Design and Implementation of Audit Cloud for Consistency in Cloud Computing

D. Veerabhadraiah[1], M. Revathi[2]

[1]M.Tech Student, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering and Technology, Chittoor (D), Andhra Pradesh, India.

[2]Assistant Professor, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering and Technology, Chittoor (D), Andhra Pradesh, India.

Abstract: ***Cloud computing is a new computing paradigm that has been making strides to establish and serve the computing world in its own way. In fact cloud computing is the technology that enables individuals and organizations to gain access to huge amount of computing resource in pay per use fashion. It is complemented by virtualization technology in order to make the offerings affordable. Cloud is able to provide various services that are categorized into Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Cloud provides plethora of advantages that can avoid capital investment besides gaining access to services without geographical and time restrictions at affordable prices. It also provides many business opportunities and services. However, there is consistency problem in cloud due to replicas maintained in many servers. This is a challenging problem to be addressed. Based on the existing solution provided by Liu et al., in this paper we design and implement a consistency mechanism with algorithms for cloud data integrity and consistency. The proposed system takes care of various violations of data integrity with corrective measures. We also proposed a mechanism that takes care of consistency of data and overcome drawbacks of the previous approaches. We built a prototype application that demonstrates the proof of concept. The empirical results are encouraging.***

Keywords: Cloud computing, consistency, integrity, security.

1. Introduction

Cloud computing is a new model of computing that is based on Internet. This technology enables public in general to gain access to a shred pool of resources. The pool of resources is maintained by cloud service provider (CSP). There are many cloud service providers such as Microsoft, Amazon, IBM, Apple, and Google and so on. Cloud provides many services including important services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). The first service allows people to obtain software as a service instead of purchasing it in pay per use fashion. In the same fashion the second service provides infrastructure such as storage and servers while he third service provides platform as a service for building various cloud applications.

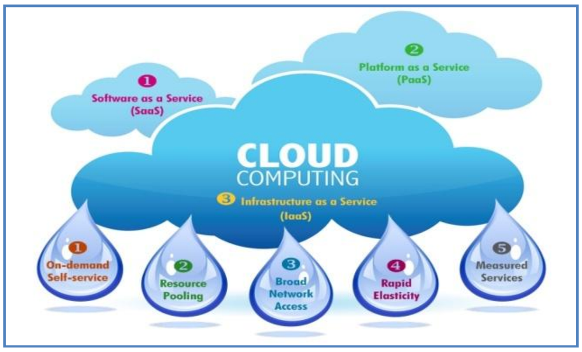


Figure 1: Cloud computing services and features

As shown in Figure 1, the cloud service stalk has 3 specific services described already. There are many features such as on-demand self-service, resource pooling, broad network access, rapid elasticity and measured services. These features help the cloud users to avail services in pay per use fashion and the availability of service and scalability are high. The computing resources provided by cloud service providers like IBM, Microsoft, Google, Amazon etc. are made accessible to public through any Internet-aware device and applications such as enterprise applications, desktop applications, and browser based applications and mobile applications (Torry Harris). Cloud computing is of many types namely private cloud, public cloud, community cloud and hybrid cloud. Private cloud is limited to an organization and only the users of it can access it. Public cloud on the other hand can be accessed by anyone in the world in pay per use fashion. Community cloud is the cloud managed by some sort of similar organizations. The hybrid cloud is the combination of one or more cloud deployments.

Our contributions in this paper include a mechanism for security and data integrity in cloud computing. We also proposed an algorithm for ensuring consistency of data which will be crucial in multi-user environment. The remainder of the paper is structured as follows. Section 2 reviews relevant literature. Section 3 presents the proposed system. Section 4 provides details of experiments and results while section 5 concludes the paper besides providing recommendations for future work.

2. Related Works

This section reviews literature on data integrity and security issues in cloud computing. It throws light into security issues in IaaS, PaaS and SaaS.

2.1Security Challenges in IaaS

Infrastructure does mean many things. That encompasses hardware and software infrastructure. Storage facilities also come under this layer. Thus it assume much importance in cloud computing. Cloud users feel that the cloud storage is un-trusted. The security factors include data integrity, service availability and data intrusion. Data integrity is lost when data is access illegally or modified. This could be done by external threats or internal threats. Data intrusion refers to hacking of data such as passwords, sensitive data etc. Service availability refers to the round the clock service expected by the cloud users with time and geographical restrictions. Information privacy is one of the security challenges pertaining to IaaS. From the literature it is found that many solutions came into existence for cloud storage security and service availability. However there is much room for further research in the area of data intrusion (M.Ignacio *et al*., 2007 [1]). There are many technical and security challenges in service stack of cloud with respect to IaaS. The important areas of security concern include digital forensics, new attack strategies, resource sharing and operational trust modes. Trust level is the primary concern in IaaS. Different cloud service providers are providing different trust levels that are to be used to analyze the risks involved as well. Since the cloud service provider has access to public data, it is essential to protect data. Towards it encrypted communication channels, computations support on the encrypted data, and security of cloud computing resources are to be given paramount importance. There are certain legal issues involved in the security challenges of IaaS. They include jurisdiction issues, cloud stakeholder rights, and technical issues pertaining to safeguarding interests of cloud users (Dillon *et al*., 2014[3]). IaaS and SaaS services can be combined effectively for many domains. For instance, in education, these two together can be used for e-Learning services. However, security needs to be part of the framework of e-Learning application that takes care of secure communications. Single sign-on (SSO) can be enforced to support secure services with single authentication process. There is inherent security risk involved when VMs are used in cloud computing service stack. As VMs allows programs to be executed and they might carry malicious code, there is hidden security threat with VM usage. User access policies play an important role in securing communications in the layers of cloud. Security components are to be deployed in such e-Learning applications since the IaaS and SaaS cloud layers are vulnerable to attacks (Doelitzscher *et al*., 2011[4]). Virtualization manager plays an important role in IaaS layer. However, it might throw security challenges if that is compromised. Once it is compromised, it causes all security problems in the entire infrastructure being used by cloud. This is because the cloud infrastructure is built on top of virtualization technology and that is under control of virtualization manager (Subashini and Kavitha, 2011[6]).

2.2Security Challenges of Software as a Service

Cloud service architectures have been providing service architectures that are providing more security features. For instance, SaaS layer of cloud takes care of malware detection through scanning and filtering of content through cloud-based proxies. Some of the commercial cloud services are also offering enterprise level security configuration facilities that can prevent many security attacks including SQL injection. Third party management is the main concern in cloud security. Other security concern is the technical issues such as non-availability of encrypted communications. Other security issues are related to the architectural concerns where cloud depends on Internet and that dependence can have inherent security threats since Internet is untrusted network (Dorey and Leite, 2011[5]). Cloud security challenges can be related to trust and assurance, data security and identity and access management. The risk of cloud service provider gaining access to sensitive information of client always exists. Cloud service providers can have access to software being deployed in cloud so as to provide software services in pay per use fashion. The float corporate architectures and possibility of social engineering are the other possible security issues in cloud computing (Dorey and Leite, 2011[5]).

2.3Security Challenges of Platform as a Service

Platform as a Service provides application development environment that can be used by cloud application developers across the globe. There are five common challenges that need to be addressed to improve adaption of cloud computing service stack. They include service life cycle optimization, market and legislative issues, multi-cloud architectures, adaptive self-preservation, and dependable sociability (Chen,Z *et al*., 2010[2]). (Subashini and Kavitha [6] (2011)) studied security issues in PaaS. As this service helps applications developers across the globe to built cloud applications, they are given freedom to customize features that leads to security problems. The usage of web services and the underlying vulnerabilities are threat to the PaaS layer of the cloud service stack. Cloud Security Alliance (2013) investigated and reported the top 10 security challenges and they are categorized into infrastructure security, data privacy, data management and integrity and reactive security. To overcome these issues many solutions came into existence. The solutions are towards data integrity in cloud computing. The solutions also focused on the consistency in the data storage and retrieval. These solutions were explored in [7], [8], [9], [10], [11], [12] and [13] and [14]. In this paper, based on the solution in [14] we designed and implemented a security mechanism for data integrity in cloud computing. We also built an algorithm for data freshness.

3. Proposed Solution

The proposed solution is based on [14] where consistency is provided as a service. In this paper we explore more robust security mechanism. We design and implement a security mechanism for cloud data integrity and consistency. The proposed mechanism also takes care of data security. Figure 2 shows the parties involved in the proposed architecture.

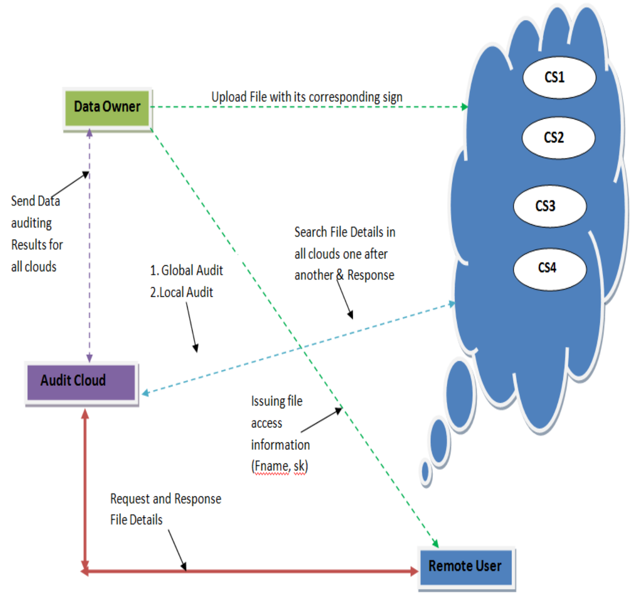

CS1
CS2
CS3
CS4
Data Owner
Upload File with its corresponding sign
Send Data auditing Results for all clouds
1. Global Audit
2.Local Audit
Search File Details in all clouds one after another & Response
Audit Cloud
Issuing file access information (Fname, sk)
Request and Response File Details
Remote User

Figure 2: Architectural overview of the proposed system

As seen in Figure 2, there are many participants in the cloud computing phenomenon. The data owner is responsible to outsource data to cloud. However, the data owner encrypts data and sends it to cloud. He can also decrypt the data and use it whenever required. The data owner can be give access to the data to other users who can download and decrypt data. The administrator has privileges to access data and performs other operations. The audit cloud is responsible to ensure integrity of cloud data.

Algorithm for Local Consistency Auditing

```
• Initial UOT with Ø
• while issue an operation op do
• if op = W(a) then
• record W(a) in UOT
• if op=r(a) then
• W(b) ∈ UOT is the last write
• if W(a) → W(b) then
• Read-your-write consistency is violated
• R(c) ∈ UOT is the last read
• if W(a) → W(c) then
• Monotonic-read consistency is violated
• record r(a) in UOT
```

Listing 1 – Proposed algorithm for Local consistency auditing.

Global Consistency Auditing

1) Time edge. For operation op1 and op2, ifop1 → op2, then a coordinated edge is added from op1 to op2.
2) Data edge. For operations R (an) and W(a) that originate from distinctive clients, a coordinated edge is included from W(a) to R(a).
3) Causal edge. For operations W(a) and W(b) that originate from distinctive clients, if W(a) is on the course from W(b) to R(b), then a coordinated edge is included from W(a) to W(b

```
Each operation in the global trace is denoted by a vertex
for any two operations op1 and op2 do
```

```
• ifop1 → op2 then
    o A time edge is added from op1 to op2
• ifop1 = W(a), op2 = R(a), and two operations come from different users then
    o A data edge is added from op1 to op2
• if op1 = W(a), op2 = W(b), two operations come from different users, and W(a) is on the route from W(b) to R(b) then
A causal edge is added from op1 to op2 Check whether the graph is a DAG by topological sorting.
```

Listing 2 – Algorithm for global consistency auditing

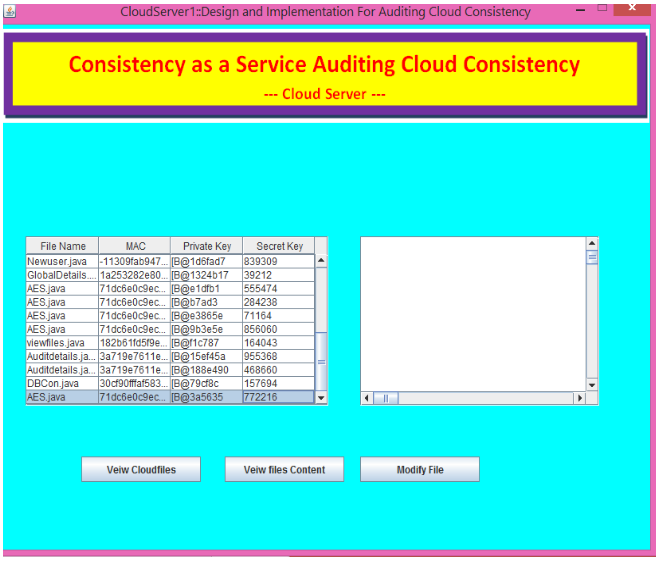
As shown in listing 1, the algorithm works as per the proposed algorithms that have stakeholders like user, cloud server, data owner and audit cloud playing their respective roles. The next section provides details of the implemented prototype application that demonstrates the proof of concept. The algorithm can also work for real time traces of security at run time and provide the details pertaining to security violations and other results. The ensuring section throws light into the results and implementation of the prototype.

Other Algorithms Used for Enhancing Security

In addition to the two algorithms presented in the previous sub section, two more algorithms are used in the implementation of the proposed system. AES (Advanced Encryption Standard) is used for encryption and decryption of data. Since the cloud servers are treated as untrusted the encryption and decryption standards are used to ensure secure data transmission. In the implementation of prototype digital signature is used in order to enhance security. Towards this end, Sha1 algorithm is used. It is one of the secure hash algorithms available. By using these two algorithms which are proven secure algorithms, the proposed system is leveraged with fool proof security.

4. Implementation and Results

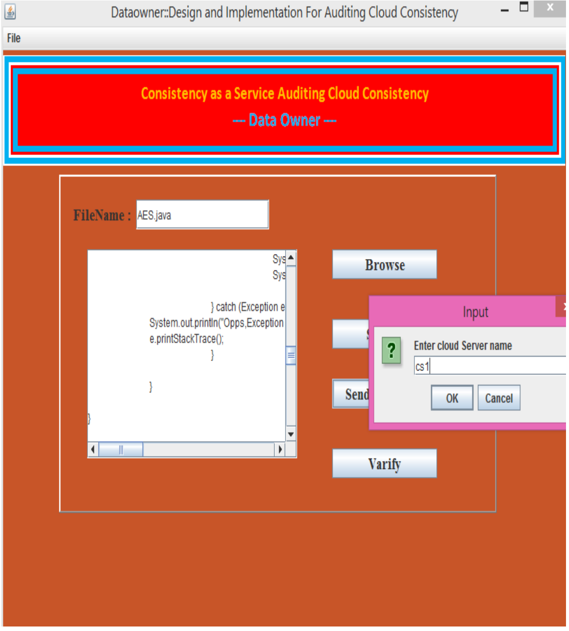
The proposed system has been implemented using Java platform. We designed and implemented a prototype application to demonstrate the proof of concept. The application simulates the behaviour of multiple parties involved in the system. The implementation mimics the functionalities of each party in the system. There are multiple services among which security, integrity and consistency are spread so as to make it a robust solution that will provide fool proof security. A typical cloud server UI is as shown in Figure 3. However, there are four servers used in simulation.


CloudServer1::Design and Implementation For Auditing Cloud Consistency
Consistency as a Service Auditing Cloud Consistency
--- Cloud Server ---
Veiw Cloudfiles
Veiw files Content
Modify File

File Name	MAC	Private Key	Secret Key
Newuser.java	-11309fab947...	[B@1d6fad7	839309
GlobalDetails....	1a253282e80...	[B@1324b17	39212
AES.java	71dc6e0c9ec...	[B@e1dfb1	555474
AES.java	71dc6e0c9ec...	[B@b7ad3	284238
AES.java	71dc6e0c9ec...	[B@e3865e	71164
AES.java	71dc6e0c9ec...	[B@9b3e5e	856060
viewfiles.java	182b61fd5f9e...	[B@f1c787	164043
Auditdetails.ja...	3a719e7611e...	[B@15ef45a	955368
Auditdetails.ja...	3a719e7611e...	[B@188e490	468660
DBCon.java	30cf90fffaf583...	[B@79cf8c	157694
AES.java	71dc6e0c9ec...	[B@3a5635	772216

Figure 3: Typical cloud server UI

As can be seen in Figure 3, it is evident that the cloud server side activities can be performed explicitly using the interface given. The content of data owners is saved in encrypted format. However, it is possible to view and manipulate content as per the privileges provided. In the same fashion data owner can interact with cloud with user-friendly interface. The interface for data owner is shown in Figure 4.


Dataowner::Design and Implementation For Auditing Cloud Consistency
File
Consistency as a Service Auditing Cloud Consistency
--- Data Owner ---
Browse
Send
Varify
Input
OK
Cancel

FileName : AES.java

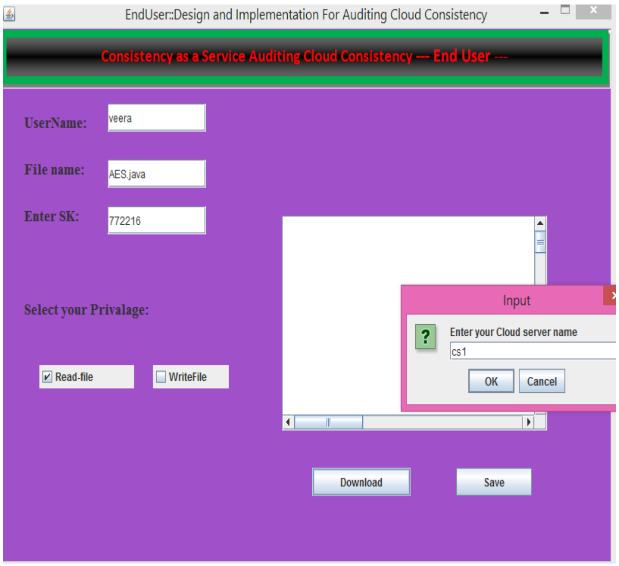
```
                                    Sys
                                    Sys

                   } catch (Exception e
       System.out.println("Opps,Exception
       e.printStackTrace();
                   }

       }

}
```

Enter cloud Server name

cs1

Figure 4: UI for data owner

As can be seen in Figure 4, it is evident that the data owner is able to save files to cloud in secure fashion. The file will be stored in encrypted format and the data owner can use it later. The data owner can also opt for audit cloud for checking for consistency. Data owner will be able to verify data that is stored in different cloud servers. Data owner can add new users who can access his data based on the privileges granted. It does mean that the data owner has provision to restrict accessibility to his data. Read file and Write file are the privileges available for user. A typical end user interface is shown in Figure 5.


EndUser::Design and Implementation For Auditing Cloud Consistency
Consistency as a Service Auditing Cloud Consistency --- End User ---
Input
OK
Cancel
Download
Save

UserName: veera

File name: AES.java

Enter SK: 772216

Select your Privalage:

☑ Read-file ☐ WriteFile

Enter your Cloud server name

cs1

Figure 5: UI for end user

As shown in Figure 5, end user can obtain data provided by data owner based on his privileges. User needs to choose privileges and resource details including security information and server name in order to data obtain data. At this stage audit cloud will check for inconsistency. End user can download the data and update to server as well after modifications based on his permissions given by the data owner. As discussed above, it is evident that the parties involved in the proposed system have distinct functionalities to be performed. The security is weaved among all these parties as described in the previous section. Data owner is responsible to provide permissions to users so as to let them gain access to data. Cloud server is meant for is responsible to accept the user data so as to let it be outsourced to cloud. Audit cloud is responsible for checking and verifying the data that has been verified by the cloud server so that the verified files can be made visible to users. Users can access data for which they have privileges.

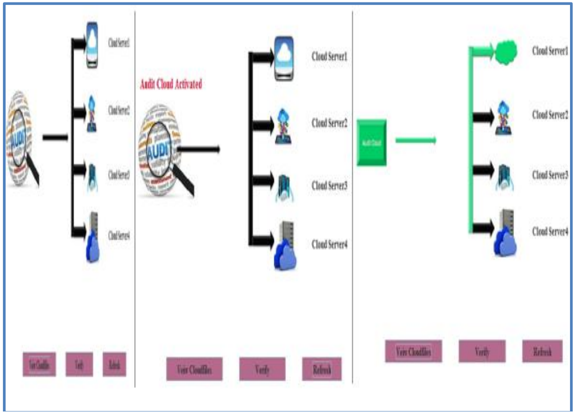


Figure 6 : Audit cloud simulation with three phases

As far as auditing is concerned, the auditing phases are shown in Figure 6. In the first phase, auditing is not initiated. In the second phase audit cloud gets activated and ready to perform its intended work. The simulation view shows how the process of auditing so as to ensure consistency of data.

5. Results

The prototype application is tested for its intended security. The proposed system has been tested with experiments. The proposed algorithm is also tested with traces of security violations and the results are compared with other existing systems.

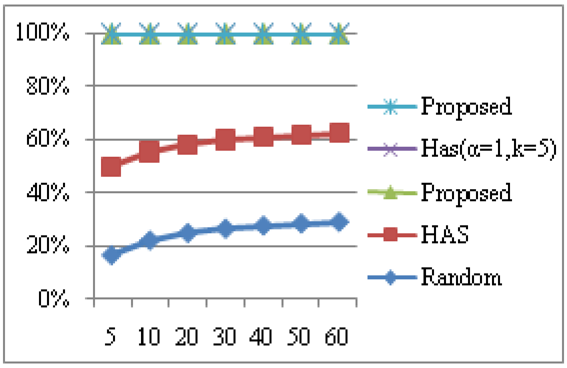


Figure 7: Percentage of revealed violations compared with Random and HAS

As shown in Figure 8, it is evident that the horizontal axis represents interval length while the vertical axis represents percentage of revealed violations. From the results it can be understood that the proposed system performs better than other existing systems.

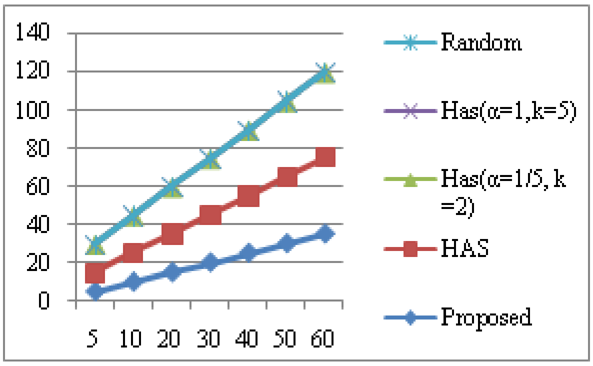


Figure 8: Number of reds compared with Random and HAS

As shown in Figure 7, it is evident that the horizontal axis represents interval length while the vertical axis represents percentage of revealed violations. From the results it can be understood that the proposed system performs better than other

6. Conclusion and Future Work

In this paper we explored cloud data integrity and consistency. Many solutions came into existence to provide consistency and integrity in cloud. They used different techniques for the same. However, the recent solution explored in [14] provided a method known s consistency as service so as to provide the consistency service to all cloud users. Based on this solution, in this paper we designed and implemented a security mechanism for cloud data integrity. Our solution has many parties involved. They are user, cloud server, data owner and Audit could server. Our solutions make use of policies to enforce data integrity in cloud. Based on the policies, it can identify and prevent violations. The proposed algorithms provide fool proof security and consistency. Our consistency mechanism can ensure that data owners' data is consistent. We built a prototype application that demonstrates the proof of concept. The experimental results reveal that the proposed system provides security to the cloud operations and also ensure that the data integrity is not lost. In future we will work on security issues in cloud computing

References

[1] Borja, S.Ruben, M.Ignacio, L. & Ian. (2007, July 7). *An Open Source Solution for Virtual Infrastructure Management in Private and Hybrid Clouds*. Retrieved from http://www.mcs.anl.gov/papers/P1649.pdf

[2] Chen,Z. Yoon, J. (2010). *IT Auditing to Assure a Secure Cloud Computing*. Retrieved from http://ieeexplore.ieee.org

[3] Dillon, T. Chen,Wu. & Chang, E. (2014). *Cloud Computing: Issues and Challenges*. Retrieved from Retrieved from http://ieeexplore.ieee.org

[4] Doelitzscher, F. Sulisto, A. Reich, C. Kuijs, H. & Wokf, D. (2010, July 30). *Private cloud for collaboration and e-Learning services: from IaaS to SaaS*. Retrieved from http://wolke.hs-furtwangen.de/assets/downloads/CRL-2010-01.pdf

[5] Dore, P. Leite, A. (2011). Commentary : *Cloud computing e A security problem or solution?*.Retrievedfromhttp://www.sciencedirect.com/science/article/pii/S1363412711000495

[6] Subashini,S. Kavitha, V. (2011). *Journal of Network and Computer Applications*. Retrieved from http://www.sciencedirect.com/science/article/pii/S1084804510001281

[7] "Pushing the CAP: strategies for consistency and availability," *Computer*, vol. 45, no. 2, 2012.

[8] E. Anderson, X. Li, M. Shah, J. Tucek, and J. Wylie, "What consistency does your key-value store actually provide," in *Proc. 2010 USENIX HotDep*.

[9] C. Fidge, "Timestamps in message-passing systems that preserve the partial ordering," in *Proc. 1988 ACSC*.

[10] A. Tanenbaum and M. Van Steen, *Distributed Systems: Principles and Paradigms*. Prentice Hall PTR, 2002.

[11] W. Vogels, "Data access patterns in the Amazon.com technology platform," in *Proc. 2007 VLDB*

[12] H. Wada, A. Fekete, L. Zhao, K. Lee, and A. Liu, "Data consistency properties and the trade-offs in commercial cloud storages: the consumers' perspective," in *Proc. 2011 CIDR*

[13] M. Rahman, W. Golab, A. AuYoung, K. Keeton, and J. Wylie, "Toward a principled framework for benchmarking consistency," in *Proc. 2012 Workshop on HotDep*.

[14] Qin Liu, Guojun Wang, and Jie Wu, Fellow. (MARCH 2014). Consistency as a Service: Auditing Cloud Consistency. *IEEE*. 11 (1), p25-35.