STRENGTHENING USER'S CONTROL OF DATA IN THE CLOUD SERVICE - AUDITING and LOGGING MECHANISM

A. Anuba Merlyn[1] , Asst.Prof. V. Veera Ragavan[2], Dr. K. Selva Kumar[3].

Abstract -**To strengthen user's control of data in the cloud service , a novel approach, namely cloud information accountability (CIA) framework is proposed which secure data during transmission and storage. Experimental results are reported to demonstrate the efficiency and effectiveness of the proposed approach.**

Index Terms - **accountability, cloud computing, data sharing**

I. INTRODUCTION

In cloud computing, to allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service- level agreements made at the time they sign on for services in the cloud.

Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments. To overcome the above problems, we propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability[28]. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information account- ability focuses on keeping the data usage transparent and track able.

Our proposed CIA framework provides end-to- end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful account- ability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach where by the user (or another authorized party) can

Mrs. A. Anuba Merlyn B. Sc, M.C.A.[1], *Research Scholor, School of Computing Sciences, Vels University, Chennai, India.*

Mr. V. Veera Ragavan M.C.A., M.Phil, PGDBI[2], *Assistant Professor, Department of M.C.A. Vels University, Chennai, India.*

Dr. K. Selva Kumar M.E. Ph.D.[3], *Assistant Professor, Department of Mathematics, University VOC College of Engineering, Anna University (Thoothukudi Campus), Thoothukudi, India.*

ISSN: 2278 – 1323

retrieve the logs as needed. The design of the CIA framework presents substantial challenges, including uniquely identifying CSPs, ensuring the reliability of the log, adapting to a highly decentralized infrastructure, etc. Our basic approach toward addressing these issues is to leverage and extend the programmable capability of JAR (Java ARchives) files to automatically log the usage of the users' data by any entity in the cloud. Users will send their data along with any policies such as access control policies and logging policies that they want to enforce, enclosed in JAR files, to cloud service providers. Any access to the data will trigger an automated and authenticated logging mechanism local to the JARs.

We refer to this type of enforcement as "strong binding" since the policies and the logging mechanism travel with the data. This strong binding exists even when copies of the JARs are created; thus, the user will have control over his data at any location. Such decentralized logging mechanism meets the dynamic nature of the cloud but also imposes challenges on ensuring the integrity of the logging. To cope with this issue, we provide the JARs with a central point of contact which forms a link between them and the user. It records the error correction information sent by the JARs, which allows it to monitor the loss of any logs from any of the JARs. Moreover, if a JAR is not able to contact its central point, any access to its enclosed data will be denied. Currently, we focus on image files since images represent a very common content type for end users and organizations (as is proven by the popularity of Flickr [8]) and are increasingly hosted in the cloud as part of the storage services offered by the utility computing paradigm featured by cloud computing. Further, images often reveal social and personal habits of users, or are used for archiving important files from organizations. In addition, our approach can handle personal identifiable information provided they are stored as image files (they contain an image of any textual content, for example, the SSN stored as a .jpg file). We tested our CIA framework in a cloud testbed, the Emulab testbed [18], with Eucalyptus as middleware . Our experiments demonstrate the efficiency, scalability and granularity of our approach. In addition, we also provide a detailed security analysis and discuss the reliability and strength of our architecture in the face of various nontrivial attacks, launched by malicious users or due to compromised Java Running Environment (JRE).

In [1], they provide a CIA framework for avoiding the loss of data during the data sharing on the cloud. The CIA framework conducts automated logging and distributed auditing of appropriate access performed by any entity, carried out at any point of time at any cloud service provider using programmable capabilities of JAR. Using this mechanism, Data owner can audit his content on cloud, and he can get the confirmation that his data is safe on the cloud. Data owner also able to know the duplication of data made without his knowledge. Data owner should not worry about his data on cloud using this mechanism and data usage is transparent, using this mechanism. [2], presents a framework CIA for accountability and auditing which is used to protect user's data and also monitor the actual usage of data in the cloud. In particular, a logging mechanism is provided for the user's data with access policies, and ensures that any access to their data will trigger authentication, by this mechanism data owner may know his/her data is handled as per his access policies. By means of the CIA, data owners can track

ISSN: 2278 – 1323

not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. The distributed auditing mechanism is followed and information about the user is collected simultaneously in-order to monitor the usage of data.

In [3], the data owner fully focused the users data. An object-centered approach is proposed so that it facilitates by including our logging method together with users' data and strategy. To make sure that any admission to users' data will trigger validation and automatic logging local to the java archives and we persuade the java archive programmable abilities to both create a dynamic and traveling object. In [7], they provide effective mechanism to using accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, they proposed an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. Accountability is checking of authorization policies and it is important for transparent data access. They provide automatic logging mechanisms using JAR programming which improves security and privacy of data in cloud. To strengthen user's control, they also provide distributed auditing mechanisms. They provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

In [10], they provide a secure sharing of data. They proposed an Object-Centered approach that performs logging and auditing. To ensure the authentication and automated logging mechanism, they use JAR programmable capabilities. For this mechanism, data owner knows all the actions about the data. In [11], the author uses the Software as a Service (SaaS) model of cloud computing. In this paper, they discussed about different types of threats and solutions for preventing from the different threats. In [12], they provide accountability and authentication for securing data. In this the data owner secures not only the original data and audits even those copies of its data that were made without his knowledge. They designed and implemented *FADE*, a secure overlay cloud storage system that achieves fine-grained, policy based access control and file assured deletion. In [13], author classified cloud security based on the three service models of cloud computing SaaS, PaaS and IaaS. Attributes for each type of security. They compared securities provided in different services by world's best known cloud service providing companies such as Amazon AWS, Google App Engine, Windows Azure etc. considering cloud security category.

In [14], they provide the research towards an Event Gathering Mechanism which is envisioned to allow the modeling of legal aspects in a multi layered cloud environment. An event based evidence gathering mechanism is proposed to provide compliance with legal aspects regarding data protect as well as SLA regulations. This work will eventually help to set a security standard for audit-able logging information and therefore increase overall security and accountability of the cloud environment as well as enabling CI providers to outsource data handling into the Cloud. This paper presents to overcome the security issues they provide automated – decentralized mechanism to capture and monitor the every usage of the users from various location. In [15], they proposed a logging mechanism to keep track of the actual usage of the system. They leverage the jar file mechanism to ensure any data access will trigger authentication and automated logging mechanism. To consolidate user's control, they

ISSN: 2278 – 1323

provide distributed auditing mechanisms, we also provide comprehensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches. In [16], they proposed CIA frame work for secure data sharing between Data owner and multi users. To make sure that any admission to users' data will trigger validation and automatic logging local to the java archives and they persuade the java archive programmable abilities to create a dynamic object. An object-centered approach is proposed so that it facilitates by including our logging method together with users' data and strategy.

In [17], a secured cloud storage system that achieves policy-based access control and file assured deletion is proposed with an information accountability cloud framework to keep track of the actual usage of the clients' data. Automated logging and distributed auditing of relevant access performed by any entity is handled. The access policy generated for the file controls the file accesses and policy revocation makes the file permanently inaccessible. The system is built upon a set of cryptographic key operations that are self-maintained by a set of key managers and adds security features. A logging mechanism records the access information and auditing mechanism provides this information to the owner. The files and log records are kept as encrypted in the cloud storage system for avoiding various attacks. File assured deletion can be done by policy revocation, which removes the control key of the file from the database and hence the decryption of file is impossible. The functions of various cryptographic keys and operations are discussed along with key sharing. The performance evaluation reveals the constraints. In [19], they proposed decentralized Cloud Data Logging (CDL) framework for losing control of user's own data stored in remote servers is proposed. By the proposed framework the information owner styles the policy and hides the information in a compressed format to supply authentication access to the data. To strengthen user's management, they additionally proposed a distributed logging mechanism that is triggered once accessing the user's information. They have proposed a logic that enable audited agent to prove their actions and to possess explicit information by implementing auditing mechanism.

In [20], they proposed CIA frame work for secure data sharing. Here it uses Java Archives(JAR) files for automatically log the usage of user's data. To support user's control, it can provide distributed auditing mechanism. So data also encrypted in this scheme Hierarchical identity based encryption (HIBE). In this method various significant security services including compression, encryption and authentication also. To avoid the data loss they[21] provide decentralized information accountability framework for keep the records about the users and object oriented approach for authentication and logging mechanism. For logging mechanism, JAR file is used. Their approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of their work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

In [23], they proposed an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. To strengthen user's control, they also provide distributed auditing mechanisms. Users will send their data along with any policies such as access control policies and logging policies that they want to

ISSN: 2278 – 1323

enforce, enclosed in JAR files, to cloud service providers. Any access to the data will trigger an automated and authenticated logging mechanism local to the JARs. Their system is highly distributed where storage servers independently encode and forward messages and key servers independently perform partial decryption. They analyze suitable parameter for more flexible adjustment between the number of storage servers and robustness. They provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches. In [25], they provide accountability and authentication for securing data. From that, the data owner knows the details, where they are actually stored. The details are stored in JAR files. A JAR file includes user's data and their policies such as access control policies and logging policies. In [26], This paper provides a concise all around analysis of the challenges faced by cloud computing community and also presents the solutions available to those challenges.

In [27], they provide data sharing and distribution on cloud based strategy by using JAR file.In [29], they provide automatic logging mechanism using JAR for protecting the data of the owner. For that mechanism, data owner knows the details, if any modification occurs in his/her data. In future, they install JRE and JVM to do the authentication of JAR.

In [4], a fully functional identity based encryption service(IBE) Is proposed. The scheme has shown cipher text security in the random oracle model assuming and elliptic curve variant of the computational Diffe-Hellmen problem. In[5], a game based machine checked retention of the security of the Branch- Franklin (IBE) scheme to the Bilinear – Diffie-Hellman assumption is presented.

In [24], an attempt is made to strengthen users control of data in the cloud service using CIA. In this project, based on the works in [24], another attempt is made to strengthen users control of data in the cloud service using CIA. The data information received by the owner is secured by the JAR files. And, the owner can view the data information since the last trial.

In brief, the objective of this paper is to provide a secure CIA framework for data sharing in cloud computing environment.

II. CLOUD INFORMATION ACCOUNTABILITY

Our proposed CIA framework is given in the following figure 1. This work is different from traditional logging methods which use encryption to protect log files. This CIA framework prevents various attacks such as detecting illegal copies of user's data.

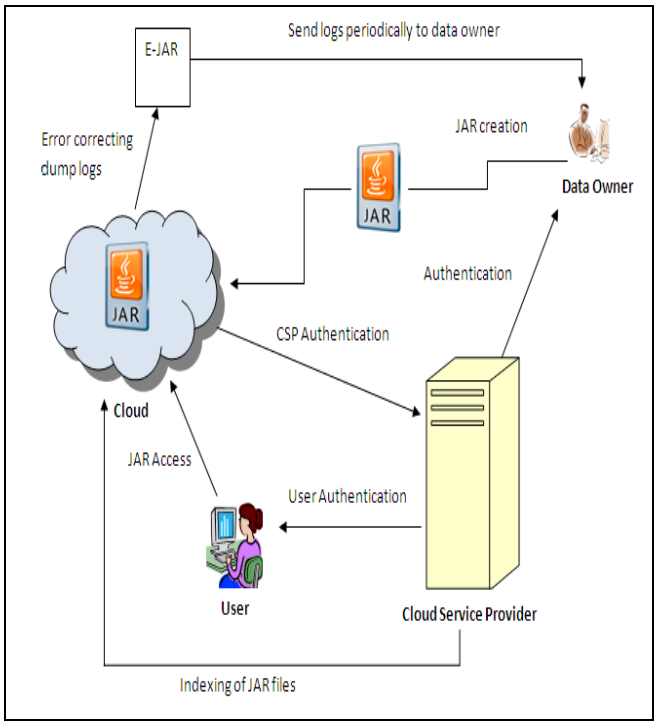

Fig1: Cloud Information Accountability framework

ISSN: 2278 – 1323

III. PERFORMANCE AND EXPERIMENTAL RESULTS

To demonstrate the efficiency and effectiveness of the proposed approaches, we examine the time taken to create a log file and measure the overhead in the system with respect to time and storage. The overhead with respect to time are during authentication, during encryption of a log record and during the merging of the log records. The overhead with respect to storage, only data to be stored are the actual file and the associated log files. In this paper, the size of the data are of different sizes and one data owner is implemented for experimental study by Smitha et. al.,[24].

A. Log Creation Time

We find out the time taken to create a log file when there are entities continuously accessing the data causing continuous logging. The results are given in figure 2

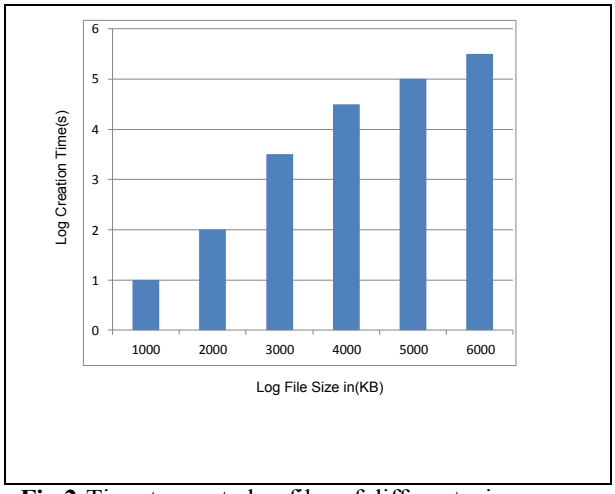

Fig 2: Time to create log files of different sizes

It is observed that, from figure 2, the time to create log files increases linearly with the size of the log files. In addition, it is observed that, the time taken to create log files decreases linearly with respect to the size of the newly uploaded files into the data of the four data owners after finding the log creation time for the initially stored data in the four data owners. In particular, the log time get increased when four owners are introduced, it is shown in Table 1.

Table 1: Log creation time

Work	Data Owners	File Size	Log creation time
Smitha et.al[24]	**1**	**100KB**	**114.Ms**
Present work	**1**	**140KB**	**180.Ms**

B. Authentication Time

We consider both the authentication time of the CSP and an end user. During the authentication of a CSP the overhead can occur. It is given in the Table2. It is observed that, the authentication time get reduced than in the works of Smitha et. al., [24], on using four data owners.

Table 2: Authentication tim

Work	Data Owners	Authentication Time CSP	USER
Smitha et.al[24]	**1**	**920ms**	**1.2seconds**
Present work	**1**	**920ms**	**1.0seconds**

C. Time taken to perform logging

In this experiment, we let multiple servers continuously access the same data JAR file for a minute and recorded the number of log records generated. Table 3, shows the time taken to perform logging of the present work is better than the works of Smitha et.al.,[24].

ISSN: 2278 – 1323

Table 3: Time taken to perform logging

Work	Data Owners	Average time log an action	Log encryption time per second
Smithaet .al[24]	1	10 seconds	300MS
Present work	1	10 seconds	180MS

D. Log Merging Time

In this experiment we measure the amount of time required to merge two log files. The two files will have common records with each other. We tested time to merge up to 100 log files of size each 10KB, 500KB, 800KB and 1MB.The result is in Figure 3.

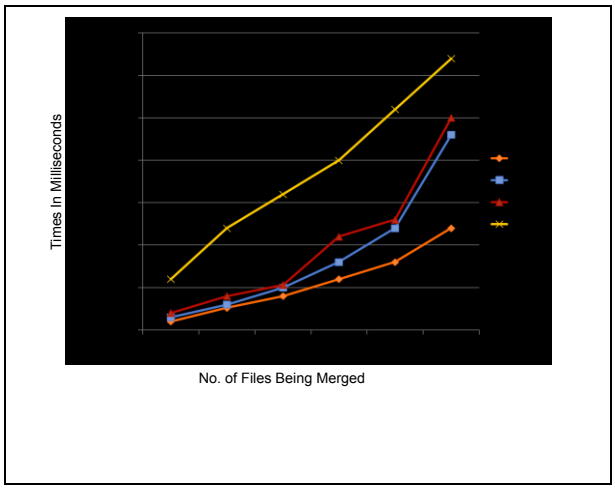

Fig 3: Time to merge log files

We observe that the log merging time increases linearly as the number of files increases with respect to the increase in size of files.

Table 4 shows time get increased due to increase in size of files.

Table 4: Log merging time

Work	Data Owners	File Size	Log merging time
Smitha et.al[24]	1	100KB	5.3MS
Present work	1	140KB	1.87MS

E. Size of the *Data JAR Files*

We measure the overhead results in storage, when a single logger handles more than one file. We measure the size of the logger(JAR) by varying the number of JARs and the size of the data inside the JAR. Figure 4, shows that the size of the logger(JAR) grows as the size of the original file increases in KB..

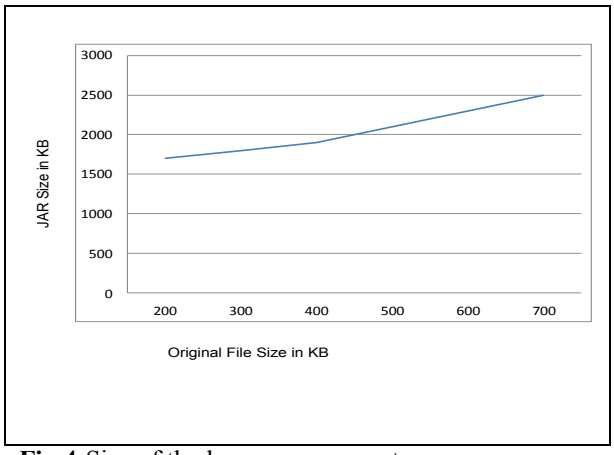

Fig 4: Size of the logger component

F. Overall time taken to complete the work

The total time taken to complete the entire work is lesser than that of work of Smitha et al.,[24] and it is shown in the Table 5.

ISSN: 2278 – 1323

Table 5: Time to complete the work

Work	Data Owners	Overall time taken to complete the work
Smitha et.a[24]	**1**	**6.5 minutes**
Present work	**1**	**6.48 minutes**

G. Log record received by Data owner in his/her e-mail in JAR file

adam,115.242.189.133,18.png,download,Sep 20, 2013 1:29:33 PM
115.242.204.117,view,Sep 20, 2013 10:02:27 AM
adam,101.63.229.38,6.jpg,download,Oct 13, 2013 10:14:03 AM
san,101.63.172.79,10.jpg,download,Sep 19, 2013 6:24:43 PM
115.242.204.117,view,Sep 20, 2013 10:01:28 AM
adam,115.242.186.53,10.jpg,download,Oct 12, 2013 7:58:56 AM
101.63.172.79,view,Sep 19, 2013 7:16:29 PM
tom,115.242.232.68,20.JPG,download,Oct 9, 2013 1:28:52 PM
san,192.168.1.34,10.jpg,download,Sep 17, 2013 7:21:47 PM

In general, on comparing all the experimental results, our approach is more efficient and effective.

IV. CONCLUSION AND FUTURE RESEARCH

With an auditing mechanism, we proposed innovative approaches for logging any access to the data in the cloud. In our approach, the data owner can audit his contents and enforce back-end protection whenever needed. The main features of our approach is that it enables the data owner to audit even those copies of his data that were made without his knowledge. Moreover, we provided more security to the system which strengthens user's control of data in the cloud.

Future plan is to refine our approach to verify the integrity of his JRE and authentication of JARs. We also plan to investigate practical encryption schemes that will allow encryption of log records in such a way that the logging cloud can execute necessary quires on the encrypted logs which is sufficient for privacy or confident ability.

ACKNOWLEDGEMENT

Dr.K.Selvakumar wish to acknowledge the financial support from Anna University, Chennai-600 025, India project for young faculty members under research support scheme.

REFERENCES

[1] H. Arun, R. Nilam, R.Namrata And S.Purva, 'Review On Techniques To Ensure Distributed Accountability For Data Sharing In The Cloud', *International Journal Of Advanced Research In Computer And Communication Engineering*, Vol. 2, Issue 10, October 2013.

[2] AmandeepkaurAndSatinderpal Singh, 'Design And Development Of Novel Distributed Information Monitoring Framework To Check Actual Information Usage Over Cloud', *International Journal Of Innovaive Research And Development*, Vol 2 Issue 8 August 2013

[3] BheemeshwarYerra, AmjanShaik And M.Sudhir Kumar, 'Liability As An Approach For Confidentiality Fortification In The Cloud', *International Journal Of Computer And Electronics Research*, Volume 2, Issue 4, August 2013.

[4] Boneh D and Franklin M.K, 'Identity-based encryption from the well pairing', *Proc. Int'l Cryptography Conf. Advances in Cryptography*, pp. 213-229, 2012

[5] Buneman P, Chapman A and Cheney J, 'Provenance management in crated databases., *Proc. ACM SIGMOD Int'l Conf. Management of Data(SIGMOD'06)*, PP. 539-550, 2006

[6] EmulabNetwok Emulation Testbed, *www.emulabnet*, 2012.

[7] EpuruMadhavarao, M Parimala and ChikkalaJayaRaju, 'Data Sharing in the Cloud Using Distributed Accountability', *International Journal of Advanced Research in Computer Engineering & Technology*, ISSN: 2278 – 1323 Volume 2, Issue 4, April 2013.

[8] Fliker, Http//www.fliker.com/. 2012.

[9] Jaeger P.T, Lin J and Grimes J.M, 'Cloud computing and information policy: computing in a policy cloud?'. *Information Technology and Policies*, Vol. 5, No. 3, pp. 269-283, 2009

ISSN: 2278 – 1323

[10] Mr.R. Karthik Ganesh And Ms. AranyaHari, 'Enhancing Privacy In Cloud By Avoiding Misuses Of Files', *International Journal Of Advanced Research In Computer Science And Software Engineering*, Volume 3, Issue 3, March 2013.

[11] Kranti Kumar Dewangan, Akashwanjari And Somesh Kumar Dewangan, 'A Valued Analysis Of Information Security, Threats And Solutions For Cloud Computing', *International Journal Of Advanced Research In Computer Science And Electronics Engineering*, ISSN: 2277 – 9043 Volume 2, Issue 9, September 2013.

[12] A.Krishna Mohan, Abdul Khalil AziziAndRayhana Ibrahim, 'Decentralized Information Accountability Framework For Cloud', *International Journal Of Research In Computer And Communication Technology*, Vol 2, Issue 8, August-2013.

[13] LipiAkter, Prof. Dr. S M MonzururRahman And Md. Hasan, 'Information Security In Cloud Computing', *International Journal Of Information Technology Convergence And Services*, Vol.3, No.4, August 2013.

[14] Markus Florian, Saritapaudel And Markus Tauber, 'Trustworthy Evidence Gathering Mechanism For Multilayer Cloud Compliance', *IEEE ICITST*, 2013.

[15] Muthulakshmi V, Ahamedyaseen A, Santhoshkumar D And Vivek M, 'Enabling Data Security For Collective Records In The Cloud', *International Journal Of Recent Technology And Engineering*, ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[16] B.Navaneetha, B.Madhavi Devi And Ch.Srinivasulu, 'Liability For Data Distribution In Cloud Computing', *International Journal Of Reviews On Recent Electronics And Computer Science*, Volume-1/Issue-6/1435-1440October 2013

[17] Nishana Rahim And K. Saravanan, 'Secured Image Sharing And Deletion In The Cloud Storage Using Access Policies', *International Journal On Computer Science And Engineering*, 2013.

[18] Pearson S and Charleswurth A, 'Accountability as a way forward for privacy protection in the cloud', *Proic. First Int'l Conf. Cloud Computing*., 2009.

[19] Prabha M And Hariharasitaraman S, 'Distributed Auditing Mechanism For Achieving Accountability With Secure Provenance In Cloud Data Storage', *Research Journal Of Computer Systems Engineering*, Vol 04; Special Issue; June 2013.

[20] Ms.R.Punitha, Mr.D.Vijaybabu, 'Data Storage Security In Cloud By Using Jar Files And Hierarchical Id-Based Cryptography', *International Journal Of Advanced Research In Computer Engineering & Technology*, Volume 2, Issue 1, January 2013.

[21] B. Rajani, K. NagasindhuAnd K. Saikrishna, 'Integrity Verification & Distributed Accountability In High Performance Distributed Clouds', *International Journal Of Electronics Communication And Computer Engineering,* Volume 4, Issue (6) NCRTCST-2013.

[22] Sang Y, Cunming R and Gansen Z,'Strengthen cloud computing security with management using hierarchical security-based cryptography', *CloudCom, LNCS*, 5931, PP.167-177, 2009.

[23] J.Shyamala, D.Femila And B.VinishaCathrineAntonus, 'Automated Auditing And Logging Mechanism For Secure Data Storage In Cloud Using Proxy Re-Encryption', *International Journal Of Advanced Research In Computer Engineering & Technology*, Volume 2, Issue 3, March 2013.

[24] Smitha S, Anna C.S and Dan L,'Ensuring distributed accountability for data in the cloud', *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 4, pp. 556-568, 2012.

[25] P Sobha Rani, V.SangeetaAndP.Sureshbabu, 'Achieving Information Accountability In Cloud Computing Environment', *International Journal Of Computer And Electronics Research*, Volume 2, Issue 2, April 2013.

[26] Sultan Ullah, Zhengxuefeng, Zhou Feng And Zhao Haichun, ' Tcloud: Challenges And Best Practices For Cloud Computing',2013

[27] TajMahammad Khan And K.Rakesh, 'Sharing Of Data By Accountability Distribution On Cloud Based Strategy', *International Journal Of Professional Engineering Studies*, Volume 1 Issue 1 Dec 2013.

[28] Weitzncr D.J, Abelson H, Berners-Lee T, Feigen-baum J, Hemdeler J and Sussman G.J, 'Information Accountability', *Comm. ACM*, Vol. 51, No. 6, pp.82-87, 2008.

[29] Yathi Raja Kumar Gottapu And A. Raja Gopal, 'Optimal Storage Services In Cloud Computing Ensuring Security', *International Journal Of Advanced Research In It And Engineering* ISSN: 2278-6244, 2013.

Mrs.A.Anuba Merlyn received the M.C.A. degree from the Anna University, Tamil Nadu, India, in 2012 and is currently pursuing the M.Phil degree in Computer Science at Vels University, Tamil Nadu, India. Her research interests covers cloud computing and networking.

Mr.V.Veera Ragavan received his M.C.A. degree from Bharathidasan University, India, M.Phil fom Periyar University, India. He is working as an Assistant Professor in Vels University, Tamil Nadu, India. His research interests covers compiler construction techniques, visual programming and web designing.

Dr.K.Selvakumar received his M.E. Computer Science and Engineering from Anna University, India, Ph.D.and PostDoctorate from Bharathidasan University, India in 1993 and 1994 respectively. He is an aassistant professor at University VOC College of Engineering, Anna University (Tutucorin Campus). His research interests covers cloud computing, networking, image processing, numerical analysis, singular perturbation problems in control system and stiff.Computations. He is doing research for the last 27 years and publishing research papers regularly.

ISSN: 2278 – 1323