

OTP Generation- A secure approach towards file storage on a cloud

Kapila Purohit, Anurag Rana

Research Scholar, CSE Department, Arni University, H.P, India
Assistant Professor, Department, Arni University, H.P, India

ABSTRACT

Cloud computing is the new trending model used for computing in which the internet is used for communicating and storing the data. Some of the crucial functionalities of cloud computing is data uploading and securely storing the data into cloud. The protection of the confidential and data processed and generated during the computation is becoming the major security concern. In cloud computing, data protection is the most important security issue. This issue, will concern in which data is accessed and stored, audit requirements, compliance and notification requirements, issues involving the cost of data breach, and damage the brand value. The main objective of this paper is to propose an algorithm, which uses a address of users as a reference key. To generate an OTP (One Time Password) key after uploading a data file in cloud. To store sending details of users which is a reference key generated by OTP which itself is a reference key. So in this paper we have compared both techniques according to their features available.

Keyword: - *Cloud Computing, Security in Cloud, OTP*

1. Introduction

Cloud Computing is a novel networking technology, which is a combination of Distributed Computing, Parallel Computing, Grid Computing, Virtualization Technology and Utility Computing to offer scalable, virtualized resources (Infrastructure, Platform and Software) in pay-as-you-go manner in the form of 'X as a Service' service model. Our dissertation is focused on the augmenting Cloud Computing security system using One Time Password System. As User Profiling System requires Artificial Intelligence techniques to build behavioral models of users and their analysis, some research work experiments with Fuzzy Systems and Genetic Algorithms in their conventional ways to design a UPS for Cloud Computing security and studies their behavior (of UPS) and purposes a new and comprehensive hybrid approach to design a UPS for Cloud Computing security using Fuzzy guided Genetic Algorithm.

1.1 Security Issues

IDC (International Data Corporation) enterprise panel report in August 2008 [31] highlights the problems facing during Cloud Computing Platform development and depicts how the domain of security in Cloud Computing dominates all other problems with the highest percentage of 87.5%. That is the reason, why research in Cloud Computing Security becomes a hot spot area. Some of the main areas identified as the threats to Cloud Computing security are as [32]:

- **Threats to Cloud User:** The Cloud user may face the following threats:
- **Threat of data leaks:** Service-provider accesses the user's data very first instead of the intended user, which can pose the threat of data leaks.
- **Threat of management right loss:** Because of the non- clarity of actual location of the service or data, it is difficult for maintain compliance between the jurisdiction of different nations and users should understand this risk.
- **Threat of unintended data mixture and threat of data location change virtualization:** Cloud Computing has flexible sharing nature. So, users' data are located on a shared hardware, which poses the risk of data mixture and location virtualization.

- **Challenge of data recovery and restoration:** Data should be erased completely to ensure data security in Cloud environments, when requested.

1.2 Service Models of Cloud Computing

According to the NIST, Cloud Computing can be divided into three layers based on the Service Model (i.e. services provided by Cloud Computing) [10].

- **The infrastructure layer** is comprised of processed hardware resources by virtualization technology and distributed technology. The Cloud service-providers offer the processed hardware resources, namely Infrastructure as a Service, to the users through internet and users have to just connect to cloud through internet terminal and subscribe these services to utilize the infrastructure resources offers by the Cloud service-providers.
- **The platform layer** is in between the Infrastructure layer and the Application layer, comprised of various middleware and software of the Cloud Computing platform. The user can make advantage of the development environment, deployment environment and management environment to carry out the development, deployment and management cycle of the application.
- **The application layer** consists of the various applications running on the Cloud, which can satisfy the general as well as some personalized demands and the users can avoid the acquisition cost of software license.

2. Our Work

The main objective of this proposed work is that we will generate an algorithm. In which reference key is to be conducted by cloud. When user wants to upload their data file in cloud before that an OTP key (One Time Password) is generated and this OTP key will send to users by message to their mobile phones and by email ids. After that user can enter their OTP key and easily can upload their data file in cloud. Database, will generate a reference key which contains a detail address of users where OTP key was sent in. Only administrator will have rights to see a detail of reference key. In future if any worms found in that data file which uploaded by user in past then administrator of that cloud will sending a message to that users for updating or correct their data within two days, if no action will performed by user in two days then administrator of that cloud will discard that data file from cloud. An OTP is a password that is valid for only one login session on a computer system. OTPs avoid number of shortcomings that are associated with traditional (static) password based on authentication. The most important advantage that is addressed by OTPs is that, in contrast to static passwords. They are not vulnerable to replay attacks. A second advantage is that user who uses the same password for multiple users. When user wants to upload their data file in cloud before that an OTP key (One Time Password) is generated and this OTP key will send to users by message to their mobile phones and by email ids. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further. OTP is generated by using mathematical algorithm where the new password is based on a challenge (eg. Random numbers chosen by the authentication server).

The Results shown below are that of the work performed to enhance security of data in a cloud computing. Every diagram shows each step of how we authenticate the data which is stored in our cloud. We all have thinking that the data in cloud environment is not safe because of the 3rd party owners who are providing us the space. So in our work we have tried to bring security in that part. Below are the diagrams that show working of how we have implemented the security by generating OTP.

First diagram shown below that is figure number 1. It shows us the clear picture of uploading of file home page in which we need to enter our email id first and then we need to enter the upload file and finally the file which we want to upload. We browse that file and then we click on upload file option. This uploading file actually allows us to take the file from the place where we have stored our file and then that file we actually select and browse and then we click on the upload option. Therefore below figure number 1 actually represents the uploading of the file from where we want to upload.

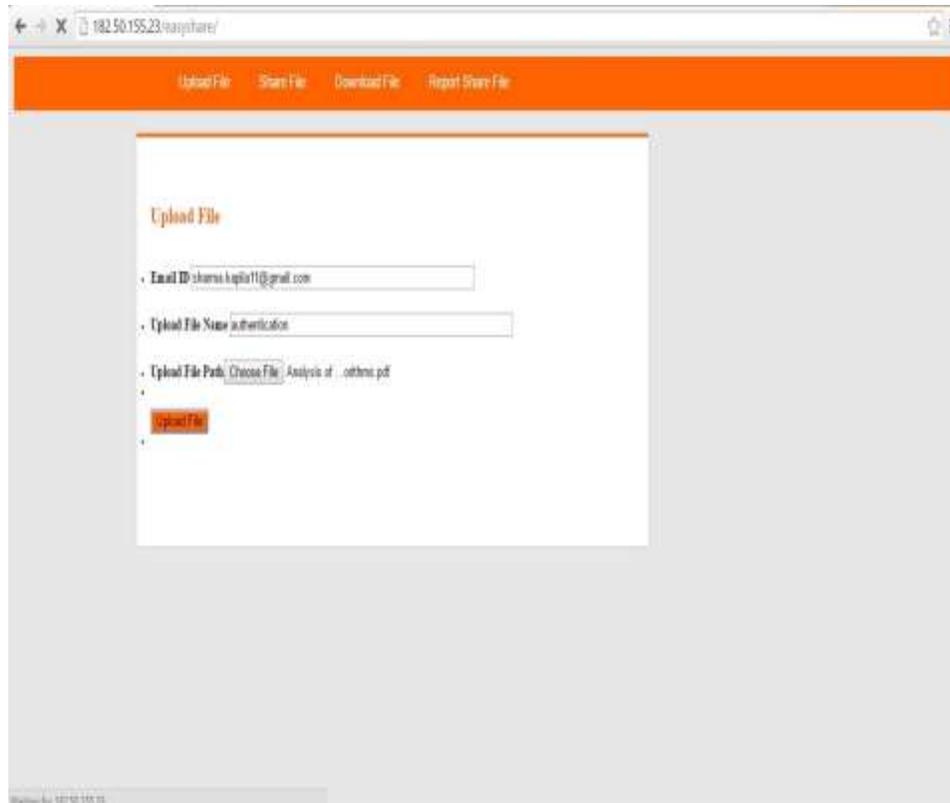


Fig 1. Page For Uploading a File

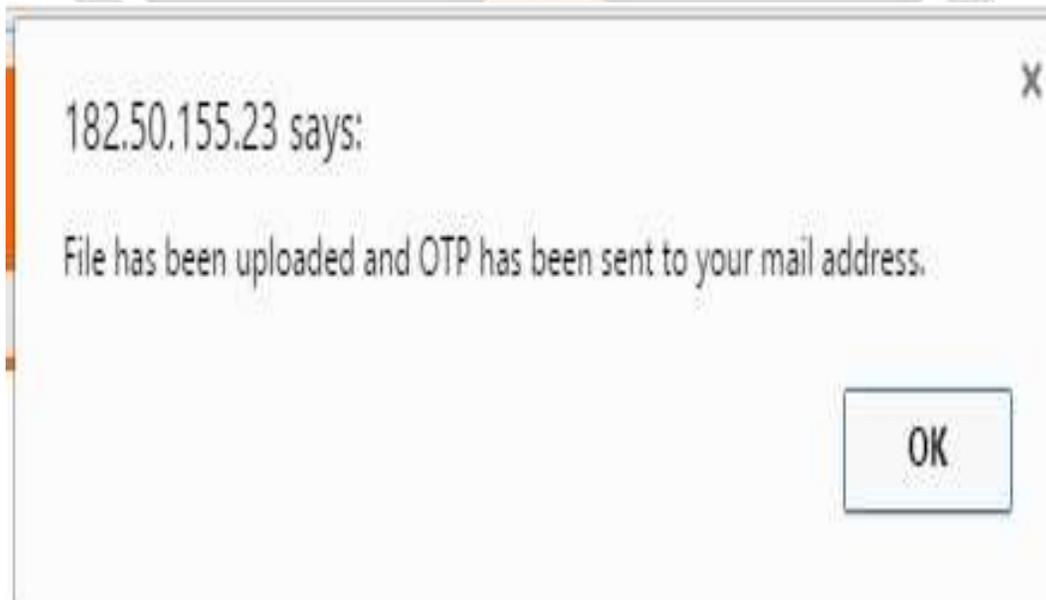


Fig 2. Generation of OTP

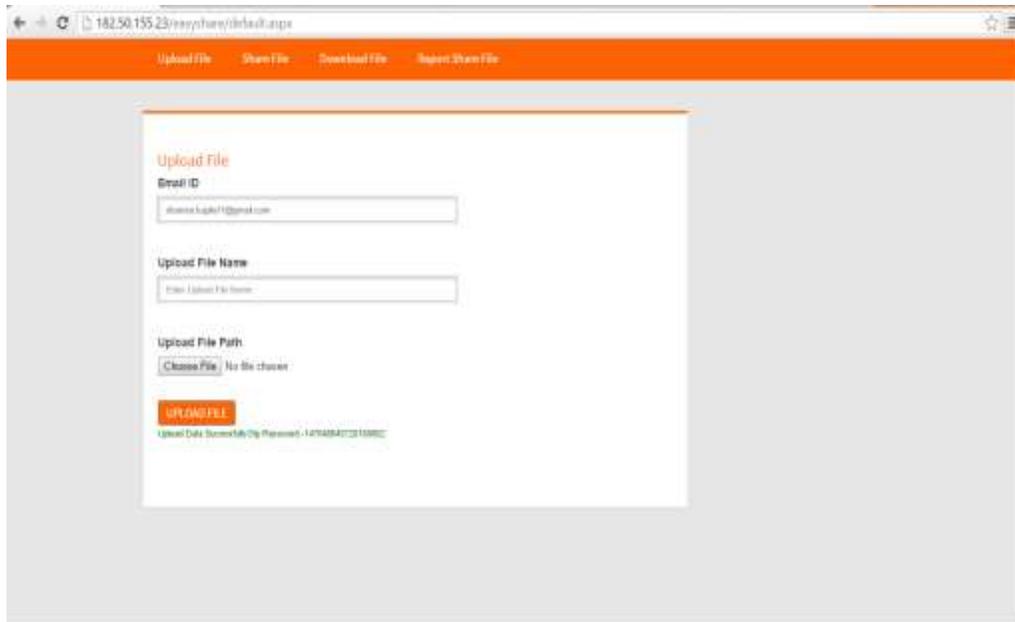


Fig 3. Completion of uploading of File

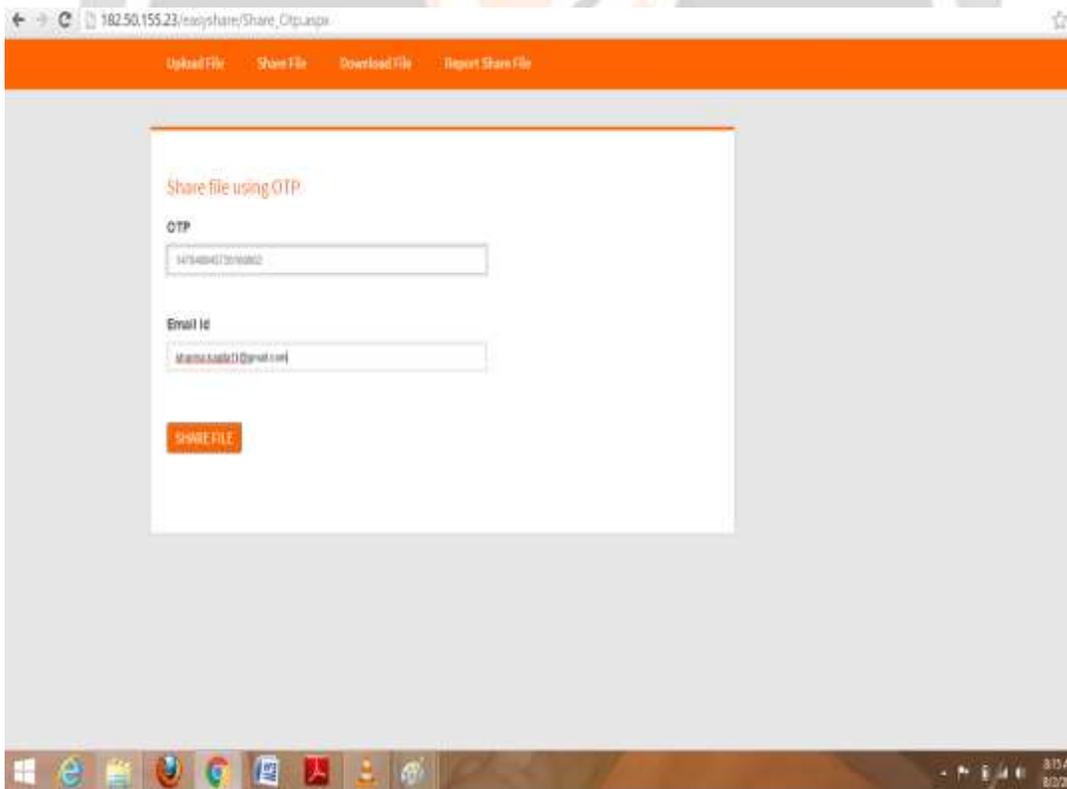


Fig 4. Entering of Generated OTP

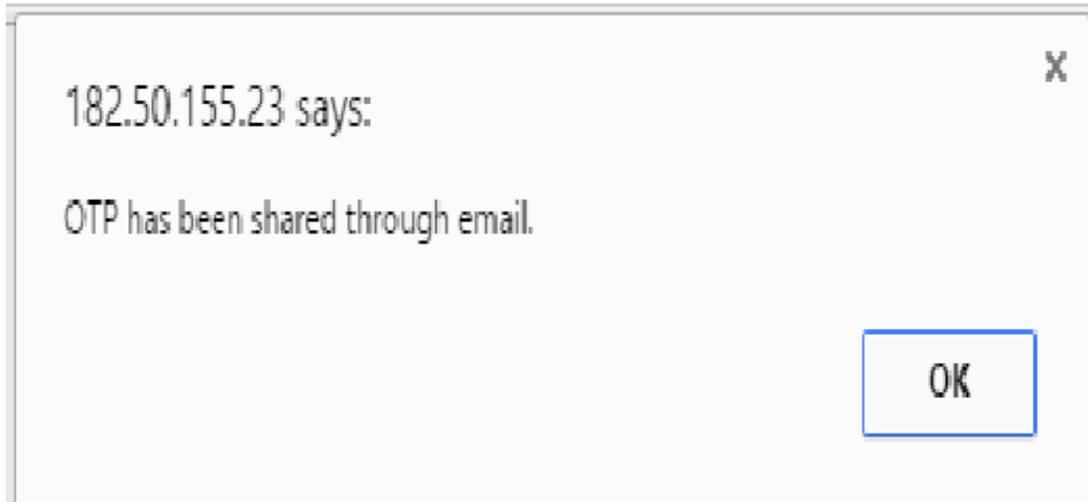


Fig 5. OTP sent Through Mail

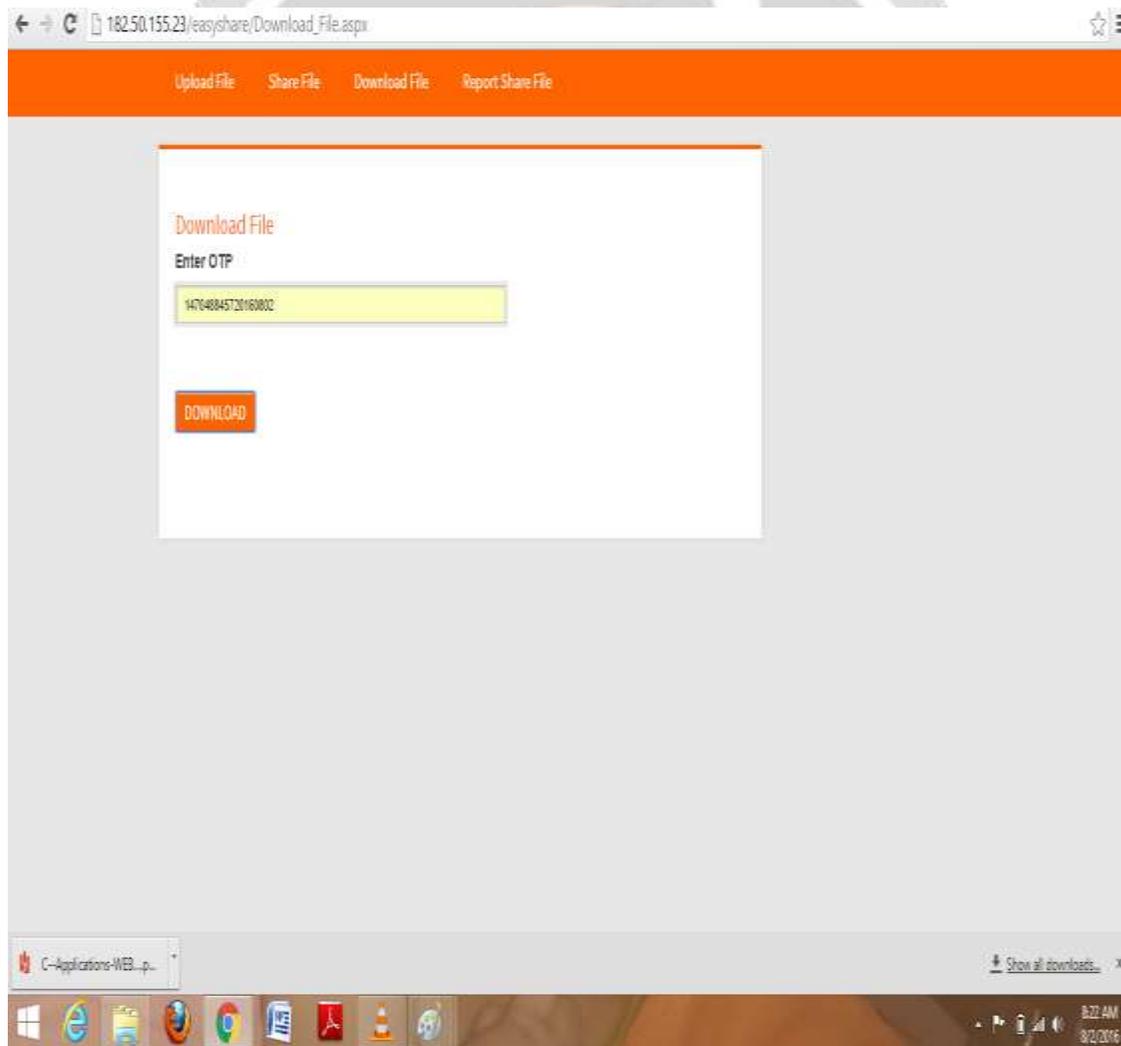


Fig 6. Downloading File Through OTP

Fig 7. Report Sharing File

4. CONCLUSIONS

Overall we can conclude that the security of data in cloud computing is decreasing day by day. Therefore every day a new technique comes and overcome the shortcoming of security and everyday hacker tries to break that security. Therefore the work which we have done shows effectiveness in increasing security. In our work when user wants to upload their data file in cloud before that an OTP key (One Time Password) is generated and this OTP key will send to users by message to their mobile phones and by email ids. After that user can enter their OTP key and easily can upload their data file in cloud. Database, will generate a reference key which contains a detail address of users where OTP key was sent in. Only administrator will have rights to see a detail of reference key. In future if any worms found in that data file which uploaded by user in past then administrator of that cloud will sending a message to that users for updating or correct their data within two days , if no action will performed by user in two days then administrator of that cloud will discard that data file from cloud. An OTP is a password that is valid for only one login session on a computer system. OTPs avoid number of shortcomings that are associated with traditional (static) password based on authentication. The most important advantage that is addressed by OTPs is that, in contrast to static passwords. They are not vulnerable to reply attacks. A second advantage is that user who uses the same password for multiple users. Therefore we can say that the work done in our research will provide authenticated data storage in cloud.

6. REFERENCES

- [1] R. Mazumder, R. H. Rakib, and M. S. Uddin, "Implementation of Cloud Computing in IT Sector: Perspective of Bangladesh," *International Journal of Research & Reviews in Computer Science*, vol. 3, no. 1, 2012.
- [2] P. Zeeshan, S. Lee, and Y-K Lee, "Multi-tenant, secure, load disseminated SaaS architecture," *12th International Conference on Advanced Communication Technology (ICACT)*, vol. 1, pp. 214-219, 2010.
- [3] M. P. Rad, A. S. Badashian, G. Meydanipour, M. A. Delcheg, M. Alipour, and H. Afzali, "A survey of Cloud platforms and their future," *Computational Science and Its Applications–ICCSA*, Springer Berlin Heidelberg, pp. 788-796, 2009.
- [4] J. Carolan, S. Gaede, J. Baty, G. Brunette, A. Licht, J. Rimmell, L. Tucker, and J. Weise, "Introduction to Cloud Computing architecture," *Sun Micro Systems Inc*, 1st edition, White Paper, 2009.
- [5] G. Gruman, and E. Knorr, *What Cloud Computing really means*, accessed April 2008, <http://www.infoworld.com/article/08/04/07/15FE-cloud-computingreality1.html>.

- [6] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the Clouds: A Berkeley view of Cloud Computing." *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, vol. 28, pp. 13, 2009.
- [7] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in Cloud Computing," *5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pp. 18-21, 2010.
- [8] S. Laniece, M. Lacoste, M. Kassi-Lahlou, F. Bignon, K. Lazri, and A. Wailly, "Engineering intrusion prevention services for IaaS Clouds: The way of the hypervisor," *IEEE 7th International Symposium on Service Oriented System Engineering (SOSE)*, pp. 25-36, 2013.
- [9] G. Chunmei, B. Xueyao and Y. Fan, "Security Technology Study and Trend of Cloud Computing," *Netinfo Security*, vol.4, 2010.
- [10] P. Mell, and T. Grance, "The NIST Definition of Cloud Computing," vol. 15, 2009.
- [11] J. Silvestre, "Economies and diseconomies of scale," *The New Palgrave: A Dictionary of Economics*, vol. 2, pp. 80-84, 1987.
- [12] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud Computing and grid computing 360-degree compared," *IEEE Grid Computing Environments Workshop (GCE'08)*, pp. 1-10, 2008.
- [13] A. Albeshri, and W. Caelli, "Mutual protection in a Cloud Computing environment." *12th IEEE International Conference on High Performance Computing and Communications (HPCC)*, pp. 641-646, 2010.
- [14] S. U. Muthunagai, C. D. Karthic, and S. Sujatha, "Efficient access of Cloud Resources through virtualization techniques," *IEEE International Conference on Recent Trends In Information Technology (ICRTIT)*, pp. 174-178, 2012.
- [15] W. Liu, "Research on Cloud Computing security problem and strategy," *IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1216-1219, 2012.
- [16] G. Lin, "Research on electronic data security strategy based on Cloud Computing," *IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1228-1231, 2012.
- [17] Sahil, and S. Dogra, "Cloud Computing and its Security Concerns A Survey," *International Journal of Innovative Technology and Exploring Engineering*, vol 3, no. 12, pp. 15-18, 2014.
- [18] Wikipaedia, *Distributed Computing*, accessed September 4, 2014, [http://en.wikipedia.org/wiki/Distributed computing](http://en.wikipedia.org/wiki/Distributed_computing)
- [19] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *International journal of high performance computing applications*, vol. 15, no. 3, pp. 200-222, 2001.
- [20] I. Foster, C. Kesselman, J. Nick, and S. Tuecke, "The physiology of the grid: an open grid services architecture for distributed systems integration. Globus Project, 2002," 2006.
- [21] G. S. Almasi, and A. Gottlieb, *Highly parallel computing*, Benjamin-Cummings Publishing Co., Inc., 1989.