International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Special Approach to Enhance the Security Level and Apply Dynamic Operations on Cloud Computing

G. Rama Subba Reddy[1], A.Rama Obula Reddy[2]

[1]Associate Professor &Head Department of CSE, VBIT, Proddatur, Y.S.R, A.P, (India)

[2]Assistant Professor, Department of CSE, CBIT, Proddatur, Y.S.R, A.P, (India)

Abstract: ***Now a days Internet grows up rapidly. Anything depends on network. This internet provide huge services to the users like data transfer, uploading, downloading etc… some of network services also provide security too. But here data storage is major task, its highly impossible to store huge data in network. Now the new emerging technology is cloud computing, its improve the performance, scalability and low cost to implement. Its provide many services to clients. Like upload the data retrieve the data etc… many organizations are depends on this storage service. We can install the cloud private or public or both. But cloud computing suffer from unauthorized data access. Still there is no permanent solution. These paper main objects are a) Prevent from unauthorized access b) prevent unnecessary steps to access the cloud c) To apply some tasks on cloud.***

Keywords: cloud computing, authentication, security methods, networks, TS (Trusted System)

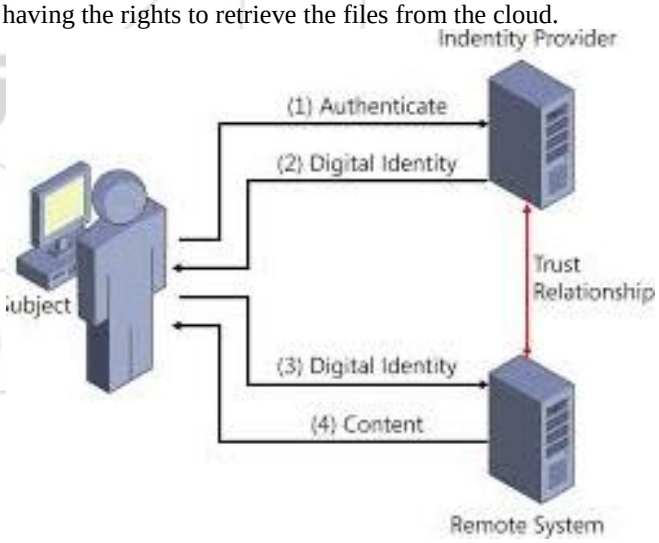
1. Introduction

Cloud computing is emerging area for the organisations.it gives great platform for the to store all kinds of information. Although cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures, it also introduces a range of new security risks. As cloud computing brings with it new deployment and associated adversarial models and vulnerabilities, it is imperative that security takes center stage.Continuously data will be stored from various IT services. Easy to store the data in the cloud but in existing no guarantee to provide security. In the network world data protection is not a simple task; various advanced encryption methods are available. For especially in private cloud data protection is easy because all the systems are under the single controller and also private cloud computing connected only less number of clients here easy to observe and test the status frequently.In case of public cloud computing everything data will be public, the main intention is to keep the data available to all. In distributed environment data protection is not easy to store the data securely we use some encryption methods, based on data securecy require either can use symmetric and public cryptography method. In hybrid cloud computing protects data in two ways, i.e.; some data belongs to only private and others are public. Existing papers described only about data protect from unauthorizedusers, for each transaction to require authentication permission from the ID provider. Suppose in case if want do two or more transactions on same server to take that number of requests from the controller.so it is delay process and to follow this method all the next coming request are always waiting state. To overcome the problem our proposed system divides the entire procedure into three steps.

1. Request connection
2. Data Transfer connection
3. Disconnect the connection.

2. Existing Systems

In Existing method client upload the to the cloud there no restriction to upload and download the files especially in case of public cloud computing in later days before upload and retrieve the data cloud test the authentication. Now a days client should to protect the from unauthorized users encrypt the data before uploading, and those clients only having the rights to retrieve the files from the cloud.

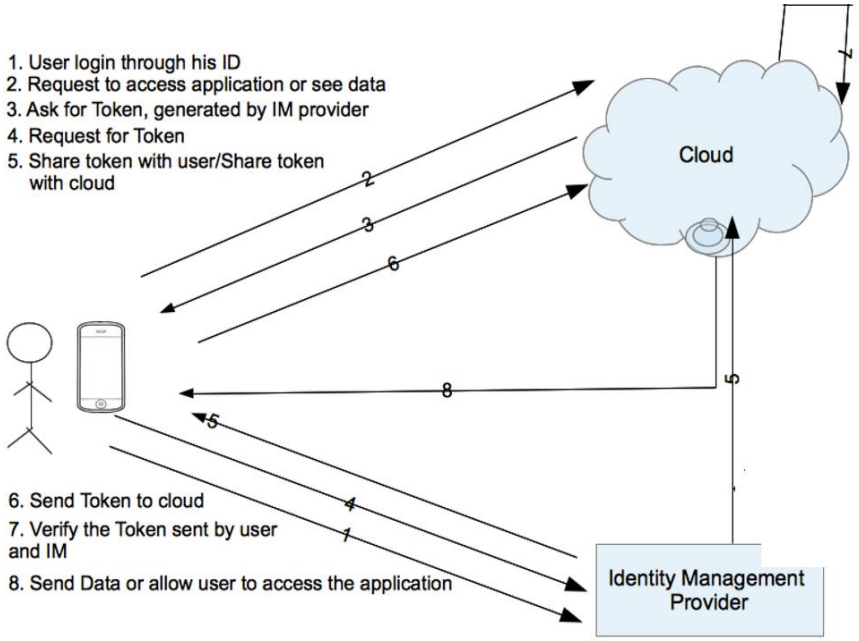


From this fig subject (client) want to make a connection with cloud (server) first it cloud be authenticate by trusted party.it checks the details and provide id to make connection with server (cloud).here there is no session time for the connection, due to this reason may b chance occur a collision because there no expire time for the connection and if the existing connection is release still there no proper notification. For initial step client authenticated by trusted system (TS) and get the digital id from TS. Using this id client start either upload the files or download the files. But still have some problems those if want to upgrade file on

cloud there no possible, for that download the file and do modification and then upload again.

3. Proposed System

In this paper, we would like to examine what can be achieved in a fully identity-based approach for cloud environment.



It is similar to existing method but here enhance some futures those are

1) **Prevent from unauthorized access**
   In this case special encryption techniques are applied, tofind outclient is authenticate or not. If the client is authenticated allow request to either upload or download otherwise not.
2) **Reduce the steps to access the cloud**
   Basically for every connection client should authenticated by TS.but in proposed paper once the client authenticated by TS for many several steps there no need to take a permission from the TS ,so finally save the bandwidth and time. For every connection TS assignedSession time if the session time is expire connection close automaticalluy.here session time started at Initial step itself it expire until to close the connection. If client want extend the connection send request to TS.
3) **Apply the task on cloud dynamically**
   Cloud support both static and dynamic methods. In Existing follows static methods to change the data on the cloud. It take more time to do any dynamic operations. But in this paper modification and renaming the files dynamically. The cloud itself to do any modifications without ant data loss and interrupts.

Finally by using above steps improve the dynamical usage of the cloud computing. All the authentication services are implemented by using Kerberos alogorithms.it also support confidentiality and integrity.

4. Conclusion

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, renaming, and append. The growing need for secure cloud storage services and the attractive properties of ID-based cryptography lead us to combine them, thus, defining an innovative solution to the data outsourcing security issue. We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified.

References

[1] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.
[2] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing",http://www.ibm.com/developerswork/websphere/zones/hipods/library.html, October 2007, pp. 4-4
[3] "Wesam Dawoud, Ibrahim Takouna, Christoph Meinel Infrastructure as a Service Security.
[4] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.
[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. of CCS '07, pp. 598–609, 2007.
[6] Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
[7] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic

Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
[8] Amazon, "Amazon simple storage service (amazon s3)." [Online]. Available: http://aws.amazon.com/s3/
[9] "A dynamic key infrastructure for grid," in Proceedings of the 2005 European conference on Advances in Grid Computing, ser. EGC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 255–264.

Author Profile

G. Rama Subba Reddy received his M.E (Computer Science &Engineering) from Sathyabama University, Chennai. Presently he is working as Associate Professor & Head department of Computer Science & Engineering, Vignana Bharathi Institute of Technology, Proddatur, Kadapa Dist, and A.P, India

A. Rama Obula Reddy received M.Tech (Computer Science) from JNTU Hyderabad. Presently working as Asst.Prof in Computer Science & Engineering, Chaitanya Bharathi Institute of Technology, Proddatur, Kadapa Dist., A.P, India