IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Data Integrity and Performance Comparison of New Type- Based Proxy Re-encryption (TB-PRE) and Provable Data Possession (PDP) in Mobile Cloud Computing

Ankit Chamoli[1*], Anshika Goyal [2]

[1]Computer Science and Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India
[2]Computer Science and Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India

[*]Corresponding Author: ankitchamoli66@gmail.com, Tel.: +91-75792-15035

Available online at: www.ijcseonline.org

Accepted: 17/May/2018, Published: 31/May/2018

Abstract— Cloud computing gives shared pool of assets (computers resources like networks, server and storage) on the demand of the user in ubiquitous and simple way that can be provisioned to the user with a very little management effort. The basic concept of cloud computing can be understood by the following definition according to NIST. It can be concluded from the above discussions that the demands required by the user are fulfilled by the cloud computing. These demands include both hardware and software resources which are present on the internet. A shared pool of resources is provided by the cloud computing provider which can be accessed by the users as per their demands. The users subscribe as per their requirements and access the resources until it wants to. Virtualization is the technique which helps in providing such services and also in reducing the cost of implementation and also adding hardware parts which will help in meeting the requirements of the user. The PDPT and NTBPRET are the techniques which ensure the data integrity.

Keywords— Mobile cloud computing, secure data distribution, data integrity, access control, proxy re-encryption.

I. Introduction

An on-demand and ease of access of network is provided by the cloud computing environment to its users. The computing resources are provided to the users such as storage, servers, applications, networks etc. The data that is stored in centralized data known as cloud is retrieved and modified by the users. Cloud Service Provider (CSP) is designed for giving users the services on the basis of their demands. The services required by the users are to be paid for being served. A system which offers an enormous amount of functions underneath different topologies and every topology provides some new specialized services.

A main dilemma exists is that any consumer can access any other consumer's data without the understanding of other consumer. At this instant the problem occurs that how we avoid these types of issues. Standard enterprise security (such as firewall, antivirus and IDPS) is adopted by organizations to ensure the security for cloud computing. As the defence against the malicious services or services like identify frauds, almost all service provider organizations use the access control and user authentication mechanisms. The best feature mostly cloud service providers are providing is user can access the cloud from anywhere in the world. To protect the consumer data, ventures employ the security system, for instance USB port control Full Disk Encryption (FDE). But, these methods are fined sufficient to secure the consumer data in cloud? The machines which runs 24*7 or else the entire time the above elucidations are not effectual that much. It cannot avoid the attackers to access data.

The strategy of centralizing storage, processing, bandwidth and memory help in providing more effective computing in cloud computing. Figure 1.1 overview and is showing the environment of cloud computing.

CLOUD
COMPUTING

Figure1.1: Cloud Computing Environment

Data integrity in Cloud Computing:
The data and computation are outsourced to a remote server; the data integrity has to be preserved and verified regularly in order to demonstrate that data and computation are undamaged. Data integrity implies that data must be reserved as of unauthorized alteration. Every alteration to the data must be identified [5], [6].

After the introduction in Section I the rest of this dissertation is organized as follows: Section II contains the related work, section III explains the methodology with flow chart, Section VI describes results and discussion, Section V concludes research work with future directions.

II. RELATED WORK

Anchal Srivastava, et.al in 2014 [7], Explained that in order to ensure the data integrity within storage outsourcing, the Cooperative Provable data possession (CPDP) is applied. The construction of an efficient CPDP scheme and dynamic audit service is addressed for distributed cloud storage. Further, the scenario which provides scalability of service and data migration can be presented with the help of entrusted and outsourced storage which is ensured through the utilization of hash index hierarchy and holomorphic verifiable response within CDDP. On the basis of zero-knowledge proof system the security of the system is proved. In order to enhance the performance of the system and minimize the cost of client and the cloud storage providers, various optimal parameters are involved within this system. A cooperative provable data possession method is to be presented through these enhancements which thus ensure integrity and availability of the method.

Preeti Siroh et.al (2015) presented in this paper [8] presented that data security is well thought-out as the regular concern driving to a drawback in the acceptance of distributed computing. Data integrity, privacy and conviction concerns are couple of serious security concerns prompting broad acceptance of distributed computing. The dawn of the suggested representation has adequate services and abilities which guarantees the data integrity and security. The proposed agenda concentrates on the encryption and decryption move toward encouraging the cloud client with data security guarantee. The proposed elucidation just discusses the improved security yet do not discuss the performance. The elucidation additionally incorporates the performance of malware detection, forensic virtual machine and constant observing of a framework. In this manuscript, a study of various security concerns and risks is likewise presented. A data security agenda likewise gives the clearness to mutually the cloud service provider and the cloud consumer in this way dropping data security risks into cloud condition. The anticipated representation is connected particular towards the data security in the entire the three levels of the cloud services which be recommended to the cloud consumer through the cloud provider.

Xuefeng Liu, et.al in 2017 [9] presented that a study related to the integrity auditing problems arising within the storage of cloud de-duplication process. This paper not only ensures the confidentiality of outsourced data but also helps in ensuring the integrity of this storage. Without using any additional proxy server, a novel message-locked integrity auditing method is proposed in this paper. This method can be applied within the file-levels and chunk-levels of these systems. As this method helps in enabling integrity tag de-duplication along with the elimination of the cipher-text redundancy, this method is known to be storage efficient. A message-derived signing key is used to help in ensure integrity of the data which helps in causing least client-side computation overhead within these systems. Within the Computational Diffie-Hellman (CDH) assumption, the information related to data ownership is not disclosed and kept secure. The evaluation of performance of proposed method is done with the help of conducting various experiments and the effectiveness and efficiency of this method is ensured on the basis of results achieved.

Andrey N. Rukavitsyn, et.al in 2017 [10] presented that there is complete access provided to the consumer’s data to the cloud providers. This can result in compromising the integrity of data as all the users can access it easily. Active techniques of giving security consider techniques to enhance the haste and decrease the heap amid authorization and data encryption. It explains the utilization of partitioned facilities remote the cloud for authentication, data administration and metadata stockpiling to eradicate the likelihood of getting unapproved permission to data, and the utilization of metadata to achieve integrity control. The expanded technique is being utilized to make a rise in light of Open Stack and two facilities on isolated servers. Database of owner limits the entrance to stored data in an encrypted frame and provider does not able to connect with database. Unpredictability of the encryption algorithm and utilization of techniques of data handling in distributed computing will enable improvement of data security and hacking confrontation. Moreover, it is relatively not possible to concession data because of confirmation of checksums accumulated by the assessor.

III. METHODOLOGY

In recent years, electronic technologies have gained lots of development but still smart phones are weak compared to desktops devices in terms of computational capability, storage etc. The mobile user’s demands are getting increased day by day and an existing technology is not able to meet it. The two mobile computing and cloud computing has been integrated to make a new mobile cloud computing (MCC) that have extended a boundary of the mobile applications.

The data privacy and data integrity like different challenges of cloud computing has also been inherited in new scheme. A new type-based proxy re-encryption like several cryptographic primitives has been used by authors to design a secure and efficient data distribution system in MCC that is able to provide data privacy, data integrity, data authentication, and flexible data distribution with access control.

They have used MIRACL Crypto SDK to conduct a proof-concept-implementation of their data distribution system. In their TB-PRE scheme they have chosen a Barreto-Naehrig (BN) curve over base field Fp-256 along with BLS signature for 128-bit security. The hash function and symmetric encryption algorithm has been used for 128 bit security as both AES and SHA-256 are implemented in the MIRACL Crypto SDK. They have used platform of C++ for their code and run it on single computer to examine the computation overhead of our data distribution system in a better way that also avoid influence of the bandwidth. The movement of files between the data owner's/consumer's foldersand the cloud's folder is the uploading and downloading operations. The computer in the simulation runs Linux Ubuntu 12.04 system, and equips a 2.83 GHz Intel Core2 CPU and 4GB memory.

The proposed system has been compared with existing traditional cloud based storage systems and its results show that it is a lightweight, easily deployable solution for present mobile users in MCC. In order to perform all cryptographic operations there is only need to keep short secret keys consisting of three group elements as no trusted third party is involved in it. An extensive performance analysis and a proof-of-concept implementation show that their data distribution is practical.

Type based proxy re encryption Technique (TBPRE):

A single-hop unidirectional TB-PRE scheme consists of the following algorithms [12], [13], [26]:

- **Setup (1*k*):** Taking a security parameter 1*k* as input, the setup algorithm outputs a public parameter *param*, which specifies the plaintext space *P* and the type space *T.*
- **KeyGen (*param; i*):** Taking a parameter *param* and a user identity *i* as inputs, the key generation algorithm outputs a pair of public key and secret key (*pki; ski*) for user *i*.
- **ReKeyGen(*ski; pkj ; t*)**: Taking a secret key *ski* of user *i*, a public key *pkj* of user *j*, and a type *t 2 T* as inputs, the re-encryption key generation algorithm outputs a unidirectional re-encryption key $rk_{i->j}$;*t*.
- **Enc (*pki; t; m*):** Taking a public key *pki* of user *i*, a type *t 2 T* and a message *m 2 P* as inputs, the encryption algorithm outputs a ciphertext *Ci*.
- **ReEnc (*rk*$_{i->j}$*; t; Ci*):** Taking a re-encryption key $rk_{i->j}$;*t* and a ciphertext *Ci* under *pki* as inputs, the re-encryption algorithm outputs a re-encrypted ciphertext *Cj* under *pkj* .

Dec (*ski; Ci*): Taking a secret key *ski* of user *i*, and a ciphertext *Ci* under *pki* as inputs, the decryption algorithm outputs a message *m ϵ P* or an error symbol _|_ indicating the failure of the decryption.

Provable Data Possession (PDP):

It refers to a method that assures a data integrity over distant server. In this a consumer is able to validate that server acquires the original data without retrieving it. If data is stored at an unfaithful server. A metadata is generated through processing information file by data owner to store it locally [11], [27]. The native copy of the file is deleted after it being sent to the server and challenge response protocol is used by owner to verify a possession of file. Ateniese et al. are think about public audit ability in their described "provable data possession" model designed for guarantee possession of files on unfaithful storages. This is a procedure employed by consumers to ensure the data integrity and periodically verify their data stored on the cloud server.

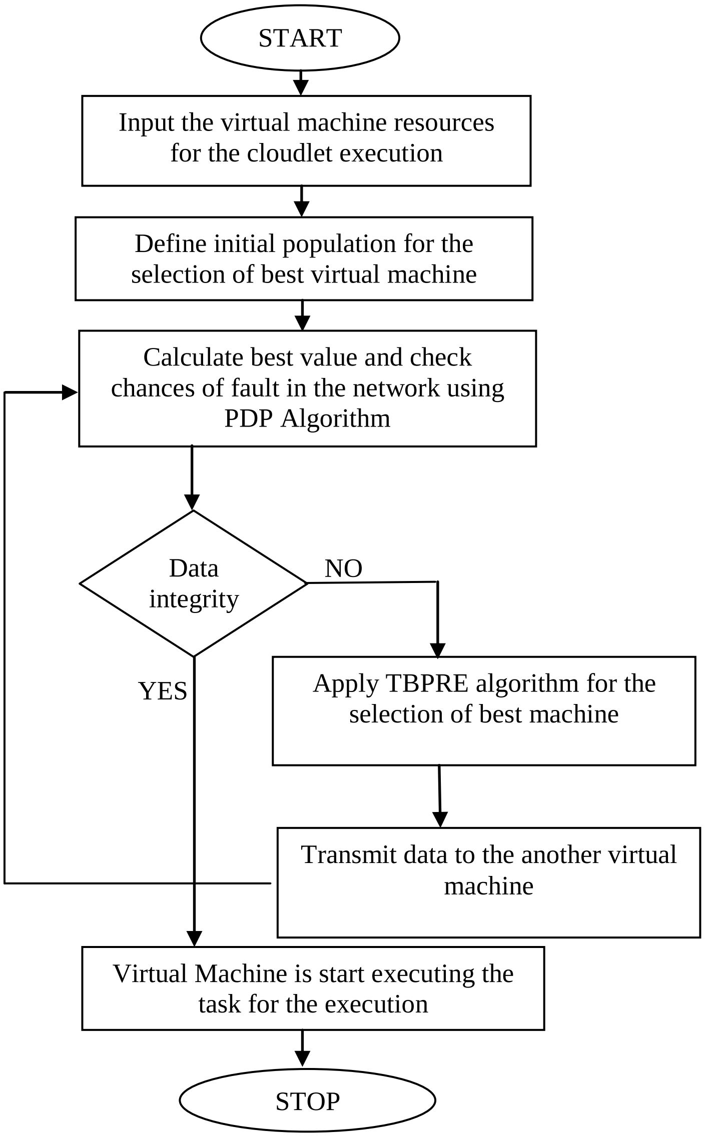

START
Input the virtual machine resources for the cloudlet execution
Define initial population for the selection of best virtual machine
Calculate best value and check chances of fault in the network using PDP Algorithm
Data integrity
NO
YES
Apply TBPRE algorithm for the selection of best machine
Transmit data to the another virtual machine
Virtual Machine is start executing the task for the execution
STOP

Fig 3.1 Flow Chart of TBPRE

IV. Results and Discussion

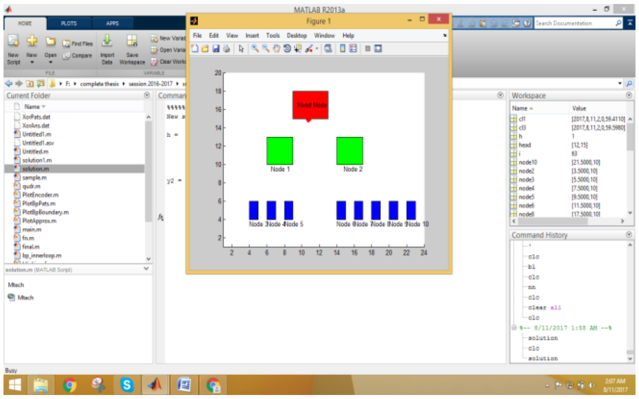
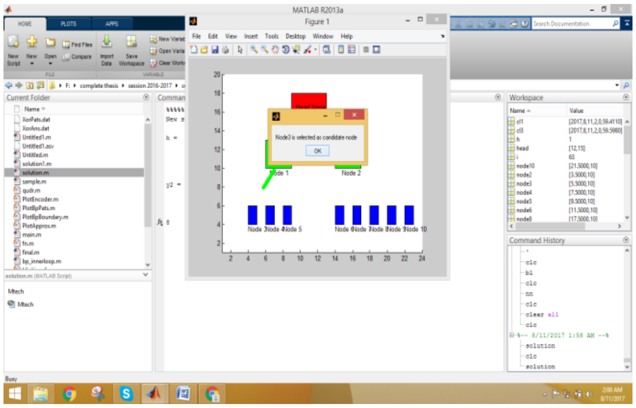


Fig 4.1: Deployment of the network

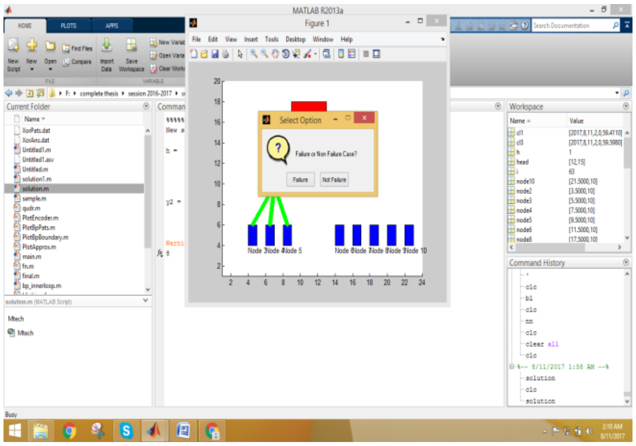
As shown in figure 4.1, the cloud network is deployed with the finite number of virtual machines. In the network the cloud server is responsible to assign the task to the virtual machines for the execution.



Node3 is selected as candidate node

Fig 4.2: Task assignment

As shown in figure 4.2, the TBPRE algorithm is applied which will assign the task to the most reliable nodes in the network. The most reliable node is selected on the basis of execution time and failure rate in the network.



Failure or Non Failure Case?

Fig 4.3: Execution of condition

As shown in figure 4.3, the condition is executed which is based on failure and non-failure conditions. The failure condition is executed when task need to assign from one virtual machine to another.

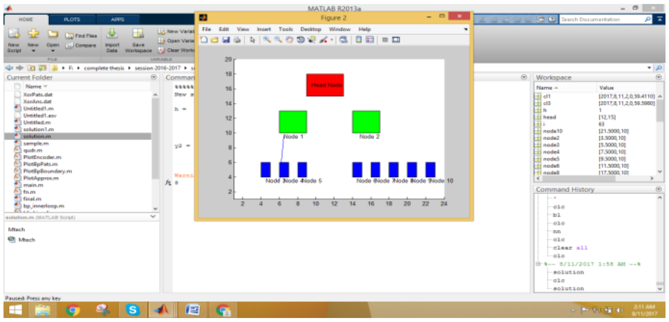
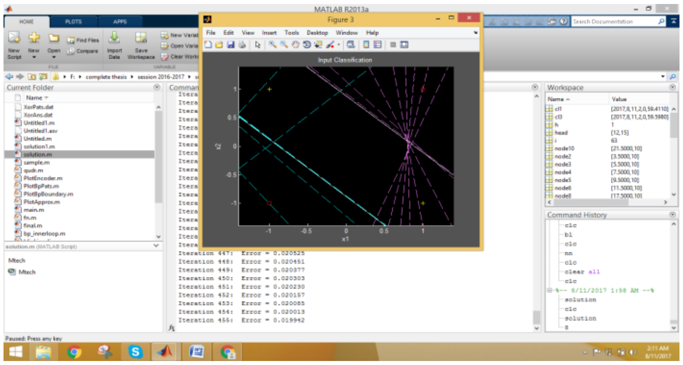


Fig 4.4: Machine overloading condition

As shown in figure 4.4, the machine which is overloaded will not revert back the cloud service provider. The machine when not revert for the 10 seconds will be considered as the overloaded machine.



```
Iteration 447:  Error = 0.020525
Iteration 448:  Error = 0.020451
Iteration 449:  Error = 0.020377
Iteration 450:  Error = 0.020303
Iteration 451:  Error = 0.020230
Iteration 452:  Error = 0.020157
Iteration 453:  Error = 0.020085
Iteration 454:  Error = 0.020013
Iteration 455:  Error = 0.019942
```

Fig 4.5: Execution of TB-PRE algorithm

As shown in figure 4.5, the TB-PRE algorithm will be executed which will re-assign the task to another virtual machine. The second virtual machine will be the most reliable virtual machine for the task execution.

GRAPHICAL COMPARISON OF PDP AND TBPRE:

In this chapter, the graphical results of the provable data possession (PDP) and new type based proxy re- encryption (TBPRE) techniques are discussed.

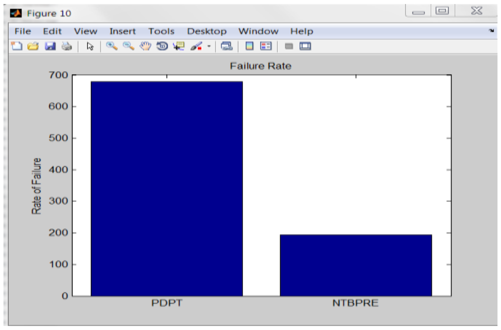


Fig 4.6: Failure Rate of PDPT and NTBPRE

As shown in figure 4.6, the performance of the PDPT and NTBPRE is shown and it has been analyzed that failure rate of TBPRE is less.

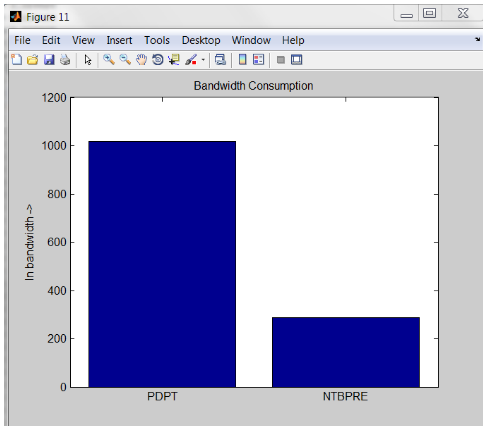


Fig 4.7: Bandwidth Consumption of PDPT and NTBPRE

As shown in figure 4.7, the performance of the PDPT and NTBPRE is shown and it has been analyzed that bandwidth consumption of NTBPRE is less.

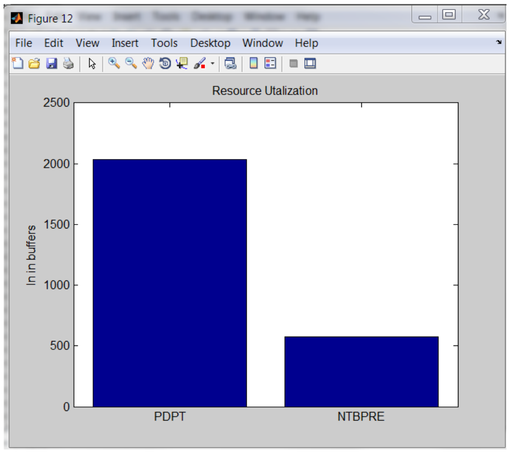


Fig 4.8: Resource Utilization of PDPT and NTBPRE

As shown in figure 4.8, the performance of the PDPT and NTBPRE is shown and it has been analyzed that resource utilization of NTBPRE is less.

QUALITATIVE COMPARISON:

PARAMETER	**PDP**	**TBPRE**
Technique used for Data integrity	Key Generation algorithm.	Key Generation algorithm.
Dynamic support	No Dynamic support such as insertion, deletion, modification and updation functions are not allowed.	Yes Dynamic support such as insertion, deletion, modification and updation functions are allowed.
Computation power	It requires low computation power.	It requires more computation power.
Data support	This Technique is only applicable for the static data only.	This Technique is applicable for both the static and dynamic data.
Error correction	Lack of error-correcting codes to address.	As same as PDP, Lack of error-correcting codes to address.
Client support	Not suitable for thin client.	As same as PDP, Not suitable for thin client.
Throughput	Low Throughput.	High Throughput.

Table 1: Qualitative comparison

V. Conclusion and Future Scope

In this work, it has been concluded that Cloud computing gives shared pool of assets (computers resources like networks, server and storage) on the demand of the user in ubiquitous and simple way that can be provisioned to the user with a very little management effort. It can be concluded from the above discussions that the demands required by the user are fulfilled by the cloud computing. These demands include both hardware and software resources which are present on the internet. Many algorithms are proposed for data integrity such as PDP, PoR, and HAIL. In this research work, new type based proxy re-encryption technique (TBPRE) and provable data possession technique (PDP) has been compared on these parameters i.e. Failure rate, Bandwidth Consumption and Resource Utilization. From Fig 4.6, Fig 4.7 and Fig 4.8 it is concluded that the TBPRE is more efficient than the PDP. In this research work, the PDP and TBPRE techniques are implemented which ensure data integrity in the network. Following are the various future possibilities, In future; NTBPRE technique will be further improved using the SHA algorithm to increase security of the cloud networks. The proposed improvement will be compared with other algorithms to check its reliability.

References

[1] Shui Han, Jianchuan Xing, “Ensuring Data Storage Through A Novel Third Party Auditor Scheme in Cloud Computing” , 2011, IEEE computer science & Technology, pp 264-268.

[2] Bhavna Makhija, VinitKumar Gupta, “Enhanced Data Security in Cloud Computing with Third Party Auditor”, 2013, International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345

[3] Sultan Aldossary, William Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions”, (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, pp. 485-492, 2016.

[4] Saranya Eswaran, Dr. Sunitha Abburu, “Identifying Data Integrity in the Cloud Storage”, IJCSI International Journal of Computer Science Issues, vol. 9, pp. 403-408, 2012.

[5] Gaurav Pachauri, Subhash Chand Gupta, “ENSURING DATA INTEGRITY IN CLOUD DATA STORAGE”, IJCSNS International Journal of Computer Science and Network Security, vol. 14, pp. 34-38, 2014.

[6] S. P. Jaikar, M. V. Nimbalkar, “Verifying Data Integrity in Cloud”, International Journal of Applied Information Systems (IJAIS), vol. 3, pp. 38-46, 2012.

[7] Anchal Srivastava, Ashutosh sehgal, Vikas Kumar Singh, Nitish Kumar Bose, “Provable data possession for integrity verification”, 2014, International Refereed Journal of Engineering and Science (IRJES), Volume 3, Issue 4

[8] Preeti Siroh and Amit Agarwal, “Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust”, 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015)

[9] Xuefeng Liu, Wenhai Sun, Wenjing Lou, Qingqi Pei, Yuqing Zhang, “One-tag Checker: Message-locked Integrity Auditing on Encrypted Cloud Deduplication Storage”, IEEE INFOCOM 2017 - IEEE Conference on Computer Communications

[10] Andrey N. Rukavitsyn, Konstantin A. Borisenko, Ivan I. Holod, Andrey V. Shorov, “The Method of Ensuring Confidentiality and Integrity Data in Cloud Computing”, 2017, IEEE

[11] G. Ateniese, R. D. Pietro, L. V. Mancini, G. Tsudik, “Scalable and Efficient Provable Data Possession”, in Proceedings of SecureComm, vol. 2, pp. 23-28, 2008.

[12] Benoˆıt Libert and Damien Vergnaud. Unidirectional chosenciphertext secure proxy re-encryption. *Information Theory, IEEE Transactions on*, 57(3):1786 –1802, march 2011.

[13] Qiang Tang. Type-based proxy re-encryption and its construction. In DipanwitaRoy Chowdhury, Vincent Rijmen, and Abhijit Das,editors, *Progress in Cryptology - INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 130–144. Springer Berlin Heidelberg, 2008.

[14] Parsi, K., & M.Laharika, “A Comparative Study of Different Deployment Models in a Cloud”, 2013, International Journal of Advanced Research in Computer Science and Software Engineering , 3 (5), 512-515.

[15] Srinivas.J, K. Venkata Subba Reddy, Dr. A. Moiz Qyser, “Cloud Computing Basics”, 2012, International journal of advanced research in computer and communication engineering , pp. 343-347

[16] Seyyed Mansur Hosseini and Mostafa Ghobaei Arani,” Fault-Tolerance Techniques in Cloud Storage: A Survey”, 2015, International Journal of Database Theory and Application, Vol.8, No.4 (2015), pp.183-190

[17] SookKyong Choi, KwangSik Chung, Heonchang Yu,” Fault tolerance and QoS scheduling using CAN in mobile social cloud computing”, 2013, Springer Science+Business Media New York

[18] Dr. Lakshmi Prasad Saikia, Yumnam Langlen Devi,” FAULT TOLEREANE TECHNIQUES AND ALGORITHMS IN CLOUD COMPUTING”, International Journal of Computer Science & Communication Networks, Vol 4(1),01-08

[19] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, “Provable Data Possession at Untrusted Stores”, in Proceedings of 14th ACM Conf. Computer and Comm, Security (CCS ’07), vol. 5, pp. 231-238, 2007.

[20] MS. R. K. Pandya, prof. K. K. Sutaria, “Data integrity techniques in cloud: an analysis”, journal of information, knowledge and research in computer engineering”, vol. 2, pp. 413-417, 2012.

[21] Soumya Ray and Ajanta De Sarkar, “Execution Analysis of Load Balancing Algorithm in Cloud computing Environment”, International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.5, October 2012

[22] Sanjoli Singla, Jasmeet Singh, 2013 “Cloud Data Security using Authentication and Encryption Technique” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235

[23] Tushar Desai, Jignesh Prajapati, “A Survey of Various Load Balancing Techniques and Challenges in Cloud Computing”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 11, NOVEMBER 2013

[24] Vimmi Pandey, “Securing the Cloud Environment Using OTP” International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4, 2013

[25] Anandita Singh Thakur, P.K. Gupta, and Punit Gupta, “Handling Data Integrity Issue in SaaS Cloud”, 2014, Proc. of the 3rd Int. Conf. on Front. of Intell. Comput. (FICTA) 127– Vol. 2, Advances in Intelligent Systems and Computing

[26] Jiang Zhang, Zhenfeng Zhang, Hui Guo. "Towards Secure Data Distribution Systems in Mobile Cloud Computing", IEEE Transactions on Mobile Computing, 2017

[27] RezaOsamaRandal CurtmolaKhanBurns. "Robust remote data checking", Proceedings of the 4th ACM international workshop on Storage security and survivability - StorageSS 08 StorageSS 08, 2008

[28] ZHU, YAN, SHANBIAO WANG, HONGXIN HU, GAIL-JOON AHN, and DI MA. "SECURE COLLABORATIVE INTEGRITY VERIFICATION FOR HYBRID CLOUD ENVIRONMENTS", International Journal of Cooperative Information Systems, 2012.

Authors Profile

Mr. Ankit Chamoli Completed Bachelor of Computer Science From Hemwati Nandan Bahuguna Garhwal University Srinagar Garhwal in 2015 and He is Currently Pursuing Master of Technology under Uttarakhand Technical University Dehradun,India.

Mrs. Anshika Goyal working as an Assistant Professor. Computer Science And Engineering Faculty of Technology, Uttarakhand Technical University, Dehradun, India .