC (H_{CSP})
19. Compare H1 with H_{CSP}

16. $ID_{CDO/CDU} \,||\, E_{PU_{CSP}}(ID_{CDO/CDU} \,||\, FileID)$
17. $H_{CSP} = E_{PU_{CDO/CDU}}(H(C))$
18. $ID_{CDO/CDU} \,||\, H_{CSP}$

Fig. 6. Integrity Check

CONCLUSION

In spite of offering numerous benefits, due to lack of physical control over data, users still hesitate to use Cloud for their data storage. Security has been identified as one of the key challenges in Cloud. In this research, we have addressed the issue of Cloud data security by proposing a model prototype. Our model prototype aims to achieve confidentiality and integrity. The proposed prototype has been classified among various functions and each block of the prototype has been implemented. We have also setup the Cloud environment using VMWare ESXi server. In next phase of our dissertation, we wish to check the security aspects of our prototype through security protocol verification tool such as Scyther. Further, the proposed modules are to be tested on VMWare ESXi server.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my advisor prof. Dhiren Prajapati for the continuous support of my research, for his patience, motivation, enthusiasm and immense knowledge his guidance helped me in all the time of research. I am grateful to all the faculties, HOD, principal for providing sufficient information about the research. I am also thankful to my beloved parents.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, “National Institute of Standards and Technology, Information Technology Laboratory 800-145, September 2011.

[2] Mastering cloud computing by Rajkumar Buvya, C. Vecchiola & S. Thamarai Selvi McGraw Hill Publication, 2013.

[3] M Sulochana ,Ojaswani Dubey, “Preserving Data Confidentiality using Multi-Cloud Architecture”,2nd International Symposium on Big Data and Cloud Computing (ISBCC’15) ,Procedia Computer Science 50(2015)357-362.

[4] Akshita Bhandari, Ashutosh Gupta,Debasis Das, “A framework for Data Security and Storage in Cloud Computing”,2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),978-5090-0082-1/16/$31.00 ©2016 IEEE.

[5] Arjun Kumar,Byung Gook Lee,Hoonjae Lee,Anu Kumari, “Secure Storage and Access of Dara in Cloud Computing”,978-1-4673-4828-7/12/$31.00 © 2012 IEEE,ICTC 2012.

[6] Swapnali More, Sangita Chaudhari, “Third Party Public Auditing scheme for Cloud Storage”,7th International Conference on communication, Computing and Virtualization 2016,Procedia Computer Science 79(2016)69-76.

[7] Mrinal Kanti Sarkar ,Sanjay Kumar, “Ensuring DATA Storage Security in Cloud Computing Based on Hybrid Encryption Schemes” 2016 Fourth International Conference on Parallel ,Distributed and Grid Computing (PDGC), 978-1-5090-3669-1/16/$31.00 ©2016 IEEE.

[8] G.L.Prakash,M. Prateek and I. Singh, “Data Encryption and Decryption Algorithms using Key Rotation for Data Security in Cloud System", International Journal Of Engineering And Computer Science vol .3 , issue 4, pp. 5215-5223,April 2014.

[9] Zissis, Dimitrios, and Dimitrios Lekkas. “Addressing cloud computing security issues”, Future Generation computer system 28.3 (2012):583-592.

[10] Con Wang , Qian Wang ,Kui Ren ,and Wenjng Lou, “Ensuring Data Storage Security in Cloud Computing”,17th International workshop on Quality of service, USA, pp1-9 ,2009,ISBN:978-42443875-4.