IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Importance of TPA and Homomorphic Token for Data Storage Security in Cloud

Sneha S. Bhandarkar[1], Buri Chanukya[2], Sandhya Rani[3], Y. V. N. Phani Kishore[4]

Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology,

Hyderabad, India [1,2,3,4]

Abstract: Cloud computing has been envisaged as the future architecture of IT industry. It has many benefits such as flexibility, scalability. However, it poses many new security challenges such as data integrity and confidentiality. In this paper, we mainly focus on cloud data storage security, which has always been an important feature to assure the quality of service. To be certain of the accuracy of users' data in the cloud, we have put together the studies based on the effective and flexible mechanism of utilizing the homomorphic token combined with the distributed verification of erasure-coded data which helps achieve the integration of storage correctness insurance and data error localization. In addition to the above, the mechanism also supports secure and efficient dynamic operations. Substantial security and execution analysis shows that the proposed mechanism is highly successful and resistant against Byzantine failure, server colluding attacks and unauthorized data modification attack.

Keywords: Cloud; Cloud Computing; Data Integrity; Confidentiality; Homomorphic token; Data Error Localization; Byzantine failure.

I. INTRODUCTION

Cloud Computing refers to the conveyance of computing resources over the internet [1]. It provides individual and the businesses to use software and hardware resources. Cloud users do not have to invest on the infrastructure, hardware, software hence providing us with the rapid deployment and flexible use. Cloud Computing provides the user with the pay-as-you-go model.

The benefits [2] are improved flexibility, reduced capital costs, scalability, higher utilization through virtualization, lower operation cost, collaboration efficiency, less environmental impact, automatic software integration, quick deployment.

However, there are also a few challenges [3] to be considered. Security and Privacy are the main important challenges in cloud computing. Security is the main concern while moving the data to the cloud [4]. The user has no control over the data. Selecting where and how your data is stored is an important aspect to be known by the user. Service Quality is to assure the requirements for running the production application on the cloud. So when the network or internet connection is unavailable, it also means that cloud services are also unavailable; thus data cannot be accessed. Making the correct choice of services such as-PaaS, IaaS, SaaS to provide the right kind of required service is equally important. Transparency of service delivery, billing and interoperability are also to be considered.

Cloud Computing provides the user with several Deployment and Service models. Some of the deployment models [5] are:

Public Cloud: It is a type of cloud hosting provided over a network, in which the cloud services are open and easily available for use by the public. It can be accessed by anybody with an active Internet connection, a subscription and with access to the cloud space.

Private Cloud: It permits only the authorized users and gives the organization greater and direct control over their data.

Hybrid Cloud: It can be a combination of two or more cloud servers like the private, public or community cloud that is enclosed together but remain individual servers. The advantages of the multiple deployment models are present in a hybrid cloud hosting.

Mobile Cloud Storage: In mobile cloud storage, separate data is stored in the cloud and accessed at anytime from anywhere.

Figure 1 depicts the various Cloud Deployment Models.

Some Service Models [6] are as follows:

In **Infrastructure-as-a-Service** (IaaS), cloud users will have direct means towards the hardware resources and Clouds will typically utilize set of virtual resources.

In **Platform-as-a-Service** (PaaS), is an archetype for distributing operating systems and associated services. This layer contains application frameworks that form the basis of the SaaS layer.

In **Software-as-a-Service** (SaaS)**,** or a software distribution model has applications that are distributed by a service provider or vendor and made available to subscribers over the Internet.

In **Security-as-a-Service** (SaaS), core security services are provided to the client while exchanging the data over the Internet.

DOI 10.17148/IJARCCE.2016.5273

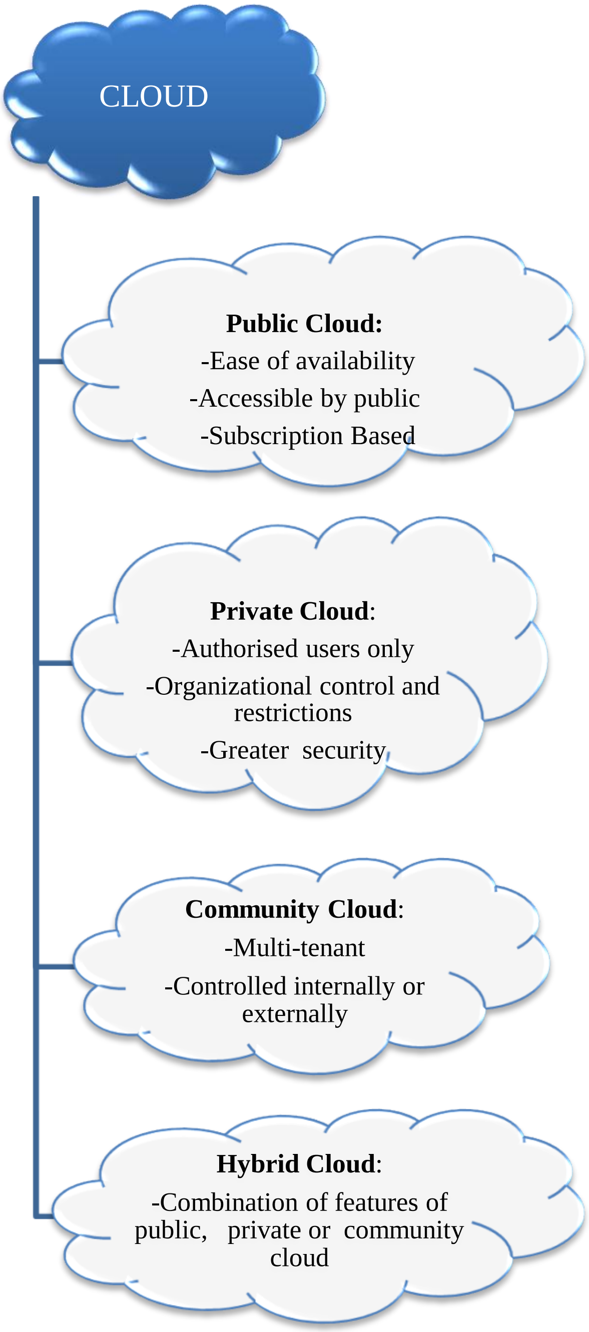

Fig. 1 Cloud Deployment Models

Figure 2 depicts the various Cloud Service Models.

In this paper, we emphasize on the importance of TPA and homomorphic tokens, which is applicable to the above service and deployment models and which can be used to provide better security services for data storage.

The various sections covered in this paper are as follows: Section II mentions about Security as a Major Challenge, Section III talks about the Related Works, Section IV gives us the Conclusion followed by References.

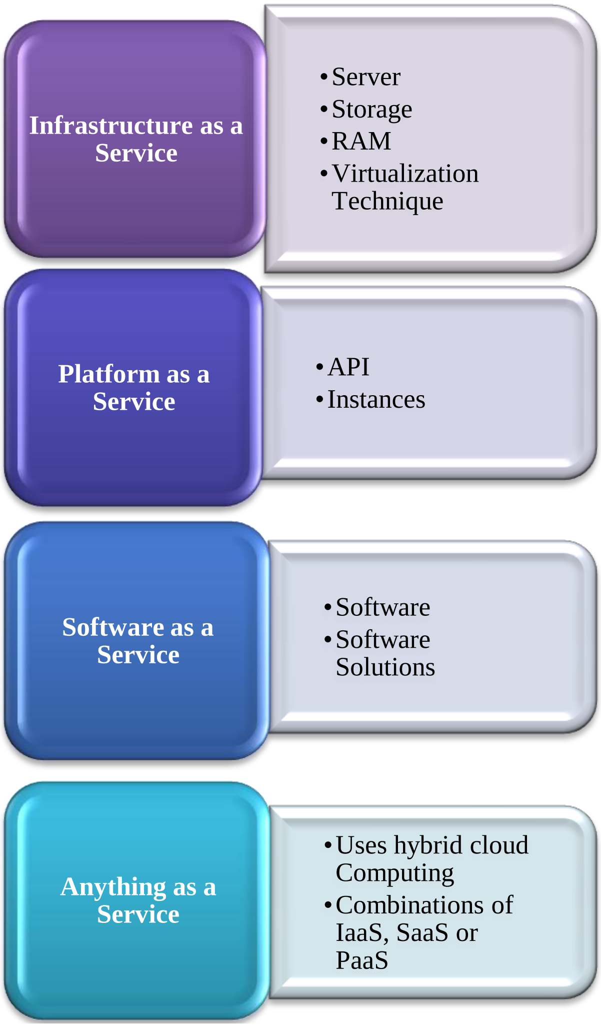

Fig. 2 Cloud Service Models

II. SECURITY AS A MAJOR CHALLENGE

Security is the major challenge in cloud [7]. The user is entirely dependent on the Cloud Service Provider to secure his data. However the user is unaware of where exactly that data is being stored. The CSP also cannot be trusted entirely. If the CSP fails to provide the desired services, they might try to cover it up by misinforming the user. Then the user will not know whether his data has been properly stored and secured. The issue of security can further be divided into issues like –

Data Integrity- Normally, the cloud user should be able to derive his original data in the same way that he had stored. It is to be noted that the cloud not only acts like a data warehouse but should also be capable of maintaining the integrity whenever any changes are made to it.

Data Intrusion- This is the second major issue in security which occurs when intruder or an unauthorized person has access to the user’s account and his files and is capable of making any changes to the data.

Service Availability- Before the user is given the opportunity to use the cloud, the user would have to agree

DOI 10.17148/IJARCCE.2016.5273

to some terms and conditions regarding the services offered by the cloud. There may be situations where the user may be unable to utilize some services when needed and when he has to urgently access the data in the cloud through those services. Since all the data is stored off-premise, the user might be unable to access that data, resulting in a loss.

Confidentiality- Several encryption techniques have been used to encrypt the data that is stored in the cloud. The CSP should guarantee the user that the data will not shared with anybody else no matter what, to maintain the confidentiality of the data.

Non-Repudiation- Mainly used for email, contracts and digital signatures, this assures the communication of messages between groups and assurance that which cannot be refused. It does not guarantee the genuineness of the message.

Service Oriented Architecture [8] – Here we can combine various services to create applications in various ways. WS- SecurityPolicy, WS- SecureConversation and WS- Trust are some of the several Web Services standards which rely on security features of SOA.

Service Level Agreement [9] – It provides information between client and Cloud Service Provider, about responsibilities, services, warranties, priorities and guarantees.

Figure 3 depicts the various Security Challenges in cloud.

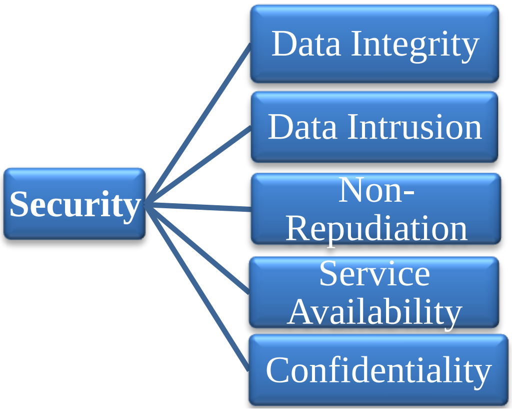

Fig. 3 Security Challenges in Cloud

III. RELATED WORKS

From [10]-[19], the importance of TPA (Third Party Auditor), to audit user data has been mentioned. In [10], Maulik Dave et al, have mentioned the security issues that arise- like user authentication, SLA, data storage, open source provision, virtual infrastructure and resource request. The importance of TPA [11] has been stressed upon. In [12], Rakhi Bhardwaj et al, the dependency of Cloud Service Provider (CSP) [13] on TPA and the reason why the user cannot entirely trust the CSP have been specified. In [14], Gaurav Pachauri et al, the problem of Public Auditability and Dynamic Data Operations which are not solved by Provable Data Possession (PDP) [15] and Proof of Retrievability (POR) [16], have been solved to some extent by TPA. In [17], Mehul Shah et al, the privacy preserving protocol is our main scheme like TPA. In [18], Niyamat Ujloomwale et al, has proposed that the TPA uses technique of data correctness, to assure that the data in cloud is being stored securely. In [19], Giuseppe Ateniese et al, allows a cloud user who has kept his data at a dubious server to verify the server which possess the original data, without retrieving it.

From [20]-[26], the benefits of using homomorphic tokens to identify the faulty server. In [20], Nikitha Pathrabe et al, have mentioned about the homomorphic token and its properties based on Universal Hash Function [21]. By using this, the problem of data correctness and identification of misbehaving servers can be solved. In [22], Hemant Dhole, et al, the homomorphic encryption algorithm has been referred to. In [23], Manasi Doshi et al, the data error location can be identified by allotting tokens to the data which has been divided into fixed blocks. In [24], Cong Wang et al, the importance of Correction verification and error localization using challenge response protocol has been given. In [25], Kevin Bowers et al, HAIL (High Availability and Integrity Layer) manages file integrity and availability across servers by making use of POR as building blocks by which storage resources can be tested and re-allocated and failures are detected. In [26], Kalpana Batra et al, the importance of authentication and authorization to access files and make dynamic changes to them has been mentioned.

In [27] and [28], the protection of data through encryption and OTP has been mentioned. In [27], Rupali Sachin Vairagade et al, the technique of using encryption algorithm like RC4 and CRC for password generation and file encryption is being proposed. In [28], S.A. Gade, the technique of One Time Password (OTP) can be used to solve the problem of Byzantine failure.

Table 1 depicts the different schemes supporting different features in cloud security with a tick mark in their respective cells in the table.

TABLE I: DIFFERENT SCHEMES SUPPORTING DIFFERENT FEATURES IN CLOUD SECURITY

Reference Numbers	TPA	Homomorphic Token	Others
[10]	✓		✓
[11]	✓		
[12]	✓		
[13]	✓		
[14]	✓		
[15]	✓		
[16]	✓		
[17]	✓		
[18]	✓		
[19]		✓	

[20]		✓	
[21]		✓	
[22]		✓	
[23]		✓	
[24]		✓	✓
[25]		✓	
[26]		✓	✓
[27]			✓
[28]			✓

From Table 1, we observe that [24] and [26] are providing solutions through Homomorphic Token and Encryption Algorithms, OTP respectively.

Table 2 gives an overall picture of the problems discussed and solved, with a tick mark in their respective cells in the table.

TABLE II: OVERALL PICTURE OF THE PROBLEMS DISCUSSED AND SOLVED

Reference Numbers	**General**	**Byzantine Failure**	**Unauthorized User**	**Server Colluding Attacks**
[10]	✓		✓	
[11]	✓			
[12]	✓			
[13]	✓			
[14]			✓	
[15]			✓	
[16]		✓		
[17]			✓	
[18]			✓	
[19]			✓	✓
[20]		✓		✓
[21]		✓		✓
[22]		✓		
[23]		✓		
[24]		✓	✓	✓
[25]		✓		
[26]			✓	
[27]	✓			
[28]	✓		✓	

From Table 2, we observe that [24] is solving the problems of Byzantine Failure, Unauthorized User and Server Colluding Attacks.

IV. CONCLUSION

In this paper, we have examined the problems of data security in cloud data storage. The mechanism of using homomorphic token combined with distributed verification of erasure-coded data can be used to achieve the integration of storage correctness, data error localization and to identify misbehaving servers.

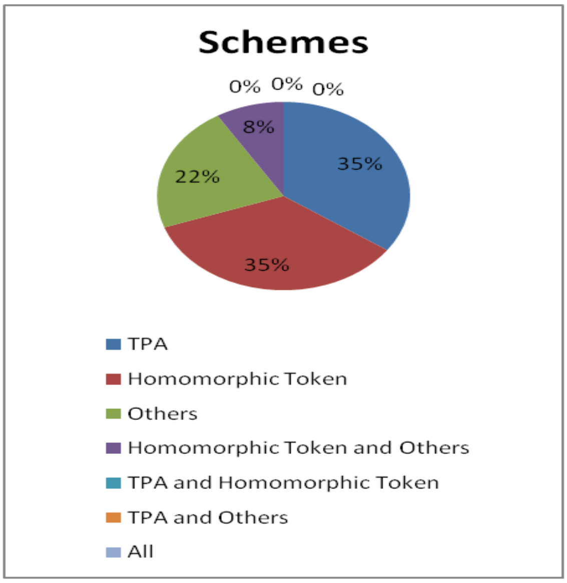

Fig. 4 Pie chart representation of various schemes and their features

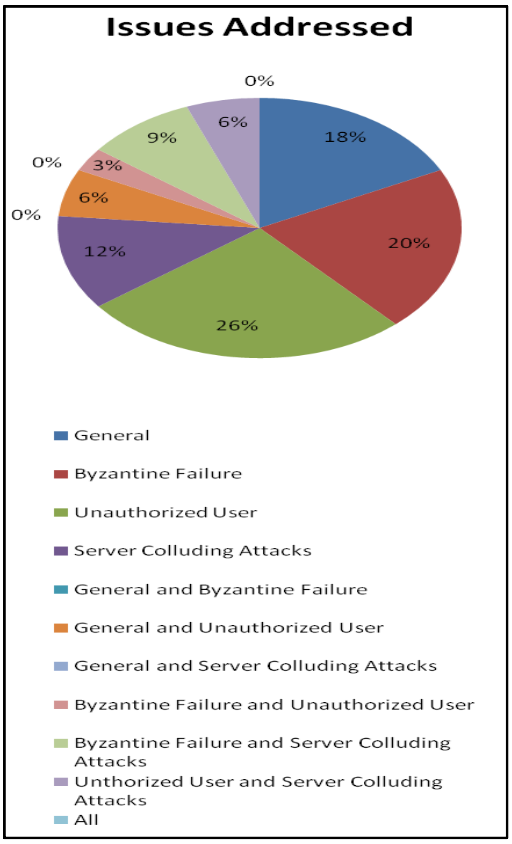

Fig. 5 Pie chart representation of various issues addressed in the references

DOI 10.17148/IJARCCE.2016.5273

By conducting proper investigation in all these techniques, the problems of Byzantine failure, unauthorized data modification attacks and server colluding attacks can be solved to a major extent. This field is still in its infancy stage and many researches are yet to be identified and carried out with respect to it.

From Figure 4, it can be observed that TPA and Homomorphic Tokens contribute to 70% solution to the security problems. If they are combined with other techniques like Encryption algorithms or OTP, then 92% of the problem can be solved. From Figure 4 and Figure 5, if the techniques in [24] are combined with the ones from [10]-[13], then we can solve general problems theoretically. This can then be implemented practically in the future.

ACKNOWLEDGEMENT

We would like to sincerely thank our college faculty and management for giving us the opportunity and resources to complete the paper. A special thanks to Mr. M. Raja Krishna Kumar, for guiding and supporting us throughout.

REFERENCES

[1] John W. Rittinghouse and James F. Ransome, "Cloud Computing – Implementation, Management and Security" Edition 1 CRC Press ISBN 978-1-4398-0680-7.

[2] S. Sajithabanu, E. George Prakash Raj – "Data Storage Security in Cloud", IJEST VOL. 2 Issue 4, Oct-Dec. 2011.

[3] Chun-Ting Huang, Lei Huangy, Zhongyuan Qinz, Hang Yuan, Lan Zhoux, Vijay Varadharajan and C.C. Jay Kuo – "Survey on Securing Data Storage in the Cloud", January 2014.

[4] Tharam Dillon, Chen Wu and Elizabeth Chang – "Cloud Computing: Issues and Challenges", IEEE 2010, Perth, Australia, Apr. 20, 2010 to Apr. 23, 2010, ISBN: 978-0-7695-4018-4

[5] Shivangi Goyal –"A Comparative Study of Cloud Computing Service Provider", Vol. 2 Issue 2 Feb 2012.

[6] Gaurav Pachauri, Subhash Chand Gupta – "Ensuring Data Integrity in Cloud Data Storage", ISSN 2348 – 7968, Vol. 1 Issue 3, May 2014.

[7] "A Survey on Data Security in Cloud Computing: Issues and Mitigation Techniques" - Satarupa Biswas, Abhishek Majumder. IJRET, eISSN: 2319-1163 | pISSN: 2321-7308

[8] John W. Rittenhouse and James F. Ransome, "Cloud Computing – Implementation, Management and Security" Edition 1 CRC Press, ISBN 978-1-4398-0680-7.

[9] David S. Linthicum, "Cloud Computing and SOA Convergence in your Enterprise" ISBN – 13:978-0-13-600522-1, 2009, Addison-Wesley Information Technology Series

[10] Maulik Dave – "Data Storage Security in Cloud Computing: A survey", Volume 3, Issue 10, October 2013 ISSN: 2277 6451.

[11] Nupoor M. Yawale, Prof. V. B. Gadichha – "Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm", Volume 3, Issue 11, November 2013 ISSN: 2277 6451.

[12] Rakhi Bhardwaj, Vikas Maral – "Dynamic Data Storage Auditing Services in Cloud Computing", IJEAT ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[13] Ashish Bhagat Ravi Kant Sahu, "Using Third Party Auditor for Cloud Data Security: A Review", Volume 3, Issue 3, March 2013 ISSN: 2277 6451.

[14] Gaurav Pachauri1, Subhash Chand Gupta – "Ensuring Data Integrity in Cloud Data Storage", ISSN 2348 – 7968, Vol. 1 Issue 3, May 2014.

[15] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song – "Provable Data Possession at Untrusted Stores", CCS 2007, 14th ACM conference on Computer and Communications Security, ISBN: 978-1-59593-703-2.

[16] Hovav Shacham, Brent Waters – "Compact Proofs of Retrievability", 14th International Conference on Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. 978-3-540-89255-7

[17] Mehul A. Shah, Mary Baker, Jeffrey C. Mogul, Ram Swaminathan – "Auditing to Keep Online Storage Services Honest", (HP Labs, Palo Alto), Conference: Proceedings of HotOS'07: 11th Workshop on Hot Topics in Operating Systems, May 7-9, 2005, San Diego, California, USA doi=10.1.1.148.4139.

[18] Mrs. Niyamat Ujloomwale, Mrs. Ranjana Badre – "Data storage security in Cloud", Volume 16, Issue 6, Ver. III (Nov – Dec. 2014).

[19] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, Dawn Song – "Provable Data Possession at Untrusted Stores", CCS 2007, 14th ACM conference on Computer and Communications Security, ISBN: 978-1-59593-703-2.

[20] Nikita Pathrabe, Deepali Khtawar – "Ensuring Data Storage Security in Cloud Computing", Vol.2, No.2, February 2014 E-ISSN: 2321-9637.

[21] J. Lawrence Carter and Mark N. Wegman – "Universal Classes of Hash Functions" - Received August 8, 1977; revised August 10, 1978.

[22] Hemant T. Dhole, Praful C. Papade and Sachin B. Bhosale – "Ensuring Data Storage Security using Cloud Computing", Volume 2, Issue 1, January 2014.

[23] Manasi Doshi Swapnaja Hiray – "Secure and Data Dynamics Storage Services on Cloud", Volume 3, Issue 11, November 2013

[24] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou – "Ensuring Data Storage Security in Cloud Computing", Quality of Service, 2009 17th International Workshop, E-ISBN: 978-1-4244-3876-1

[25] Kevin D. Bowers, Ari Juels, Alina Oprea – "HAIL: A High-Availability and Integrity Layer for Cloud Storage", Proceedings of the 16th ACM conference on Computer and communications security, 2009,ISBN: 978-1-60558-784-4

[26] Kalpana Batra, Ch. Sunitha, Sushil Kumar – "An Effective Data Storage Security Scheme for Cloud Computing", Vol. 1, Issue 4, June 2013.

[27] Rupali Sachin Vairagde and Nitin Ashokrao Vairagde – "Cloud Computing Data Storage and Security Enhancement", IJARCET, 2012.

[28] Prof. S.A.Gade, Mukesh P.Patil, Ganesh D. Bagul – "Security for Data Storage in Cloud Computing", October 2015, IJESRT, ISSN: 2277-9655.

BIOGRAPHY

Sneha S. Bhandarkar is a final year undergraduate student belonging to the Department of Computer Science and Engineering from Geethanjali College of Engineering and Technology, Hyderabad.

Buri Chanukya is a final year undergraduate student belonging to the Department of Computer Science and Engineering from Geethanjali College of Engineering and Technology, Hyderabad.

Sandhya Rani is a final year undergraduate student belonging to the Department of Computer Science and Engineering from Geethanjali College of Engineering and Technology, Hyderabad.

Mr. Y. V. N. Phani Kishore is currently working as an Assistant Professor, Department of Computer Science and Engineering at Geethanjali College of Engineering and Technology, Hyderabad. He is having 1+ years of teaching experience. He has played a key role in rolling out Common Service Centers in India in collaboration with DeitY, GOI.

DOI 10.17148/IJARCCE.2016.5273