International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34962-34968

A Framework to Secure Outsourced Data in Public Cloud Storage Environment

Dr. RamalingamSugumar

Professor, Christhuraj Institute of Computer Application Panjappur, Trichy-12.
rsp_sugu74@yahoo.co.in

SharmilaBanu Sheik Imam

Lecturer, Dept. of CCSIT, King Faisal University, Al-Hassa, KSA.
Sharmilasyed@gmail.com

Abstract –
Cloud computing enables the cloud users to effective store and retrieve their sensitive data in cloud virtual storage. Cloud storage provides huge virtual storage space and it is unlimitedly and automatically provisioned to cloud users based on their demand. Cloud storage is more reliable, it means that, data outsourced to the cloud is not physically damaged. Because data outsourced to the cloud is stored in multiple cloud datacenters. Different administrative staff from Cloud Service Providers (CSP) is maintained and controlled the cloud datacenters. Users don't know wherever their data are stored by the CSPs. Users don't know the authorized persons to handle their data in different cloud datacenters. Hence, there a possibility that staff from CSPs could able to access the users' data without the knowledge of users. This is the main security issue in cloud data outsourcing. Security is top most concern in cloud environment. To address the security hurdles in cloud, this paper proposes a framework to secure the outsourced data in cloud environment. The paper also describes about two cloud services named Security and Storage as a Service (SSaaS) and Key as a Service (KaaS). These two services are provided by two independent CSPs. The framework enables users to encrypt sensitive data. Keys used for encryption are generated from KaaS and kept by the users. Experiment is conduct for this framework with medical application data. The framework secures the cloud users data effectively from the CSPs and other intruders.

Keywords- Cloud Computing; Cloud Service Provider; Cloud Security; Data Outsourcing; Encryption;

INTRODUCTION

Cloud computing in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the internet [1]. Cloud Computing is defined as the utility based service since it uses "pay-as-you-work" rule [2]. Cloud is a storage system that allows users to access their data anywhere, anytime and any number of times.Cloud services are delivered over the internet. Cloud provides computational resources like server, storage, operating system and network to users as a service based on their requirements [3]. The advantage of cloud computing is that cloud users could access the resources whenever and wherever they are needed and pay-per-use basis [4]. Core of Cloud service is virtualization. The delivery of computational resources from the cloud to users is in virtualized manner.Cloud has three delivery models namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [5]. Cloud is deployed in four categories such as Public, Private, Hybrid and Community cloud. Cloud differs from other technology by the following characteristics like on-demand services, Network access, Resource Pooling, Elasticity, Auto scaling and metering payments[6].

Cloud mainly a business model. It helps enterprises to have computational infrastructure virtually in cloud environment. Most of the survey reports depicts that cloud has security problems [7]. Data security is the top most issue in cloud computing. Protection of users personal and sensitive data stored in the cloud is more important[8]. In 2007, the cloud service provider, salesforce.com sent a letter to million subscribers describing how customer emails and addresses had been theft by hackers [9].Data security life cycle includes six phases from creation to destroy. In linear progression life cycle model, once the data can bounce between phases without restriction then it will not move to the remaining stages [10]. Figure1 describes the data security life cycle and the phases are explained below.

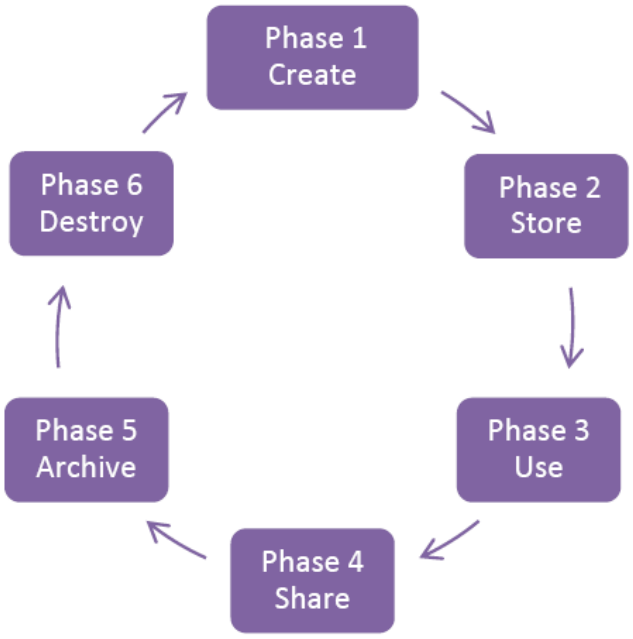

Figure 1. Security Life Cycle

- Create- This phase is the generation of new digital content.
- Store- This phase occurs simultaneously after the creation process, therefore storage of data occurs in the repository.
- Use- This phase uses the data in the repository for various processes.
- Share- In this phase, the transmission of data occurs between customers and the partners.
- Archive- In this phase, stored data is utilized for future use.
- Destroy-This phase will permanently remove the data in the repository.

This paper proposes a framework for securing the outsourced data in cloud. Framework separates the storage and key services from different CSPs. SSaaS has a security service to provide security to users' data. Security is provided by an encryption technique. This encryption technique is used by the user to secure their data. Symmetric keys are used for encryption. The encryption process is done before the data are uploaded to the cloud. Keys used for encryption are only known to the users. Hence, the CSP couldn't access the data outsourced to the cloud. Security of users' data is enhanced by this framework.

RELATED WORK

There are many numbers of research are carried out by researcher to improve the security of data outsourced to the cloud. This section describes some of the existing work done for improving the security of data in cloud. Deepanchakaravarthi et al. [11] has proposed three techniques for data security. 1) To prevent data access from authorized access. So author proposed a distributed scheme for providing security of data for achieving them used homomorphism token with distributed verification of erasure-coded data. 2) Proposed scheme perfectly stores the data and identify the cloud users. 3) Perform some tasks like data updating, deleting, appending. These techniques provide a process to avoid collusion attacks of server modification by unauthorized users.

Sudha et al. [12] have proposed work is to investigate the exiting security schemes and to ensure data confidentiality, integrity and authentication. They proposed model for symmetric and asymmetric cryptography algorithms are adopted for the optimization of data security in cloud computing. Their proposed security framework using cryptography algorithm the data protection is optimized by incorporating both public and private key cryptography systems for various cloud applications.

Abhishek et al. [13] have described a trusted cloud storage architecture which applies the specification of the Trusted Computing Group (TCG). TCG is a global industry standard, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. They are used TPM to encrypt data before storing it to the cloud. They use Kerberos Authentication service to avoid masquerading, replay attack and eavesdropping. They proposed a module widely for the security of cloud storage. Kerberos is a secure method for authenticating requests for any service, is used to authenticate the end user to the trusted gateway.

Sanjoli et al. [14] has proposed architecture used to encrypt and decrypt the file at the user side that provide security for data rest as well as while moving. They proposed Rijndael Encryption Algorithm along with EAP-CHAP. Security is the main concern in cloud computing, it will protect data from unauthorized uses. They proposed two different techniques used for ensuring security in cloud computing namely, Extensible Authentication Protocol (EAP-CHAP) and Rijndael Encryption Algorithm.

Cong Wang et al. [15] described cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, the author has proposed an effective and flexible distributed scheme with two silent features, opposing to its predecessors. Their scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack and even servercolluding attacks. The scheme supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. The strength of their work is reduces the communication overhead and storage overhead when compared to the traditional replication-based file distribution techniques.

Shuai Han et al. [16] described a novel third party auditor scheme. Their strength is a cloud service provider can offer the functions which were provided by the traditional third party auditor and make it trustful and reduces the complexity in the cloud. They proposed architecture for cloud storage which is just composed two parts: User and Advanced Cloud Service Provider; and third party auditor function is combined with the cloud service provider.

Huifeng Wang et al. [17] planned a scheme, which allows the users to check the integrity of their data in the cloud. The author has to present the performance criteria about the

scheme, which can help the researchers optimize their mechanism efficiently and effectively. Their proposed scheme is lightweight, efficient and robust. Their proposed system model contains three parties which are the Cloud Storage Provider (CSP), the users and Third Party Auditor (TPA).

PROBLEM DEFINITION

Cloud provides many benefits to users at the same time it has big concern about security of data. More numbers of research are carried out for securing the cloud environment. But, still cloud security is top most challenge in the cloud environment. Followings are list of security problem derived from the literature.

- Outsourced data are not controlled or monitored by the users.
- Users are not able know the locations where are the data stored.
- Cloud is a public environment, so the data may disclose to other users of the cloud.
- Users are force to use the same CSP for all the services like storage, security and key generation. Hence the CSPs could know the data format and location where the data are stored.
- Key management is very crucial to CSPs, so they maintain a single key for all users data
- Some CSPs are not encrypted the data. Data may be stored in as original form.
- In most of the security framework, users have more work burden to maintain the components of the framework, encryption process and key generation.
- CSPs are the authorized people to access the data without users' knowledge.

MOTIVATION AND OBJECTIVE

The study of existing work helps to motivate to propose framework for secure cloud environment.The following factors are motivated to do this work.

- To secure the public cloud environment to maintain confidentiality of data in cloud storage.
- To reduce the work burden of users in the existing framework.
- To enhance the security by separate the CSPs for each service.
- To maintain the security using symmetric cryptographic technique.
- To ensure that the data stored in the cloud is only accessed by the date owner.

The primary objective of the paper is to propose a framework for maintaining data security in cloud storage.

The proposed frameworkis implemented asecure cloud data storage, which encrypt data using symmetric key cryptography and reduce the time for storing data in the cloud storage.

METHODOLOGY

Cloud provides resources as a service. Figure 2 represents methodological diagram of the proposed framework. The proposed framework uses two services, one for security and storage and other one for key as a service. The users' data are encrypted before they are uploaded to the cloud. Usersare no need to encrypt all data outsourced to the cloud. Before encrypting the data, user should decide which type of data is sensitive and then they select specific data type to encrypt. Once the encryption is completed, then the data are uploaded to the cloud. Symmetric keys are generated from separate key service. Same keys are used to decrypt the data.

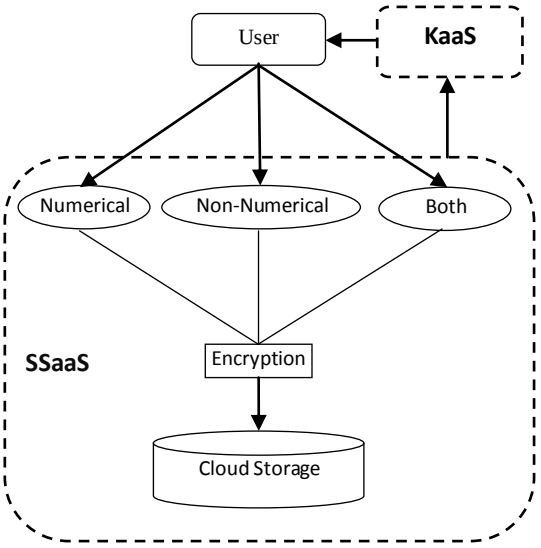

Figure 2. Methodological Diagram of proposed Framework

BASIC ARCHITECTURE OF DATA STORAGE IN CLOUD

Cloud provides an efficient storage setting for store and retrieves the users' sensitive data. Cloud users don'tknow where the data are stored, may the data are mixed with other users' data. User data are stored in cloud storage server. According to security goals are CIA (Confidentiality, Integrity, and Availability) users can store their data in cloud storage. In cloud data storage, users store their data through CSP into a pool of cloud servers, which are operating in a simultaneous, cooperated distributed manner. Users no longer possess their data locally, it is demanding concern to satisfy users that their data are being correctly stored and managed. Figure 3 depicts the basic data storage framework. The basic data storage framework consists of three major entities that are User, Cloud Service Provider and optional Third Party Auditor.

- **User-** Users are stored data in the cloud and depend on the cloud forall computation; it consists of both clients and enterprises.
- **Cloud Service Provider-** CSP who provides services to users andmanaging distributed cloud storage servers.
- **Third Party Auditor-** TPA who have to verify whether a cloud provideris providing service to

customer based on SLA or not. It is an optional entity.

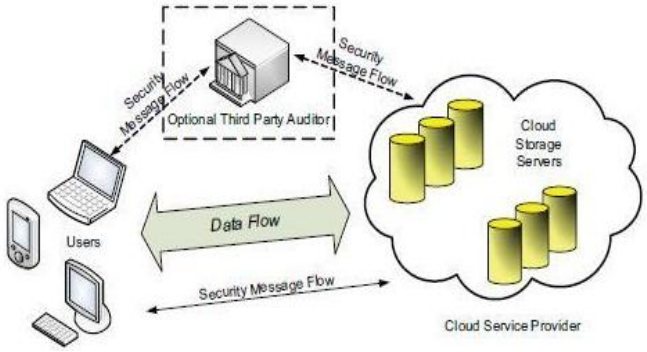

Figure 3. Basic Data Storage framework

PROPOSED FRAMEWORK

The proposed framework consists of three main cloud services, among that Security and Storage services are provided by CSP_1 and Key generation is provided by CSP_2. Figure 4 represents the entities in the proposed framework with its functionality. Users are outsourced their data to CSP_1. CSP_1 provides a security mechanism to users and also suggest the users to encrypt their sensitive data. Users are instruct to select the type of data being encrypted before uploaded to the cloud. Users are given by three choices namely Numeric, Non-Numeric and Both. If the users select numerical data then numerical data are encrypted other data are left as they are. Users should decide that which type of data are sensitive. If users select Both then all data are encrypted. This mechanism should reduce computation and time taken for encrypting insensitive data. The encryption process should not make any latency in network. In this framework, users are no need to maintain any entity of the framework. They should only keep the key for encryption and decryption. Keys are generated from KaaS and send to the users. The key are not communicated to CSP_1. CSP_1 stores the encrypted data without key. CSP_1 could not process all the data without decryption. Decryption is not possible in the CSP_1 because they don't have knowledge of the key. So data stored in the cloud storage is not accessed by the staff from the CSP_1. The framework has different steps to store and retrieve the data. Figure 5 shows the sequence process of the proposed framework. Steps involved in the framework are described below.

1. *Users send upload request to the CSP_1.*
2. *CSP_1 provides a security mechanism to users and ask users to choose the sensitive data. EaaS asks users to select the type of data to be encrypted. Users could select numeric, non-numeric or both type of data to encrypt.*
3. *CSP_1 instructs the KaaS to generate keys and send it the specific users.*
4. *CSP_2 generate the keys and forward it to the users. Keys are not communicated to the CSP_1.*
5. *Users use the key and EaaS to encrypt their sensitive data.*
6. *Once the encryption is completed then the data are uploaded to the cloud storage.*
7. *To retrieve the data users send the query to fetch the data to cloud storage.*
8. *Cloud storage fetches the data based on the user query and transfer to the cloud.*
9. *Users decrypt the data using the key and get the original data.*

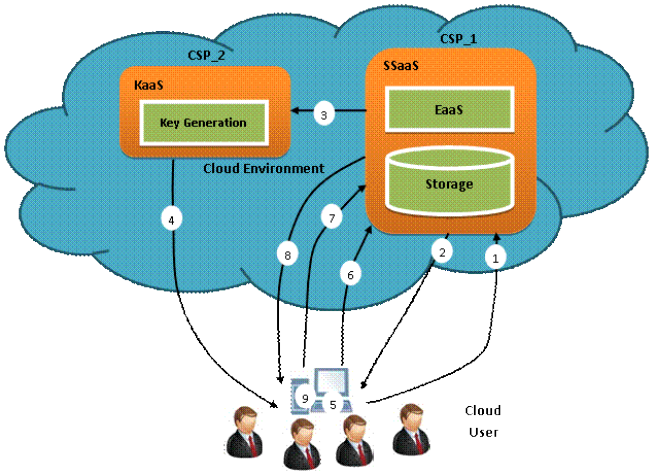

Figure 4. Functionality of Proposed Framework for Cloud Security

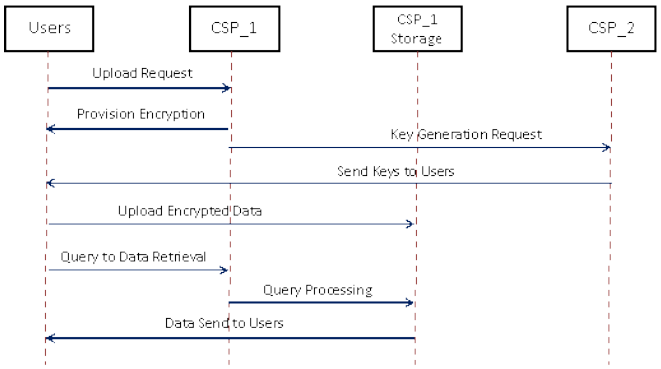

Figure 5. Sequence Diagram of Proposed Framework

EXPERIMENT WITH MEDICAL APPLICATION

The proposed framework is developed to provide a secured environment to the cloud storage users. It addresses the security issues found in the existing framework. The cloud services, namely, SSaaS and KaaS are joined together to provide security to the data in the cloud storage. Simulation is conducted for the proposed framework. Security services in SSaaS and key generation in KaaS are coded as a cloud-based web application and hosted in the Amazon Elastic cloud. SSaaS and KaaS service are implemented in JAVA. Storage service uses storage from Amazon storage servers. Simulation is performed in the cloud environment (Amazon EC2). The cloud users' machine connected to the cloud server has the configuration of Windows Operating System with core i3 Intel processor and 4GB RAM. The users' data are encrypted

before they are uploaded and decrypted when retrieved from the cloud. Thus, the encryption is done in the users' machine connected to the cloud. Time taken for encryption is calculated in the users' machine.

Amazon Elastic Compute Cloud (EC2) server is used for cloud storage. Key generation and encryption technique is developed as web service and hosted in the Amazon server. These services are used for security of data in cloud storage. The Amazon micro instance has the following configuration as Microsoft windows server 2008 Base 32 bit operating system, 2.5 GHz Intel Xeon processor, 613 MB RAM, 30GB of EBS (Elastic Block Storage). The users upload the data via user interface. Once the data are selected for encryption, then they are encrypted and uploaded to Amazon server.

Consider the Medical application; they want to maintain the data of Patients, Doctors, ClericalStaff, Management Staff and other data related to the Medical Field. They are eager to use the cloud storage to reduce their work burden in storing and maintaining the data with their own servers. However, they also have some hesitation when they think of the security of data in the cloud storage. The proposed framework enables them to store their data securely in the cloud storage. For example, consider the patient details as shown in Table I. If Hospital Management (HM) wants to store data shown in Table I into the cloud storage, they should decide which type of data is to be converted from readable into unreadable.

TABLE I SAMPLE MEDICAL DATA PATIENTS

P_ID	P_Name	P_DOB	Diagnosis	Treatment
23435	Kumar	12/03/85	Hypertension	Assessment
34543	Senthil	09/08/90	Tumor	Operated
75647	Ramesh	17/03/83	BP	Monitoring
34564	Suresh	28/05/81	Diabetics	Assessment
98564	Saleem	20/09/78	Asthma	Monitoring

HM hides only the numerical sensitive data of patient like patient id, DOB, DOA, DOL and Telephone No, then they should choose numerical data at the time of encryption or they should choose non-numerical for other data or they should choose both to hide all the data. Users are no need to encrypt all the data uploaded to the cloud.

If HM wants hide the numerical data then Table I data are encrypted and stored like Table II. In Table II, only the numerical type data are encrypted other data are left as they are.

TABLE II ENCRYPTION OF NUMERICAL DATA ONLY

P_ID	P_Name	P_DOB	Diagnosis	Treatment
I;8jr	Kumar	I8ut'5u[	Hypertension	Assessment
P4.;3	Senthil	Ik98^$rT	Tumor	Operated
7ut5.	Ramesh	Sd$e&*/E	BP	Monitoring
02ki]	Suresh	Nu%#gT;<	Diabetics	Assessment
#9io8	Saleem	p)$jfRa#	Asthma	Monitoring

If HM wants hide the non-numerical data then Table I data are encrypted and stored like Table III. In Table III, only the non-numerical type data are encrypted other data are left as they are.

TABLE III ENCRYPTION OF NON-NUMERICAL DATA ONLY

P_ID	P_Name	P_DOB	Diagnosis	Treatment
23435	EI>tj?e84	12/03/85	s@d$f:R%6	MN67%^*Yi;
34543	(*r5t4vW5	09/08/90	#3$R%G6h	T%6$5&6#
75647	T4g6Y3H;<	17/03/83	T5hUjkm>	%4fD6>;'Lk
34564	7y<{gtY5'	28/05/81	+-{UhiKl;'	6&HbF:"?$3
98564	Ae$46:}L>	20/09/78	yGrV^(P	%<>:frT^7$

If HM wants hide the all the data both numeric and non-numeric then Table I data are encrypted and stored like Table IV. In Table IV, both types of data are encrypted. So based on users requirement the data are encrypted.

TABLE IV ENCRYPTION OF BOTH NUMERICAL AND NON-NUMERICAL DATA

P_ID	P_Name	P_DOB	Diagnosis	Treatment
I;8jr	EI>tj?e84	I8ut'5u[	s@d$f:R%6	MN67%^*Yi;
P4.;3	(*r5t4vW5	Ik98^$rT	#3$R%G6h	T%6$5&6#
7ut5.	T4g6Y3H;<	Sd$e&*/E	T5hUjkm>	%4fD6>;'Lk
02ki]	7y<{gtY5'	Nu%#gT;<	+-{UhiKl;'	6&HbF:"?$3
#9io8	Ae$46:}L>	p)$jfRa#	yGrV^(P	%<>:frT^7$

ADVANTAGES OF PROPOSED FRAMEWORK

Generally, Cloud provides many advantages to users. But in security point of view it has more issues. This security issues are address by this proposed framework. The advantages the framework is list below.

- Proposed framework separates the encryption and key service from different CSPs. So CSPs with data doesn't know the key to retrieve the original data.
- Users encrypt only the sensitive data; unimportant data are left as original.
- Users no need to maintain any entities of the framework in their environment except keys
- Encrypts the data before are uploaded to the cloud storage.
- Framework uses symmetric encryption, so encryption process not makes any latency in the data upload.
- CSPs and users could easily adopt this framework.

CONCLUSION

Cloud grips the information technology. Peoples are attracted by its tremendous capabilities. Most of the enterprises are trying to adopt the cloud. Cloud computing is basically a business model. It easily leverages the medium scale enterprises to achieve their goal without huge investment. Apart from all these advantages, cloud is down rated due its security issues. This paper proposed a framework to clean and through away the security problem in cloud. This framework consists of three services; these three services are provided by two different CSPs. The Framework separates the key service and storage service. Users are easily secured their sensitive data by the services provided by this framework. Users' data are encrypted before they are uploaded to the cloud. Keys used for encryption is only known to the users. It is not communicated to the CSPs. CSPs don't able to access the data stored in the cloud. Experiment is conducted with medical data. The framework helps cloud users as well as CSP to secure the data in the cloud environment.

REFERENCE

[1] John, H., L.M. Kaufman and Bruce, P., "Data Security in the World of Cloud Computing", *IEEE Journal of Security & Privacy*, Volume 7, Issue 4, 2009, pp 61-64.

[2] Ali Khajeh-Hosseini, Ian Sommerville and IlangoSriram, "Research Challenges for Enterprise Cloud Computing", *Proceedings ofACM Symposium on Cloud Computing*, 2010, pp. 1-11.

[3] Priyajaiswal, Randeepkaur and Ashok Verma, "Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique", *International Journal of Emerging Technology and Advanced Engineering*, Volume 4, Issue 1, January 2014, pp. 161-164.

[4] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong "The Characteristics of Cloud Computing", *Proceedings of IEEE International Conference on Parallel Processing Workshops*, 2010, pp. 275-279.

[5] Cyril Onwubiko, "Security Issues to Cloud Computing", *Cloud Computing: Principles, Systems and Applications, Computer Communications and Networks*, Springer-Verlag London, Chapter-16, 2010, pp. 271-288.

[6] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", *Technical Report-800-145*, Version 15, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2011.

[7] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", *Elsevier Journal of Advanced in Control Engineering and Information Science*, Procedia Engineering, 2011, pp. 2852-2856.

[8] DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", *Security, Privacy and Trust in Cloud Systems*, Chapter-1: Cloud Security, Springer-Verlag Berlin Heidelberg, 2014, pp. 45-72.

[9] A. Huang Jing, Second B. LI Renfa, and Third C. Tang Zhuo, "The Research of the Data Security for Cloud Disk Based on the Hadoop Framework", *Proceedings ofIEEE International Conference on Intelligent Control and Information Processing*, Beijing, China , June 2013, pp. 293-298.

[10] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", *Proceedings of IEEE International Conference on Computer Science and Electronics Engineering*, 2012, pp. 647-651.

[11] DeepanchakaravarthiPurushothaman and SunithaAbburu, "An Approach for Data Storage Security in Cloud Computing", IJCSI *International Journal of Computer Science Issues*, Volume. 9, Issue 2, No 1, March 2012, pp. 100-105.

[12] M.Sudha ,M.Monica "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", *Advances in Computer Science and its Applications*, Volume 1, Issue 1, March 2012, pp. 32-37.

[13] AbhishekTripathi, Md.Sarfaraz Jail, "Data Access and Integrity with authentication in Hybrid Cloud", *Oriental International Journal of Innovative Engineering Research (OIJIER)*, Volume 1, April 2013, pp. 30-33.

[14] SanjoliSingla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique",*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 2, Issue 7, July 2013, pp. 2232-2235.

[15] Cong Wang,QianWang,KuiRen, and Wenjing Lou, "Ensuring DataStorage Security in Cloud Computing", *Proceedings of IEEE International Workshop on Quality of Service*, July 2009, pp 1-9.

[16] Shuai Han, Jianchuan Xing, "Ensuring Data Storage Security Through A Novel Third Party Auditor

Scheme in Cloud Computing", *IEEE CCIS*, 2011, pp. 264-268.

[17] Huifeng Wang, Zhanhuai Li, Xiaonan Zhao, ChanyingQi,QinluHe,Jian Sun, "A scheme to ensure data security of cloud storage",*IEEE*, 2013, pp. 79-82.

[18] L. Arockiam and S. Monikandan , "Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage", International Journal of Current Engineering and Technology, Vol.4, No.3 , June 2014, pp. 1265-1270.

[19] ArijitUkil, Debasish Jana and Ajanta De Sarkar, "A Security Framework in Cloud Computing Infrastructure", *International Journal of Network Security & Its Applications*, Volume 5, Issue 5, 2013, pp. 11-24.

[20] Basescu C., A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies", *Proceedings of IEEE International Conference on Advanced Information Networking and Applications*, 2011, pp. 459-466.