I.J. Information Engineering and Electronic Business, **2017, 4, 7-12**
Published Online July 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2017.04.02

Security and Privacy for Data Storage Service Scheme in Cloud Computing

Jayashree Agarkhed
Professor, Department of C.S.E, Poojya Doddappa Appa College of Engineering,
Kalaburagi, Karnataka – 585102, India.
Email: jayashreeptl@yahoo.com

Ashalatha R.
Research Scholar, Department of C.S.E, Poojya Doddappa Appa College of Engineering,
Kalaburagi, Karnataka – 585102, India.
Email: ashalatha.dsce@gmail.com

Abstract—The cloud computing features aim at providing security and confidentiality to its customers. The business officials have gained maximum profit using the cloud environment. Therefore the critical data moving to and from the cloud server must be secured. The security and confidentiality issue is the most critical challenge that we are facing in today's world of the cloud environment. The business officials have gained maximum profit accessing the cloud environment. Before the disaster occurrence, the critical data moving to and from the cloud must be preserved. The privacy preservation and cloud security issue is the most serious issue that we are facing in today's world in cloud era.

Index Terms—Cloud computing, Cryptography, Optimization, Privacy preserving, Security.

I. Introduction

Cloud computing targets best in class service to all its users. One of the main issues to be considered is a privacy and security of cloud data in cloud computing. The traditional database technologies cannot perfectly stock and investigate the huge volume of data. Because of the enormous growth of the customers in startups, business, and enterprises, the data security and confidentiality has become the required issue in the cloud environment. The network traffic around VMs (virtual machines) along with the data centers in the cloud must be encrypted for security and privacy reasons for any human or network failures. The breach in confidential data files and its privacy will ultimately lead to data leakage and heavy damage to the applications throughout the disaster process [1]. Hardware, software security during disaster management is considered as important issues under cloud computing. Usually, the data and applications in the network are deposited and retrieved from data centers remotely. Hence safeguarding the data and VMs plays a critical part in securing the cloud during the disaster recovery process [2]. The cloud computing features aim at providing security and confidentiality to its customers. The business officials have gained maximum profit using the cloud environment. Therefore the critical data moving to and from the cloud must be protected. The increase in a number of users in the Internet, social networking media and multimedia has led the huge management of data in a cloud computing environment. Major issues of cloud computing includes security, protection, resource management and power and energy management. Data confidentiality means safeguarding the data from unauthorized access from third party hackers. For adhering privacy and security of confidential data files, the cryptographic tool shows a critical role in cloud environments.

Cloud computing is named as virtual computing in information technology which makes use of virtual data centers and also needs an ultimate privacy protection. Privacy refers to the owner's data that is being outsourced to the cloud. Data privacy may breach because of multiple threats and data misuse from attackers. Data duplication is one method to control data leakage and misuse. Privacy is one of the biggest challenging issues in cloud computing. Privacy preserving of data means the confidential information should not be leaked to the TPA during the auditing process. The cloud service provider uses encryption technology for security over the cloud data.

The security and privacy concerns include various issues such as identity management, protection of data, data privacy and operations. Privacy requires encrypting and decrypting the data files while at rest or while transmission over the cloud. Strong authentication techniques and secure algorithms will help the confidential data to be secured within the cloud premises. The privacy preserving schemes include access control, encryption strategy, key management, policy, proxy, security, signature and central authority. Data confidentiality refers to protecting the data from unauthorized access from third party users. For adhering privacy and security of confidential data files, cryptographic tool plays a vital role in cloud environments [3].

A. Data Disaster in Cloud

Disaster Recovery refers to the cloud storage allows the backup option for the cloud data as the emergency situation required it. Reporting and monitoring were named by interviews as "a very significant part of any information security program". Thereby confidentiality, integrity, and availability issues of the cloud data files can be controlled and reported and financial institutions can still possess control over cloud providers' data accesses. Incident management, business stability, and disaster rescue management were pointed out as important measurements to guarantee the availability of data. "Data center mirroring" was named as a mandatory measure to protect data, whereby "minimal distance" between the data centers must be considered to guarantee the required response time and avoid any simultaneous outage for data centers in case of catastrophic failures or natural disasters.

B. Data Privacy in cloud

Privacy preserving of data means the confidential information should not be leaked to the TPA (Third Party Auditor) during the auditing process. The enlargement in immediate disasters from place to place is taking hundreds of surviving and demolition of infrastructure and properties. A new solution has to be formed for disaster data management in cloud framework. The cloud provider uses encryption technology for security over the cloud data. The sensitive data are protected using the encryption-based system for securing the cloud systems. Privacy requires cryptographic actions on the data files while at rest or while transmitting over the cloud during disaster recovery. The cloud service supplier should maintain disaster recovery protocols for securing the user's confidential files [4].

The remainder of this paper is organized as follows. Section 2 reviews the literature. Section 3 presents the system model. Section 4 gives methodology part. Section 5 presents the result analysis. Section 6 ends with the conclusion part.

II. Related Work

An Extensive review of the literature has been done on security issues and privacy concerns about data files in the field of cloud computing. The data sharing service in the environment of cloud provides dynamic access to the data using privacy preserving technique for data policy methods. In this method, a cipher text strategy, technique using attribute and the encryption technique helps in full preserving the privacy and confidentiality of users. The proposed identity-based encryption method allows dynamic operations securely over the cloud. The policy verifies the security using the generic bi-linear model. Data security has been ensured and the secrecy of cloud user has been preserved. The effective and scalable encryption in cloud service for sharing the data has been planned to accomplish collusion resistance of data. Random oracle method is used for sharing and security of the cloud data. The result examination shows that the given method uses smaller overhead than other methods. The scheme allows hash function using bi-linear mapping function for key generation and decryption. The system model contains four entities which are data owner, data user, cloud server and private key generator. The cloud data sharing system provides user access easily and efficiently. In order to maintain privacy preservation, effective encryption scheme has been given in this work. The attribute-based cryptographic scheme comprises of four algorithms, namely system initialization, encryption, key generation and decryption. The security requirements of the cloud system include fine-grained access control, collusion resistance as well as backward secrecy [5].

Various procedures and methods for safeguarding secure socket method are used for encoding the data. The message authentication code (MAC) is provided to verify the integrity of the data. The cloud data are protected in an encrypted manner while transmission. The procedure includes classification index building, encryption and MAC steps. Strong and secure encryption techniques are required for securing the data and for controlling the data access authorization methods are used. The system model has two phases. The first phase transfers the data and stores it in the cloud. The second phase is used for accessing the data from the cloud. Storage of data process involves classification, index building and encryption and MAC scheme. The retrieval phase includes data access requests, integrity process, and digital signatures [6].

A public key encryption technique has been proposed using encrypting and decrypting methods for the data files in the cloud. A ranked keyword examines technique has been adopted in the cipher text to access the original data files. The data storage technique in cloud system comprises of cloud data owner, service provider and authorized users. The privacy preserving approach contains three phases which include setup, retrieval and integrity verification phase [7].

The auditing framework and an auditing protocol have been designed for privacy preservation in cloud data storage systems. The protocol provides various data dynamic operations and batch auditing process in the multi cloud environment. The auditing system has three entities. Data owner, cloud storage server and third party auditor. The auditing protocol involves five algorithms. They are key generation, tag generation, challenge, prove and verification algorithms. The data storage auditor uses two techniques, namely data fragment method and homomorphic verifiable methods. The privacy preserving auditing protocol has three phases which include owner initialization, auditing using challenge algorithm and also sampling auditing phase [8].

TPA has been introduced for integrity verification in order to achieve dynamic data operations, which include data insertion, deletion, and modification in the cloud. The aggregate signature technique has been designed for handling various auditing tasks in the cloud. The public auditing method supports batch auditing processes for multiple task execution at the same time in a cloud environment. The network architecture involves a client, TPA and cloud server system [9].

The cloud data services include data owner, users and cloud service providers. CSP includes data services, namely search, computation, storage, sharing and access. The security functionality has attribute authority, third party auditor for securing data services in the cloud. The security requirements involve data confidentiality, data access controllability, integrity and privacy preservability. The security threats in the cloud data services can be recognized as malicious attackers, curious CSP, vulnerable CSP and curious TPA [10].

An auditing protocol called as Sec Cloud was used for secure storage and computation in the cloud environment. The data security, storage and computation security are well defined using batch verification process. The cost of the computation is reduced in the Sec Cloud by choosing the perfect sampling size. Sec HDFS is used for test bed implementation of given protocol [11].

The public auditability uses TPA to verify the integrity for securing the cloud data storage. An auditing protocol supports security for storage in a cloud computing environment. The auditor checks the data without any of the knowledge about its content. The privacy preservation scheme means the TPA cannot view the contents of the user's data while the auditing process. The batch auditing process is allowed for simultaneous auditing of the tasks from multiple users together [12].

The hybrid and gravitational based search algorithm achieves better output for service composition in for achieving low cost in the field of cloud computing. The imperialist search algorithm based on hybridization has been used for providing composite complex services. A gravitational attraction force search algorithm uses local search option for service composition problem in the cloud [13].

III. System Model

The overall system architecture of the cloud environment in the proposed work comprises of four phases. Fig. 1 indicates the major entities involved in the cloud environment.

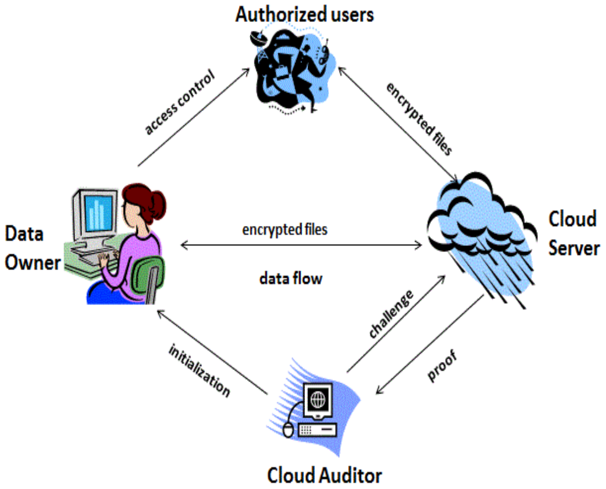

Fig.1. The System Architecture

A. *Major Entities*

The major entities included in the system architecture are given as follows.

a. Data Owner (DO)
b. Authorized Users (AU)
c. Cloud Service Provider (CSP)
d. Cloud Auditor (CA)

a. Data Owner (DO): The data owner stores the data into the cloud. Later on, these data files are verified for integrity by the cloud auditor. The data owner gives authorization for the cloud users to download the files from the cloud server. The owner has the ability to communicate with the cloud servers to access the data as well as modify or update the stored data using CSP. An owner also provides the data services along with the users from the cloud server.
b. Cloud User (CU): The cloud user accesses the cloud specific data and performs certain computations on it. Users can use the shared data and services from the server which are specifically stored in the cloud. The data consumer can use the data which is shared by the owner and which are encrypted for confidentiality and integrity. The cloud users can use computers, tablet and mobile phones that need to store their files on the cloud server. The users depend on cloud servers for the storage and maintenance of data. The users can perform dynamic operations related to cloud data with the help of a cloud server.
c. Cloud Service Provider (CSP): The CSP gives the service to the users by allowing using the storage space on the servers and the computations within the cloud limit. CS is responsible for storing the owner's data and allows the owner to insert, modify and delete the cloud data. CS holds enormous storage space for holding owners' confidentiality data files. The CSP handles various data storage services holding multiple computation resources. Every cloud server is maintained by CSP for dedicated cloud service using storage space and computations.
d. Cloud Auditor (CA): The cloud auditor is the trusted party who provides the auditing results to both cloud owner and the server. The privacy, securing auditing protocol comprises of four algorithms for security functionality of users' data. KeyGen, SigGen, GenProof and Verify proof. The key gen algorithm is given by the user during the setup phase. Signature generation is verified by user for specifying the metadata verification. Proof generation is performed by cloud server for storage correctness. Verification proof is generated by TPA during the auditing process.

B. *Main Phases*

The public auditing scheme comprises of two phases which include setup or owner initialization phase and audit phase.

a. Owner initialization phase: The key setup phase includes the algorithm for key generation in order to create a secret key and secret public tag keys. In the setup phase, the user verifies public as well as secret key parameters using KeyGen and SigGen algorithm. During the audit phase, TPA sends the challenge message to the server for file verification. The cloud server sends the response message using the GenProof algorithm which is confirmed by TPA using Verify Proof algorithm.

b. Audit phase: The auditing system protocol performs the challenge and proof algorithms who audits the data files stored on the server. TPA handles public auditing service for cloud users, which comprises of auditing protocol requirements. The public auditability process includes verification of the data which is done by cloud auditor.

IV. Methodology

Privacy is one of the biggest challenging issues in cloud computing. Privacy preserving of data means the confidential information should not be leaked to the TPA during the auditing process. The cloud service provider uses encryption technology for security over the cloud data. Privacy requires encrypting and decrypting the data files while at rest or while transmitted over the cloud. Strong authentication techniques and secure algorithms will help the confidential data to be secured within the cloud premises. The privacy preserving schemes include access control, encryption strategy, key management, policy, proxy, security, signature and central authority [14].

A. Group Search Optimization Scheme (GSO)

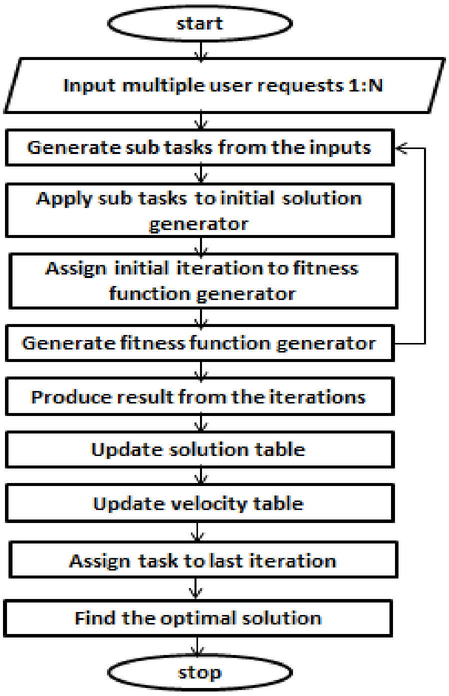
start
Input multiple user requests 1:N
Generate sub tasks from the inputs
Apply sub tasks to initial solution generator
Assign initial iteration to fitness function generator
Generate fitness function generator
Produce result from the iterations
Update solution table
Update velocity table
Assign task to last iteration
Find the optimal solution
stop

Fig.2. GSO process

A group search-based optimization method allows the load balancers to perform multitasking at the same time. The figure depicts the group search based optimization algorithm process through data flow diagram manner. The Meta heuristic algorithms like genetic algorithm and particle swarm using an optimization algorithm are applied for mining association rules in data. This method finds the interval of numeric using attributes for an association for the given intervals [15].

Fig. 2 depicts the overall process flow diagram for group search optimization scheme in cloud computing.

B. Group Search Optimization Algorithm

Algorithm for group search optimization scheme is given below.

Algorithm: Group Search Optimization

```
[Step 1:] Start
[Step 2:] Input multiple user requests for into the cloud
[Step 3:] Initial solution generator produces different sub-tasks from given requests
[Step 4:] Assign the initial iteration from sub-task generated to fitness function generator
[Step 5:] Generate result from previous iterations generated
[Step 6:] Update solution and velocity tables based on fitness value generated
[Step 7:] Combine the previous solution and generate the best solution for the given problem
[Step 8:] Assign the task to the last iteration generated with best results
[Step 9:] Find the optimal solution with less cost and execution time
[Step10:] End
```

C. The Fitness function value

The fitness value for the fitness function can be found using support and confidence methods. Fitness equation can be defined in four stages.

$$support(X \to Y) = \frac{\sigma(X \cup Y)}{N} \quad (1)$$

The first step supports the statistical significance of association rule. The second method is the confidence stage. The third stage comprises of a number of attributes in the record as NA. And the last stage is the amplitude of the intervals.

$$confidence(X \to Y) = \frac{\sigma(X \cup Y)}{\sigma(X)} \quad (2)$$

$\alpha 1, \alpha 2, \alpha 3, \alpha 4, \alpha 5$ are the user specified parameters required to adjust the parts of fitness function using parameter set. Selected is used for the attributes of a record initiated using amplitude factor. In the fitness function, the set of rules has certain attributes which are to be set at the given intervals. The fitness function determines the rule for choosing the amplitude of the intervals.

$$fitness = \alpha 1 * support + \alpha 2 * confidence - \alpha 3 * (NA - N(*)) - \alpha 4 * Int - \alpha 5 * Selected \quad (3)$$

Int part in fitness function in selected equation represents the numeric attributes using rule antecedent or consequent values [16-18].

$$Int = \frac{UB_m - LB_m}{amp_m} \quad (4)$$

D. Procedure: Fitness Function Generation

Fig. 3 represents the flow diagram representing the fitness function generation scheme in cloud computing environment.

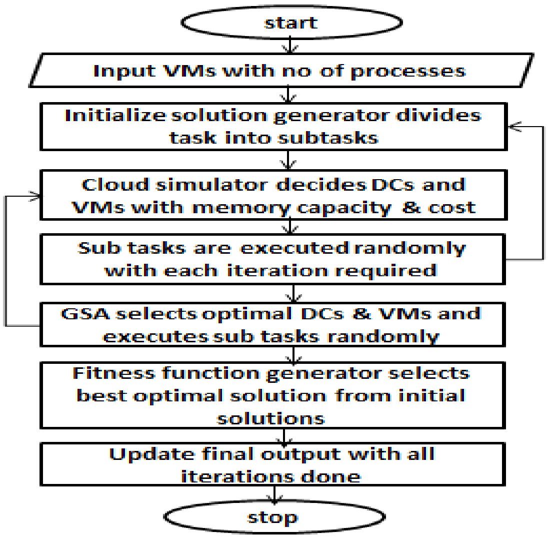
start
Input VMs with no of processes
Initialize solution generator divides task into subtasks
Cloud simulator decides DCs and VMs with memory capacity & cost
Sub tasks are executed randomly with each iteration required
GSA selects optimal DCs & VMs and executes sub tasks randomly
Fitness function generator selects best optimal solution from initial solutions
Update final output with all iterations done
stop

Fig.3. Fitness Function Generation

E. Fitness Function Algorithm

Procedure to create fitness function value is given in terms of algorithm below.

Algorithm: Fitness Function Generation

```
[Step 1:] Start
[Step 2:] Select Virtual machines with a number of processes assigned
[Step 3:] Initialization solution generator subdivides each task into various sub tasks required
[Step 4:] The cloud simulator decides final Data centers and Virtual machines with required capacity, memory and cost variations
[Step 5:] The sub tasks are executed randomly for every iteration required with specific memory locations
[Step 6:] GSO chooses optimal Data centers, Virtual machines and executes sub-tasks for every task in random order
[Step 7:] Fitness Function Generator: FFG selects the best optimal solution from the initial solutions generated
[Step 8:] Update final output once all the iterations is completed
[Step 9:] End
```

V. Result

The proposed scheme has been analyzed for the security requirements. The cloud security has been focused for privacy preserving of confidential data files in the cloud environment. The security of the proposed scheme works better than the existing algorithms like gravitational search scheme. The result analysis shows that the proposed work performs faster than other approaches.

```
0.09425854602967897  ld
sucess  0.09425854602967897 0.016666666666666666  0.11486486486486487
0.4457182637182438  float
0.4700894348894349  float
0.4562817342817368  float
0.4622522522522526  float
[0.13650149265812528, 0.0033333333333333333, 0.06894963144963145]  fmedfs
0
0.4662522522522526  dbdf
1.0 : 7.0 : 7.0 : 6.0 : 3.0 : 2.0 : asha
latha
ujwal
krishna
niharika
lakshmana
[asha, latha, ujwal, krishna, niharika, lakshmana]
2  d
1  position
7  e
[illegible]  d
[illegible]  n
Plaintext: asha latha ujwal
Ciphertext: [illegible]
7  e
[illegible]  d
[illegible]  n
7  position
5  e
[illegible]  d
[illegible]  n
Plaintext: krishna niharika lakshmana
Ciphertext: [illegible]
5  e
[illegible]  d
[illegible]  n
```

Fig.4. GSO scheme partition

Fig. 4 shows the file partition system. The key optimization process is given in the figure. Plain text has been converted into encrypted text for cryptographic issues. GSO scheme selects the best optimization key from various cryptographic keys generation while uploading a new data file into the cloud environment.

```
4488847350788211354542630918721329392022171177973064563304323672061440062493
```

Fig.5. GSO file format

Fig. 5 depicts the encrypted form of the data file in the cloud environment for confidentiality. Cloud security and confidentiality are shown in the form of cipher text in the above figure.

VI. Conclusion

The sensitive data should be protected from cloud providers without compromising the data. The cryptographic technique helps in protecting the cloud data storage. The encryption and decryption of data files within the cloud play an active role in the practice of cloud access.

References

[1] Latif, Rabia, et al. "Cloud computing risk assessment: a systematic literature review." *Future Information Technology*. Springer Berlin Heidelberg, 2014. pp. 285-295

[2] Djenna, Amir, and Mohamed Batouche. "Security problems in cloud infrastructure." *Networks, Computers*

and Communications, The 2014 International Symposium on. IEEE, 2014

[3] Rasheed, Hassan. "Data and infrastructure security auditing in cloud computing environments." *International Journal of Information Management* 34.3 (2014): 364-368

[4] Wenge, Olga, et al. "Data Privacy in Cloud Computing–An Empirical Study in the Financial Industry." (2014)

[5] Dong, Xin, et al. "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing." *Computers & security* 42 (2014): 151-164

[6] Sood, Sandeep K. "A combined approach to ensure data security in cloud computing." *Journal of Network and Computer Applications* 35.6 (2012): 1831-1838

[7] Pasupuleti, Syam Kumar, Subramanian Ramalingam, and Rajkumar Buyya. "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing." *Journal of Network and Computer Applications* 64 (2016): 12-22

[8] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *IEEE transactions on parallel and distributed systems* 24.9 (2013): 1717-1726

[9] Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." *IEEE transactions on parallel and distributed systems* 22.5 (2011): 847-859

[10] Tang, Jun, et al. "Ensuring security and privacy preservation for cloud data services." *ACM Computing Surveys (CSUR)* 49.1 (2016): 13

[11] Wei, Lifei, et al. "Security and privacy for storage and computation in cloud computing." *Information Sciences* 258 (2014): 371-386

[12] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." *IEEE transactions on computers* 62.2 (2013): 362-375

[13] Jula, Amin, Zalinda Othman, and Elankovan Sundararajan. "A hybrid imperialist competitive-gravitational attraction search algorithm to optimize cloud service composition." *Memetic Computing (MC), 2013 IEEE Workshop on*. IEEE, 2013

[14] Arjun, U., and S. Vinay. "A short review on data security and privacy issues in cloud computing." *Current Trends in Advanced Computing (ICCTAC), IEEE International Conference on*. IEEE, 2016

[15] Agbehadji, Israel Edem, Simon Fong, and Richard Millham. "Wolf search algorithm for numeric association rule mining." *Cloud Computing and Big Data Analysis (ICCCBDA), 2016 IEEE International Conference on*. IEEE, 2016

[16] Kalra, Mala, and Sarbjeet Singh. "A review of metaheuristic scheduling techniques in cloud computing." *Egyptian informatics journal* 16.3 (2015): 275-295

[17] Amanpreet Kaur, Bikrampal Kaur, Dheerendra Singh,"Optimization Techniques for Resource Provisioning and Load Balancing in Cloud Environment: A Review", International Journal of Information Engineering and Electronic Business (IJIEEB), Vol.9, No.1, pp.28-35, 2017. DOI: 10.5815/ijieeb.2017.01.04

[18] Jitendra Singh,"Study of Response Time in Cloud Computing", IJIEEB, vol.6, no.5, pp.36-43, 2014. DOI: 10.5815/ijieeb.2014.05.06

Authors' Profiles

Dr. Jayashree Agarkhed is currently working as Professor in the department of Computer Science and Engineering at Poojya Doddappa Appa College of Engineering, Kalaburagi. She has completed her Ph.D from Visvesvaraya Technological University in the year 2013. She is currently guiding Ph.D students in the field of Computer Networking and Engineering. She has published more than 90 research papers in Springer Book chapters, refereed International journals and Conferences and also in more than 50 IEEE conference proceedings. She has presented papers in various International conferences in and around India. She is the reviewer for various National and International journals and Conferences as well. Her areas of interests include Wireless sensor network, Multimedia Communication, Artificial Intelligence, Cloud computing, grid computing and data mining.

Ashalatha Ramegowda is pursuing Ph.D in the field of Computer Science and Engineering at Poojya Doddappa Appa College of Engineering, Kalaburagi. She has completed Bachelor of Engineering in Information Science and Engineering and Master of Technology from Computer Science and Engineering from Visvesvaraya Technological University, Belagavi. She has published papers in International journals and Conferences. She is the student member of IEEE and IEI. Her areas of interests include Computer networks and Cloud computing.

How to cite this paper: Jayashree Agarkhed, Ashalatha R.,"Security and Privacy for Data Storage Service Scheme in Cloud Computing", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.9, No.4, pp.7-12, 2017. DOI: 10.5815/ijieeb.2017.04.02