IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Security Enhancement through Third Party Auditing for Data Storage in Cloud Computing using RC5 Algorithm

T. Kalaiselvi[1], Dr. S. Ravichandran Ph.D.,[2]

M. Phil Research Scholar, H.H. The Rajah's College (Autonomous), Pudukkottai, India[1]

Head of the Department in Computer Applications, H.H. The Rajah's College (Autonomous), Pudukkottai, India[2]

Abstract: Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Many users place their data in the cloud, so correctness of data and security is a prime concern. Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interconnecting the large-scale computing resources to effectively integrate, and to computing resources as a service to users. To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud., the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently with RC5 Encryption Algorithm. This shows the proposed scheme is highly efficient and data modification attack, and even server colluding attacks. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

Keywords: Cloud computing, Encryption, Data integrity, Third Party Auditor (TPA), RC5 Algorithm, privacy-preserving, public auditability.

1. INTRODUCTION

A. Cloud Computing**:** Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider [1]. The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries. Since the security is not provided in cloud, many companies adopt their unique security structure. The data placed in the cloud is accessible to everyone, security is not guaranteed. To ensure security, cryptographic techniques cannot be directly adopted. Sometimes the cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, we introduce an effective third party auditor to audit the user‟s outsourced data when needed. The security is achieved by RC5 Encryption Algorithm. We utilized public key based homomorphic authenticator with random masking to achieve privacy preserving auditing protocol.TPA performs the auditing task for each user.[2]

B. Third party Auditor (TPA): Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform [3]. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.
Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. A novel and homogeneous structure is introduced [4] to provide security to different cloud types. To achieve data storage security, RC5 algorithm is used. RC5 algorithm is efficient and safer than the former algorithms. It allows TPA to perform multiple auditing tasks for different users at the same.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

2. SYSTEM STUDY

2.1 EXISTING SYSTEM:

Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public audit ability and data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing.

2.1.1 DISADVANTAGES OF EXISTING SYSTEM:

1. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.
2. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.
3. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those uncased data and might be too late to recover the data loss or damage.
4. Encryption does not completely solve the problem of protecting data privacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

2.2 PROPOSED SYSTEM:

We propose a heuristic auditing strategy (HAS) which adds appropriate reads to reveal as many violations as possible. Our key contributions are as follows. We present a novel consistency as a service (CaaS) model, where a group of users that constitute an audit cloud can verify whether the data cloud provides the promised level of consistency or not. We propose a two-level auditing structure, which only requires a loosely synchronized clock for ordering operations in an audit cloud. We design algorithms to quantify the severity of violations with different metrics. We devise a heuristic auditing strategy (HAS) to reveal as many violations as possible. Extensive experiments were performed using a combination of simulations and real cloud deployments to validate HAS.

2.2.1 ADVANTAGES OF PROPOSED SYSTEM:

1. As a rising subject, cloud consistency is playing an increasingly important role in the decision support activity of every walk of life.
2. Get Efficient Item set result based on the case.
3. A fragment technique is introduced in this paper to improve performance and reduce extra storage.
4. The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.
5. Each TPA to audit for a batch of files and to save the times for auditing the files.

2.3 LITERATURE REVIEW

Our contribution in this paper is summarized as follows:

1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data with RC5 Algorithm.

2.3.1 RELATED WORK

Ateniese et al. are the first to consider public auditability in their defined "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA based homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor.

Juels et al. describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Almost simultaneously

Erway et al. [18] developed a skip lists based scheme to enable provable data possession with full dynamics support. However, the verification in these two protocols requires the linear combination of sampled blocks just as and thus does not support privacy preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations.

2.3.2 PRESENT WORK

In this paper we know about cloud computing security and find the problem in cloud data security using third party auditor and what is work of TPA and CSP and how can solve the problem when client and csp share the data in network and literature review.

3. RESEARCH METHODOLOGY

3.1. INTRODUCTION

Cloud Computing is innovation that uses advanced computational power and improved storage. Cloud computing, is a new kind of computing model. It is extend of changing with the need. With the rapid development of the Internet, user's requirement is realized through the Internet, different from shifting with the need. In fact cloud computing is a kind of grid computing, distributed computing, and parallel computing. Its forefront is to provide secure, quick, well-situated data storage and net computing service centered by internet. The characteristics of cloud computing is the virtualization, distribution and dynamically extendibility. Virtualization is the key quality. Most software and hardware have provided carry on to virtualization.

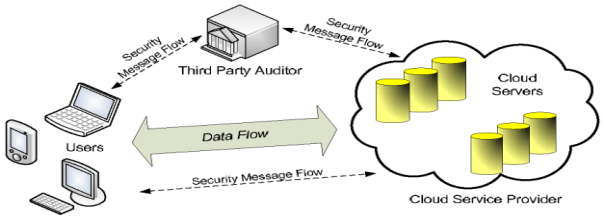


Fig. 1: The architecture of cloud data storage service

In this paper, we consider data storage and sharing services in the cloud with three entities: the cloud, the third party auditor (TPA), and users who participate as a group (as shown in Fig. 1). Users in a group include one original user and a number of group users. The original user is the original owner of data, and shares data in the cloud with other users. Based on access control policies [5], other users in the group are able to access, download and modify shared data. The cloud provides data storage and sharing services for users, and has ample storage space. The third party auditor is able to verify the integrity of shared data based on requests from users, without downloading the entire data. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud, and retrieves an auditing proof of shared data from the cloud. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

3.2 ENSURING DATA SECURITY WITH ENCRYPTION

One of the best ways to ensure confidential data is protected in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage, but few offer support for data at rest. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted [6]. Encryption plays a big role in fulfillment as many policies require specific data elements to be encrypted. The most important guidance on encryption is publically available from NIST 800-111 and FIPS-140-2. These standards can help you evaluate the encryption capabilities of a cloud provider for compliance with regulations. To protect a user,,s confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

Cloud computing describes the combination of logical entities like data, software which are accessible via internet.Client data is generally stored in banks of servers spread across the globe. The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can find multiple

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server. Computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. The fore mentioned approaches burdens the client by which makes it additionally accountable forsecuring it data before storing it to the cloud storage.

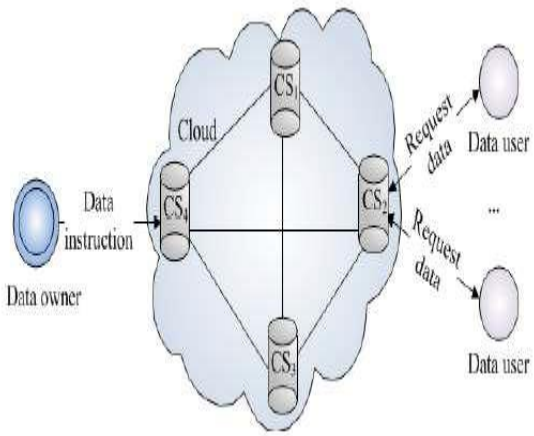


Fig. 3.2: A Typical Cloud Environment

Our objective is to build a security service which will be provided with a trusted 3rd party, and would lead to providing only security services and wouldn't store any data in its system. Detailing it further:
1. To construct Web service system which would provide data integrity verification, provide encryption/decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this web service before uploading/downloading the data to and from cloud.

3.3 DEPLOYING RC5 ENCRYPTION ALGORITHM AT MANJRASOFT ANEKA2.0 CLOUD ENVIRONMENT

Aneka is a market oriented Cloud development and management platform with rapid application development and workload distribution capabilities. Aneka is an integrated middleware package which allows you to build and manage an interconnected network in addition to accelerating development, deployment and management of distributed applications using Microsoft .NET frameworks on these networks.

The TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users. The use of RC5 algorithm for encryption, cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key that cannot be restored. Only the user knows the key, the clouds do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage. In this paper, we introduce a dynamic audit service for integrity verification of untrusted and outsourced storages. Our audit system, based on novel audit system architecture, can support dynamic data operations and timely abnormal detection with the help of several effective techniques, such as fragment structure, random sampling, and index hash table. We propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof of concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show our system has a lower computation cost, as well as a shorter extra storage for integrity verification.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

4.3MODULE

4.3.1 User Module

In this module, user should register their details and get the secret key for login and user can upload the file regarding the auditing.

4.3.2. Auditor Module

1. In this module, auditor can do the auditing based on the heuristic auditing strategy. its relates with document verification.
2. Auditor can check the auditing file he can negated or accept the file he can revise the report and check whether it's good or bad
3. And auditor can give revision report like accept or waiting.
4. If status in accept means user can view the file else status is waiting means user cant view the file.

4.3.3. Admin module

In this module admin can view all the user details, user uploads details, and TPA activities regarding the auditing strategy.

4.3.4. Data Upload Module (in cloud database)

In this module, the user uploaded files can be stored in cloud database it can be very secure auditor can view the file from the database.

5. SYSTEM DESIGN

The system provides hash, access list, encryption/decryption by a trusted 3rd party over the network in the form of "Software as a Service" (SaaS). The system has a separate storage service which is also provided as a SaaS. The data storage for each client is done in database in the form of "BLOB". The trusted 3rd party which provides these security services does not store any data at its ends, and stores only master key for each client for data encryption and decryption, and hash of the data which is calculated on client side.

To enhance the security, the communication between client and security server is secured using Diffie Hellmen key, which is used as a input for AES. This division of responsibility has big effect, as no single provider has access to other data and security key, hash at the same time.

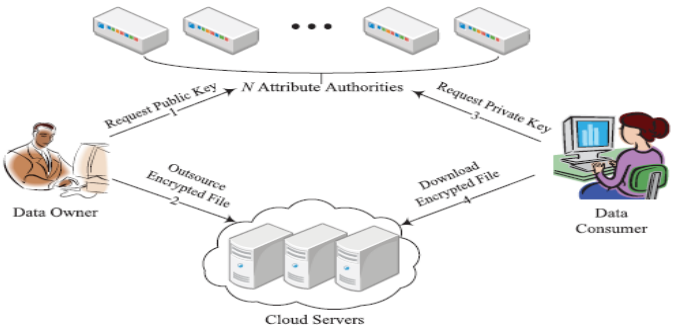


Figure show the use case diagram of the system.

6. ALGORITHM

It checks the integrity of data and maintaining consistency at cloud data storage for Client and CSP.

For example of RC5 with ElGamal digital signature algorithm.

1) Choose the two large prime number p and q.
Like **p=7 and q=17.**

2) Calculate N= (p*q). N=7*17 N= 119.

3) Select the public key □(n) = (p-1)*(q-1) such that it is not a factor of this.

ϕ(n) = (7-1)*(17-1)

ϕ(n) = 6*16

ϕ(n) = 96

Researcher have to choose **E** such that none of the factor of **E** is 2 and 3
(Can't choose E= 4, 15, 6….etc) let us choose E **= 5.**

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

4) (D*E) mod ((p-1)*(q-1)) = 1 **calculate D using this way 96*X+1 =?**
(D*5) mod ((7-1)*(17-1)) = 1 96*1+1=97
(D*5) mod (6*16) = 1 96*2+1=193
(D*5) mod 96 = 1 96*3+1=289
D = 3855/5 96*4+1=385
D = 77.
5). Suppose PT = 10, E=5.
CT=105 mod 119.
CT= 40. **For Encrypt.**
6). PT = 4077 mod 119
PT = 10.

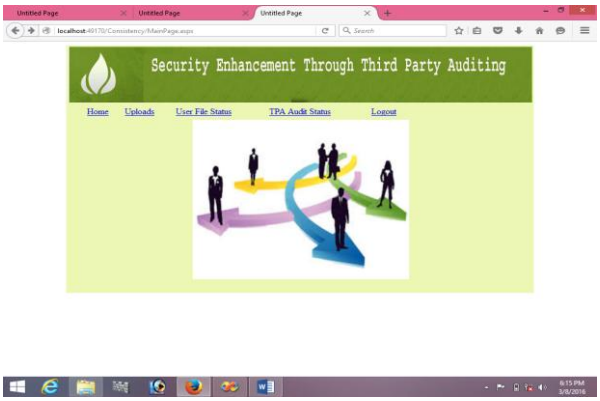
For Decrypt.

For example of RC5 with ElGamal digital signature algorithm.

1) Choose the two large prime number p and q.
Like **p=7 and q=17.**
2) Calculate N= (p*q). N=7*17 N= 119.
3) Select the public key □(n) = (p-1)*(q-1) such that it is not a factor of this.
ϕ(n) = (7-1)*(17-1)
ϕ(n) = 6*16
ϕ(n) = 96
Researcher have to choose **E** such that none of the factor of **E** is 2 and 3
(Can't choose E= 4, 15, 6….etc) let us choose E **= 5.**
4) (D*E) mod ((p-1)*(q-1)) = 1 **calculate D using this way 96*X+1 =?**
(D*5) mod ((7-1)*(17-1)) = 1 96*1+1=97
(D*5) mod (6*16) = 1 96*2+1=193
(D*5) mod 96 = 1 96*3+1=289
D = 3855/5 96*4+1=38

7. RESULT

The implemented RC5-with Elgamal Digital Signature based instantiations in windows 7. And an experiment is Conducted using Java on a System with an Intel core i5-2410M processor running at CPU @ 2.30GHz, installed memory(RAM) 4.00GB, System type: 64-bit OS, Intel® Mobile Express Chipset SATA AHCI Controller, Device type IDE ATA/ATAPI controller, 596.17 GB drive. Algorithms Elgamal Digital Signature is implemented using CloudSim and CloudAnalyst with Eclipse.
Initially researcher created one CSP, data owner and TPA. Data owner gave right to change data to 10 users with identity number and keys. In this identity number he sends to CSP and TPA. This user initially gave the file by using algorithm 1a then applied for all 10 users. Now run algorithms 1a step number 7 for TPA. TPA found all 10 files in appropriate form. Show on figure 4. Work Simulation. Give the overall response time and Response Time by Region; User Base Hourly Response Times, Data Center Hourly Loading and also find that scheme detect error probability about 99%. The data protecting from CSP and TPA is verified by the simulation as we had converted the file into encrypted form and show the analysis of response time and data center processing time and also show response time by region as show on diagram And data center request servicing time as show on figure7.1



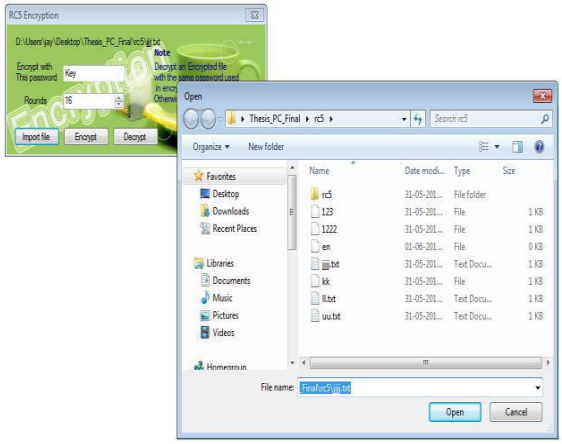
TPA login FORM7.1

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

The Secret key running and encryption wizard



8. CONCLUSION

Cloud Computing is an area full of challenges and of paramount importance. System uses encryption/decryption keys of user‘s data and stores it on remote server. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. Each storage server has an encrypted file system which encrypts the client‘s data and store. Cryptographic techniques are used to provide secure communication between the client and the cloud. The system ensures that the client‘s data is stored only on trusted storage servers and it cannot be accessed by administrators or intruders. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. TPA can perform multiple auditing tasks simultaneously. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use. This paper provides cloud data security using third party auditor.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing”.
[2] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.
[3] G.Ateniese et al., ―Provable Data Possession at Untrusted Stores,‖ Proc. ACM CCS _07, Oct. 2007, pp. 598–609.
[4] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.
[5] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. In: Proc. IEEE INFOCOM. pp. 534–542 (2010)
[6] Mohammed A. AlZain, Ben Soh and Eric Pardede AlZain, M.A.; Soh, B.; Pardede, E. A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012. [
[7] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.
[8] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues. 2010 International Conference on Computational Intelligence and Software Engineering (CiSE).
[9] Panagiotis Kalagiakos, Panagiotis Karampelas, Cloud Computing Learning, Application of Information and Communication Technologies (AICT), 2011 5th International Conference.
[10] Tharam Dillon, Chen Wu and Elizabeth Chang. Cloud Computing: Issues and Challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
[11] Wentao Liu, Research on Cloud Computing Security Problem and Strategy. 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).
[12] Cong Wang, Qian Wang. Toward Secure and Dependable Storage Services in Cloud Computing. Ieee transactions on services computing, vol. 5, no. 2, april-june 2012.
[13] Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, 2008.
[14] M. A. Shah, R. Swaminathan, and M. Baker, “Privacypreserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.
[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS’09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.
[16] R. C.Merkle, “Protocols for public key cryptosystems,” in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.