International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 3, May-Jun-2019, ISSN (Online): 2395-566X

Enhancing Data Security Using Encryption and Splitting Technique over Multi-Cloud Environment

M. Tech. Scholar Brijendra Singh Asst. Prof. Sushil Sharma
Department of CSE,
Institute of Technology and Management (ITM)
Aligarh, Uttar Pradesh, India

***Abstract*- Now days cloud computing become one of the main topic of IT and main point is cloud data storage security. Cloud computing is the fastest growing technology. This technology provides access to many different applications. Cloud computing is used as data storage so data security and privacy issues such as confidentiality, availability and integrity are important factor associated with it. Cloud storage provides user to access remotely store their data so it becomes necessary to protect data from unauthorized access, hackers or any type of modification and malicious behavior. Security is an important concern. The meaning of data storage security is to secure data on storage media. Cloud storage does not require any hardware and software management. it provide high quality applications. As we proposed the concept of cloud data storage security strategy capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. We have developed a desktop application through which user can share data. This paper enhanced advance security goal for cloud data storage.**

***Keywords*- Data security, Cloud computing, Privacy Protection**

I. INTRODUCTION

The boom in cloud computing over the past few years has led to a situation that is common to many innovations and new technologies: many have heard of it, but far fewer actually understand what it is and, more importantly, how it can benefit them. This whitepaper will attempt to clarify these issues by offering a comprehensive definition of cloud computing, and the business benefits it can bring. Security challenges are still amongst the biggest obstacles when considering the adoption of cloud services. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats.

Alongside with these security issues the cloud paradigm comes with a new set of unique features which open the path towards novel security approaches, techniques and architectures. This paper provides a survey on the achievable security merits by making use of multiple distinct clouds simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects Cloud computing offers dynamically scalable resources provisioned as a service over the Internet.

The third-party, on-demand, self-service, pay-per-use and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software.Cloud computing has been intended as the next generation paradigm in information Technology. From this cloud computing environment, both resources and applications are provided through the Internet as a service on demand. Cloud environment is comprised of software and hardware resources in the data centres that run different services over the internet or network to satisfy the user's needs and it depends on sharing resources instead of having local servers to handle application for a certain individual or organization [1] [2]. Since there is no infrastructure investment requires, shrink or expand the resources based on on-demand and the payment based on usage, it becomes popular among different technology aspects. The numerous cloud enterprise system looks for these advantages to be used in various applications.

The service of the cloud makes it possible to access the data at anytime from anywhere. Cloud computing utilize the networks of a huge group of servers naturally brings a low rate data processing with specialized connection. Therefore, cloud computing has an interesting new model of IT service provisioning and support driven by productivity and economic benefits.

Cloud computing can be separated into two subsections such as the cloud and the user. In most scenarios, the individual user is connected to the cloud environment through the internet. This process is also possible for an organization to connect the private cloud via the internet. Therefore, both subsections are alike other than the

utilization of the public and private cloud or the network [3] [4]. The cloud computing has the normal functions such as, the user requests to the cloud and the cloud response to the user [5]. The elasticity and multi-tenancy are two key features of the cloud environment (i.e.) sharing the same service instance, among the various tenants and elasticity enables a service based on the present cloud service demand. Characteristics of this service are to improve the service availability and resource utilization. Cloud services are divided into three service models such as Infrastructure-as-a-service (IaaS), Platform-as-a-service (PaaS), Software-as-a-service (SaaS). Each service has various implementations as shown in Figure 1, which complicates progress of standard security model for each cloud service.

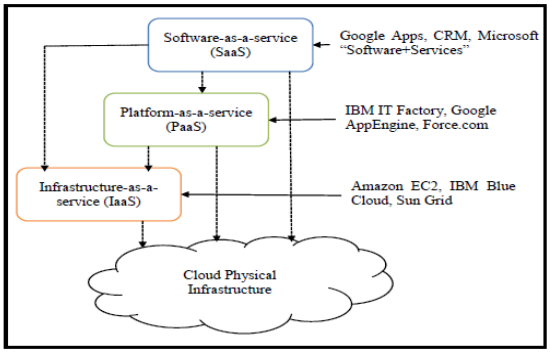

Figure 1 Cloud Service Model.

Usually, make sure that monolithic system track across various PCs means splitting the file into distinct client and server modules. In such schemes, the client module controlled the user interface and the server provided back-end handling, such as record entrance, printing, and so on. As computers proliferated, dropped in cost, and became connected by ever-higher bandwidth networks, splitting software systems into multiple components became more convenient, with each component running on a different computer and performing a specialized function. This approach simplified development, management, administration, and often improved performance and robustness, since failure in one computer did not necessarily disable the entire system.

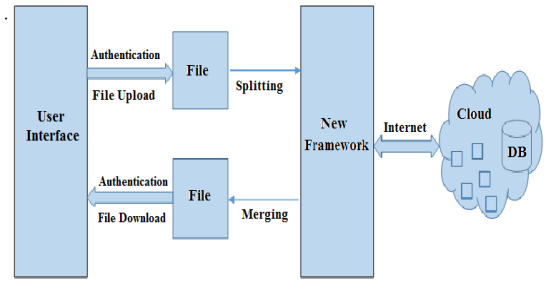

Figure.2. Architecture Diagram.

1. File content splitting: - This module used for splitting the content of file. It takes the file as it"s input. By using the user defined function it split the content of file in several parts is the output of this module. File split uses the open function is to open the file and file is divide into several parts using floor function. It also needs number of parts to be dividing as specified in program.

2. File storing:-This module used for store the split content of file randomly in different places. It takes the input from the „File content splitting module" the content are split in several parts module store it randomly in different places in the cloud storage.

3. File security:-This module generates the accessing key for the user and sends to user. The generated key is used in the login of the user. Key confirms the user authentication.

4. File merge & download:-This module merges all spitted data of specific file. And it provide authentication when retrieve file. It using hash function and key for it. Only authenticate user download the merged files.

5. Objective

The Main Objective are

- Identify existing cloud computing security challenges and their solutions from literature.
- Identify the challenges that have no mitigation strategies defined.
- To overcome Cloud Computing Security Challenges
- Techniques for shielding information within the Cloud
- Strategies for Secure Transition to the Cloud.

II. RELATED WORK

1 Literature review

This approach paper shows that, Cloud Computing becomes thriving and standard business model attribute charming options Additionally to the benefits at hand, the previous options additionally lead to serious cloud specific security problems. The folks whose concern is the Cloud security still hesitate their business to cloud computing. There are main challenges for building a secure and trustworthy cloud system. The use of multiple distinct cloud simultaneously. The various distinct architecture and introduced discussed according their security and privacy capabilities an prospects [1].

Cloud computing supply a replacement of computing with varied services models that facilitates completely different services to the users. As all the info of associate degree enterprises processed remotely and exchanges via completely different network. Security is necessary parameter and also the service supplier makes sure that there no authorized access to the sensitive information of associate degree enterprise throughout the info information [5]. They security and design a efficient decryption, and also design an efficient attribute revocation method that can achieve both forward

backward security[6]. This could be done once, multiple times, or unceasingly. associate degree offender that additionally has access to the process logic of the cloud can even modify the functions and their input and output information. despite the fact that within the majority of cases it's going to be legitimate to assume a cloud supplier to be honest and and accountable manner handling the customers' affairs during a respectful, there still remains a risk of malicious staff of the cloud supplier, palmy attacks and compromisation by third parties, or of actions ordered by a subpoena. Studies on the security of the data storage have witnessed numerous research publications most recently. It is important to strengthen cloud storage security to adhere to Service Level Agreement (SLA). Notable work done by

Popa et al. [5] has emphasized on the SLA by introducing a framework called as Cloud Proof. The framework allows the customer to identify the various forms of violations towards data integrity on Amazon S3 cloud services. The authors have studied the framework using performance parameters like storage overhead and processing time. A similar form of a frame work to identify the violations is proposed by.

Tang et al. [6]; a framework called FADE using conventional cryptography techniques is introduced. The framework is capable of detection of file cloud storage on Amazon S3 cloud. The authors have studied the effectiveness of FADE using rate of data transmission and processing time required for key management.

Ren et al. [7] have proposed a technique of secure data accessibility for mobile application in cloud computing. The study has introduced an encryption policy to maintain the integrity of the data during uploading and downloading the file from the cloud servers. However, the study provides less evidence of its outcome. Study towards security over data sharing was presented by Dong et al. [8],where the authors discussed their security algorithm using a re encryption scheme. The outcome of the study is found to support identity-based encryption scheme as well as public-key encryption scheme at the same time. The technique performs a transformation of the encrypted data of the customer into encrypted text for data security. Bessani et al. [9] have introduced a framework called as DEPSKY for enhancing the data confidentiality, availability, and integrity.

2.2 Data Loss or Leakage: Data loss or leakage, which means a data loss that occur in any device. Data loss happens when data may be logically or physically detached from the organization or user either unintentionally or intentionally[12].When the confidential information, for example, patient or customer data, design specifications or source code, intellectual property, price lists, trade secrets, budgets and forecasts are leaking out[13]. It is a negative impact on the cloud business environment. By protecting and encrypting the integrity of cloud data at the time transit is needed. Additionally, analysis of data encryption and production at both runtime and design should be done. In [14] introduced a novel Universal Serial Bus (USB) memory bus for moving data safety in a cloud environment [15].

Table 1 shows the different types of cloud security category and the table 2 show the different types of Cloud Security Issues and Classifications.

NO	Category	Description
1	Security Standards	Defines the standards needed to take precautionary measures in the cloud computing so as to prevent attacks. It directs the policies of cloud computing for security without compromising reliability and performance.
2	Network	Consist of network attacks such as Denial of Service (DoS), Connection Availability, internet protocol vulnerabilities, DDoS,flooding attack, *etc.*
3	Access Control	Access control and Authentication and. It captures the issues that affect the privacy of user information and data storage.
4	Cloud Infrastructure	Attacks that are strict to the cloud infrastructure (IaaS, PaaS and SaaS) such privileged insiders and tampered binaries
5	Data	Data related security issues, including integrity, data migration, confidentiality, and data warehousing.

Table 2 Cloud Security Issues and Classifications

NO	Category	Issues
1	Security Standards	Absence of legal aspects (Service level agreement) Absence of security standards Compliance risks Trust Absence of auditing
2	Network	Network security configurations Appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities
3	Access	Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
4	Cloud Infrastructure	Quality of service (QoS) Sharing technical flaws Insecure interface of API Multi-tenancy Reliability of Providers Server Location and Backup Security Misconfiguration
5	Data	Data location Data loss and leakage Data redundancy Data privacy Data protection Data recovery Data availability

III. REASERCH METHODOLOGY AND IMPLEMETATION METHOD

Development Phases:

Step 1: Registration Module

In registration get username, email address, password, user generate random verification code. New Random. Next() is used to generate random code. The user can sign in and proceed to next step to verification code. Mail is to user email address by using SMTP protocol. The user can verify the code if verification code is blank then redirect to login page else matched then update user status field with text active and redirect user to the home page.

Step 2: FTP Setting Module

The proposed system, file get distributed at three different location. First location that is our application and next two more FTP where 2nd and 3rd file is store. In proposed system, we design setting page where this will be further used by application to upload and download file from created table. Insert into table FTP details.

Step 3: Upload and Download module

Develop a web interface to upload and download files in cloud storage. The different file uploading links are open. The user can choose the link which we want to upload on cloud. User can upload the file on cloud such as doc file, video, mp3, etc.

Homepage will show list of file uploaded by user from user specific directory. In proposed system, we use data list to show file list .File class to get folder and file details like file name, file size.

- Upload file by using file uploader control we can let the user select file to be upload.
- Get the sever path by using Server. Map Path () function to get path of server directory.

Step 4: File encryption technique module

Setting up and configuring different cloud server in order to having storage cloud access. Each clouds its own server. Developing encryption technique like RSA, AES, DES for file decryption before storing it on cloud. In proposed system, we use combination of AES algorithm and SHA-1 algorithm for encryption and splitting of File.

Step 5: File splitting and clubbing module

In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

Advantages

- Provide authentication.
- Data Security.
- Restrict direct access of files.
- The detection of masquerade activity.
- Data confidentiality.
- Efficiency.

Scope: It introduces new cloud security management framework. The system uses the hashing function & key management to provide the security and authentication to target data. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and Privacy. Cloud computing nowadays is the precondition and essential part of the computing globe using whole day developing in its usages and popularity.

IV.SECURITY ISSUES TO THE CLOUD

The security necessities of a cloud and non-cloud server farm are genuinely similar. The Cloud Security Alliance's starting report contains an alternate kind of scientific classification in light of diverse security areas and procedures that should be followed by and large cloud arrangement. Some protection and security-related issues that are accepted to have long haul essentialness for Cloud computing are:

1 Security Issues Face by Cloud Computing Data Access Control: Generally confidential information will be illicitly accessed attributable to lack of secured information access management.Sensitive information in an exceedingly cloud computing surrounding emerge as major problem with respect to security in an exceedingly cloud based system. Information exists for an extended time in an exceedingly cloud, the upper chance of unauthorized access [4].

2 Data Integrity: Data integrity includes the subsequent cases, once some human error occurs once information is entered. Errors might occur once information is transmitted from one laptop toa nother; otherwise error will occur from some hardware malfunctions, like disk crashes. Code bug or virus can even build viruses. Therefore, at constant time, several cloud computing services clients and supplier accessed & modify information [5].

Therefore, there's a desire of some information integrity methodology in cloud.

3 Data Theft: Cloud computing uses external information server for price affection & versatile for operation. Therefore, there’s an opportunity of information will purloined from external server.

4. Data Loss: Data loss may be a terribly major problem in Cloud computing. If banking and business transactions, analysis and development concepts are all going down on-line, unauthorized individuals are going to be ready to access the dates hared. Albeit everything is secure what if a server goes down or crashes or attacked by a scourge, the complete system would go down & doable information loss might occur. If the seller closes attributable to money or legal issue, there shall be loss of information for the client or user. Client won’t bready to access those information as a result of data is not any additional obtainable for the customer [5].

5 Privacy Issues: Security of the client Personal data is incredibly necessary just in case of cloud computing. Most of the server is external, that the seller ought to make certain that's well secured from alternative operators.

6 Security problems in supplier level: A Cloud is sweet only there's a decent security provided by the seller to the shoppers. Supplier ought to build a decent security layer for the client and user. And may make certain that the server is well secured from all the external threats it's going to come upon [4].

7 User level Issues: User ought to make certain that as a result of its own action, there shouldn't be any loss of information or meddling of information for alternative users who victimization constant cloud[4-5].

V. CLOUD COMPUTING SECURITY CHALLENGES

1. Cloud Computing Security Challenges

Data protection tops the list of cloud concerns today. "Cloud Computing" study, which measured cloud computing trends among technology decision makers. When it comes to public, private, and hybrid cloud solutions, the possibility of compromised information creates tremendous angst. Organizations expect third-party providers to manage the cloud infrastructure, but are often uneasy about granting them visibility into sensitive data.There is a complex data security challenge in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data.

2. Techniques For Protecting Data In The Cloud

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks. The encryption implementation must incorporate a robust key management solution to provide assurance that the keys are sufficiently protected. It's critical to audit the entire encryption and key management solution. Encryption works in concert with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data—and mitigate risk in or out of the cloud.

Therefore, any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.

"It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities.

- Data lockdown
- Access policies
- Security intelligence

3. Strategies for Secure Transition To The Cloud

The fundamental key to data security is to protect what matters. Solutions that enable companies to confidently transition to the cloud while still leveraging many of their traditional infrastructure and investments offer significant advantages. Data Security solves the enterprise cloud security conundrum by protecting data inside of the operating environment while establishing security policies and maintaining control through a centralized management interface. One key differentiator is that works with cloud providers and enterprises to protect data regardless of whether it is located in physical, virtual, or cloud environments. This architecture enables enterprises to control access to the data itself, even as the virtual machine migrates to the virtual and cloud world. Organizations can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments.

4.Split Algorithm

File splitting and clubbing In Proposed system, we are splits the file in different portions then encode and store it on different cloud. Meta data necessary for decrypting and moving a file will be stored in metadata management server. File can club with another file.

5. Folder Lock in folder lock approach, while locking a folder we create xml file inside folder with a password. When user browse for a folder processing our program checks whether folder has xml file exist or not. if folder contain xml file then it popup for password insertion if not then it create xml file with password which user has inserted. The algorithm uses the password to encrypt the

file with a unique number that creates the unique encrypted file. The same password is use to decrypt the file thus enabling maximum security of the file. Let us now see the algorithm in detail.

Step 1: Start.
Step 2: Accept file name and password.
Step 3: Generate unique random number from the password, which serves as the key.
Step 4: Split the file and the key into n splits.
Step 5: Encrypt the first split of the file with the first split of the key, second split of file with second split of key and so on.
Step 6: Combine the splits to get the file
Step 7: Stop

5. Encryption

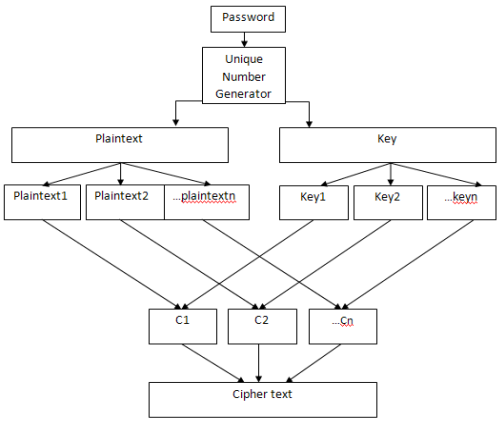

Figure 3 Encryption.

6. Flowchart – Decryption

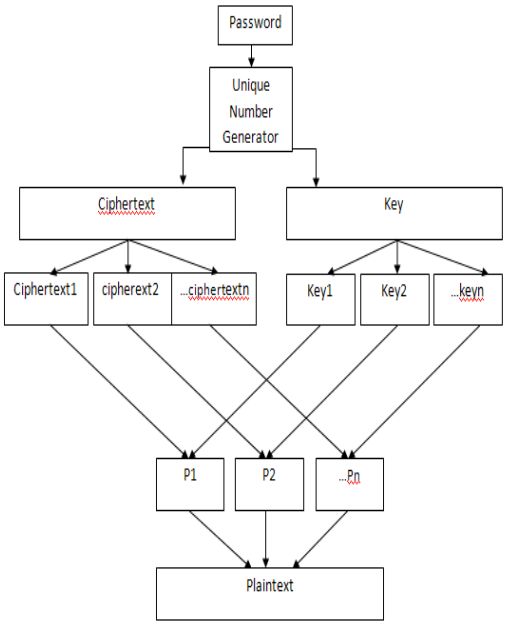

Figure 4 Split-file -key pair algorithm –Decryption

VI. CONCLUSION

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement then AES. RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data. So we are going to implement Split algorithm so that we can split long file and then after we process the encryption and decryption technique.

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be used by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of Split algorithm.

REFERENCES

[1] L. Grandinetti, O. Pisacane, M. Sheikhalishahi, "Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives", IGI Publication, Advances in Systems Analysis, Software Engineering, and High Performance Computing, ISBN-13:978-1466646834, 2013

[2] G.R. Vijay, A.R.M. Reddy, "Investigational Analysis of Security Measures Effectiveness in Cloud Computing: A Study", Computer Engineering and Intelligent Systems, Vol.5, No.7, 2014.

[3] P. Mell, T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology", Special Publication, pp. 800-145, 2011.

[4] A. J. Adoga, G. M. Rabiu, A. A. Audu, "Criteria for Choosing An Effective Cloud Storage Provider", International Journal of Computational Engineering Research, Vol.04, Iss.2, 2014

[5] R.A. Popa., J.R. Lorch., D. Molnar., H.J. Wang., and L. Zhuang.,"Enabling Security in Cloud Storage SLAs with Cloud Proof", InUSENIX Annual Technical Conference, Vol. 242, 2011.

[6] Y. Tang., P.P.C Lee., J.C.S Lui., and R. Perlman., "FADE: Secure overlay cloud storage with file assured deletion", In Security and Privacy in Communication Networks, Springer Berlin Heidelberg, pp.380-397, 2010.

[7] W. Ren., L. Yu., R. Gao., F. Xiong., "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing", TSINGHUA Science and Technology, Vol. 16, No. 5, pp. 520-528, 2011.

[8] X. Dong., R. Li., H. He., W. Zhou., Z. Xue., and H. Wu., "Secure Sensitive Data Sharing on a Big Data Platform", TSINGHUA Science and Technology, Vol. 20, No. 1, pp. 72-80, 2015.

[9] A. Bessani., M. Correia., B. Quaresma., F. Andre, and P. Sousa.,"DepSky: dependable and secure storage in a cloud-of-clouds", ACM Transactions on Storage (TOS), Vol. 9, No. 4, 2013.

[10] J. Stanek., A. Sorniotti., E. Androulaki., and L. Kencl., "A secure data deduplication scheme for cloud storage", In Financial Cryptography and Data Security Springer Berlin Heidelberg, pp. 99-118, 2014.

[11] B.H. Kim., W. Huang., and D. Lie., "Unity: secure and durable personal cloud storage", In Proceedings of the 2012 ACM Work shop on Cloud computing security workshop, pp. 31-36, 2012.

[12] N. Cao., S. Yu., Z. Yang., W. Lou., and Y. T. Hou., "Lt codes basedsecure and reliable cloud storage service", In INFOCOM, Proceedings IEEE, pp. 693-701, 2012.

[13] S. Murthy., "Cryptographic Secure Cloud Storage Model with Anonymous Authentication and Automatic File Recovery", ICTACT Journal on Soft Computing, Vol. 5, No. 1, 2014.

[14] H. Xiong., X. Zhang., D. Yao., X. Wu., and Y. Wen., "Toward send-to-end secure content storage and delivery with public cloud", InProceedings of the second ACM conference on Data and Application Security and Privacy, pp. 257-266, 2012.

[15] P. Gasti., G. Ateniese., and M. Blanton., "Deniable cloud storage: sharing files via public-key deniability", In Proceedings of the 9thannual ACM workshop on Privacy in the electronic society, ACM, pp.31-42, 2010.

[16] S. Kamara., C. Papamanthou., and T. Roeder, "Cs2: A searchable cryptographic cloud storage system", Microsoft Research, Tech Report MSR-TR, Vol.58, 2011.