International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Fine Grain Level Trust Enhancement between CU and CSP in Replication Jobs

Dr. Sandeep Singh Kang[1], Hardeep Kaur[2]

[1]HOD (CSE), CGC College of Engineering, Landran, Mohali, India

[2]M. Tech Student, CGC College of Engineering, Landran, Mohali, India

Abstract: ***In this research work we have developed on systematic approach to investigate the concepts related to usage of Third Party Auditor, in cloud computing we have done a tabular analysis of work done by authors in this area with observes in on their outcomes, results and their limitations of work, and based on these findings we have suggest few pointers towards future scope in this area with the observed on facts and figures of the trust levels, degrees between cloud users, cloud service providers and Third Party service providers who help in monitoring and auditing.***

Keywords: Trust, Fine Grain Level Trust, Third Party Auditor, Cloud User, Cloud Service Provider.

1. Introduction

Cloud Computing is very well-known today in IT industry. But in real the Cloud Computing is based on the uses of internet and computer applications. Google Apps is the one of the example of this that provides us the many online business applications and many more services. Cloud services [2] can be accessed by using the internet. Every information like Web Pages, Programmers can accessed from the servers at any time by the user. In simple words all the work related to the computer doing online by using the internet is called Cloud Computing i.e. communication between the cloud server and cloud user. All the data can be stored on the servers by using this. In actual internet is the connection of our entire world's computer in which we use the similar technique to form the connection between them. So the information that is used in the bunch of these computers or servers is collectively called the cloud. According to this, the work like any searching, any updating of world's news occurred through the cloud. First of all the request goes to server and after that the communication is initiated related to search between all the servers that are connected to each other. Before reply to the user they form the server website first and then it formatted into a single page and then it send to user. The question is arises can we trust in this? Yes, we can but there are number of risks and incentives are involved in this. Trust [1], [2] may revolves around assurance and confidence that performed by people, data and entities in many expected manners. During the interaction of entities there are number of risk and uncertainties in which trust is very beneficial. Trust might be regarded as consequences of progress towards security and privacy objectives. Trust may be machine to machine, human to machine, machine to human and human to human. STAR (Security, Trust & Assurance Registry program) [1], Trust Aware System [3], CTP (Cloud Trust Protocol) [2], Trust Prediction

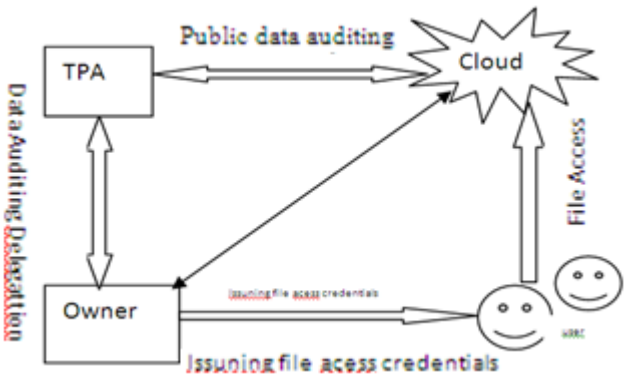

Figure 1: Architecture of simple cloud storage

Model for e-commerce [4] these are the frameworks that help to increase the trust between stack holders of cloud environment. As discussed in earlier that the no of security related issues are involved between the user and the server so we have need to TPA (Third Party Auditor) and auditing to reduce these risks between them. Auditing is required to make the data confidential against the auditor, auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds, should support the dynamic updates of the data in the cloud. Third Party Auditor [3, 4] builds the trust between two parties. It also reduces the additional communication overhead of the cloud user [1].

2. Reviews

Many authors worked on this concept all of them they used the algorithm is TPA.

Table 1: Authors reviews

Sr. No.	*Algorithm*	*Results*	*Work incomplete*
1	TPA(for maintaining consistency)	99% detect error probability[6]	Challenging issues for Public Auditing Services
2	TPA(for Publicly Auditable)	Handled multiple concurrent tasks	Challenging issues for Batch Auditing[7]
3	TPA(for Privacy Ensuring using HLA)	Minimum overhead and Minimize the BW used	Protection against server clouding attacks
4	TPA(for data sharing)	Auditing and strong back end protection	Verify the integrity of the JRE[5] and the authentication of JARs.

3. Research Gap

After conducting exhaustive systematic literature survey and are possible solicited material associated with topic from various journals conferences material we can say limited work has been done which at fine grain level (file block level) auditing, monitoring with authentication is done using Third Party service providers in replication on demand jobs scheduling in cloud providers. Hence, the existing work can move in this direction and improve this system.

4. Conclusion

As per study it is found that that previous systems lack full fledge, autonomous sub-systems that can be used for the public at large without confirming the confidentiality of system in terms of its traceability of users interacting between the CSP and CUs[1], either MAC based or private + public key mechanism are used, moreover the protocol involved become more and more robotic in nature in terms of authentication, [zero knowledge] once compromised all the process associated with get compromised. So there is an urgent need to build incidence reporting system which across multi cloud services, whose data can be publically traceable, verifiable and a black list can be build, therefore we shall implement such system.

5. Future Scope

Based on the fact and figures we have studied in this area we suggest that of focused work doing on Develop cloud simulated environment. To enhance and add value of public security system that uses TPA (Third Party Auditor) [3, 4]with file block level security mechanism by using Merkle Hash Tree (MKT). To enhance in terms of scalability in which security of file blocks is maintained without knowing the credentials of actual data. Calculate performance metrics in terms of scalability of file size, data correction, computational time, number of sampled blocks and evaluation based on CVSS scoring system.

References

[1] Francisco Moyano, Carmen Fernandez- Gago and Javier Lopez,"A Framework for Enabling Trust Requirements in Social Cloud Applications" 2013.
[2] Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey(RAND Europe) Hans Graux(time.lex) Sadie Creese & Paul Hopkins (University of Warwick) ,"The Cloud: Understanding the Security, Privacy and Trust Challenges" 2010.
[3] Ashish Bhagat Ravi Kant Sahu Using, " Third Party Auditor for Cloud Data Security: A Review" 2013.
[4] Armbrust,M., Fox, A.,Griffith,R.,Joseph, A.D.,Katz, R.H.,Konwinski, A.,Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M., "A view of cloud computing. Commun" 2010.
[5] M.Vanitha, R.Raju, "Data Sharing: Efficient Distributed Accountability in Cloud Using Third Party Auditor" 2013.
[6] Abhishek Mohta and Lalit Kumar Awasthi, "Cloud Data Security while using Third Party Auditor" 2012.
[7] Cong Wang and Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute Jin Li, Illinois Institute of Technology, " Toward Publicly Auditable Secure Cloud Data Storage Services" 2010.
[8] Vinaya. V Sumathi.P, "Implementation of Effective Third Party Auditing for Data Security in Cloud" 2013.
[9] C. Wang, Q. S.M. Chow, Kui Ren and Qian Wang, "Ensuring data storage security in cloud computing" 2011.

Author Profile

Dr. Sandeep Singh Kang is working at CGCCOE Landran as HOD (CSE) Since Nov, 2007. 2013. He did his B.Tech from Punjab Technical University and M.Tech from Punjabi University Patiala. Recently he has completed his PhD in Computer Science & Engineering in the area of Wireless Networks. He has total of 10 years of Experience. He has Published 52 Research Papers in International/National Journals and Conferences and attended 12 workshops and FDP's for enhancement of his skills. He has published a BOOK Title: "**Integrated Approach to Network Security".** Besides this, he has guided around 20 Students for PG Research Work and guiding 02 students for doctorate. His area of specialization is Security of Wireless Networks. He is the Life Member of Computer Society of India and Member Board of Studies (Computer Science), Punjab Technical University, Jalandhar.

Hardeep Kaur received the B.Tech degrees in Computer Science & Engineering from Shaheed Udham Singh Institute of Engg & Technology (Tangori) Punjab in 2011 and Now Pursuing M.Tech (2011-2013) in Computer Science & Engg in Chandigarh Group of colleges College of Engg & Technology (Landran) Punjab.