International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I5P106

Volume 68 Issue 5, 18-22, May 2020

Original Article

Hybrid-New Type- Based Proxy Re-Encryption (H-TBPRE) Technique to Ensure Data Integrity in Cloud Computing

Ankit Chamoli [1], Anshika Garg [2]

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

Received Date: 01 April 2020
Revised Date: 16 May 2020
Accepted Date: 17 May 2020

Abstract *- Cloud computing gives a shared pool of assets (computers resources like networks, servers and storage) on the demand of the user in a ubiquitous and simple way that can be provisioned to the user with 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 cloud computing. These demands include both hardware and software resources that 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 that helps in providing such services and also in reducing the cost of implementation, and also adding hardware parts that will help in meeting the requirements of the user. The TBPRE and Proposed H-TBPRE are the techniques that ensure data integrity.*

Keywords *- TBPRE, H-TBPRE, Data Integrity, Cloud.*

I. INTRODUCTION

Cloud Computing is a shared pool of appliances on the basis of the user demand in a very ordered and simple manner that can be easily accessible to the user. NIST provides a very basic definition of cloud computing. It can be concluded from the above discussions that the demands required by the user are fulfilled by cloud computing. These demands include both hardware and software resources that 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 [1]. The users subscribe as per their requirements and access the resources until it wants to. Virtualization is the Technique that helps in providing such services and also reduces implementation costs. It also adds hardware parts that can be further used by the user. In order to access cloud computing, there is no further need for details like the physical location of the system or its configuration. Cloud computing includes several features within it, such as the minimization of cost, improved security level, and so on. The users need not install the software. One can easily access their personal files through the internet connection from any location using this Technique. There are some applications like storage capacity bandwidth that makes it more effective. The storage capacity of different types of data makes it very popular in the technical market. It deals with the huge data storage and high scalability with the numerous resources available. It can be easily installed and accessed by the user from any location of the universe. All it requires is a perfect and strong internet connection [2]. It also provides computing resources with a large amount of data storage capacity and also eliminates the overload of information storage. It tells us about the flexibility, disaster recovery and easy access to the information present inside it. The user can store its data on it without keeping a single copy in their personal computers. Hence, it allows freeing up the space on the drive, so it is also known as A Hard-disk in the sky. As it has many applications, the data available on it is not completely secured [3]. Sometimes, the client forgets to maintain the copy of the required data in their system. If we want our data to be confidential for which the network should be properly secured. The network should be properly secured so that the user can store their data without any trust issues because the security of the user is the main concern. Security maintenance is very difficult. The user can delete the less used data in order to reduce the storage capacity, and he can also hide the mistakes just to have a good reputation in the market. These days, information security is ending up noticeably more important in data storage and transmission. Images are generally used in a few processes. Along these lines, the protection of picture data from unauthorized get is important. Picture encryption assumes a huge part in the field of information hiding. Image hiding or encrypting methods and algorithms range from straightforward spatial domain methods to more complicated and reliable frequency domains [4]. From the study of research papers and others, it is concluded that there are no clarifications on which sort of images they are utilizing to perform picture encryption and decryption procedure. It is likewise examined that there is no clarification about the configuration of the machine and platform where all the

experiments are calculated. This method is used to hide the original text, or it removes the sets of alphabets with the sets of numbers. The famous British author Julius Ceaser had used this Technique to remove or replace plain text messages with a set of different alphabets and numbers. It is a unique example of the replacement of words in which each alphabet is replaced by the alphabets present in the other three lines [5]. The homophonic substitution method is also used in which one plain text is replaced by one cypher character. Another method called Poly-alphabetic substitution is also used for the replacement of text which tells the user about the type of substitution method used. Cryptography strategy is used when secret messages are transferred starting with one party then onto the next over a communication line. Cryptography procedure needs some algorithm for encryption of data. The encryption/decryption process alludes to the operation of dividing and replacing an arrangement of the original picture.the picture can be decayed into blocks; every one contains a particular number of pixels. The blocks are transferred into new locations. For a better process, the block size ought to be small because fewer pixels keep their neighbours. First of all, two large distinct prime numbers p, and q, must be generated [6]. The product of these, we call n, is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least, i.e. numbers greater than 10154. We then generate the encryption key e, which must be co-prime to the number.

$$m = \varphi(n) = (p-1)(q-1)$$

II. LITERATURE REVIEW

Mahalingam et al. in 2015 [7] presented that one of the critical components for efficient operation is load balancing in cloud computing. In this paper, the present work is proposed for the distribution of incoming jobs uniformly among the virtual machine or server using a weighted based optimized load balancing approach. Using the cloud simulator and comparing the current result with existing Round Robin and EIRP algorithms, the performance is analyzed. Simulation results have proved that the proposed algorithm has distributed the load uniformly among virtual machines. A cloud simulation simulator is used for the implementation of the algorithm. Cloud simulation is used as a framework that enables modelling simulation and is applicable to make cloud computing infrastructure a self-implied platform that has been used to model data centres, service brokers, hosts, scheduling and allocation policies.

Rajat Saxena et al. in 2016 [8] presented that within the sector of service provision, the cloud computing method is growing fastest today. Within the Paillier homomorphic cryptography (PHC) system, the building blocks of the proposed Technique are provided as building blocks. They include within them the homomorphic tag and combinatorial batch codes. The homomorphic encryption can be obtained within the data blocks with the help of the PHC system. An application-based Hadoop and MapReduce framework is used in order to demonstrate the proposed method. On the basis of numerous parameters, the proposed application is tested. With the help of various experimental results, the effectiveness of the proposed method is presented, which shows that the proposed algorithm outperforms the already existing approaches.

Akanksha Bansal et al. in 2017 [9] presented that in order to store data within the cloud storage in an efficient manner, various techniques have been presented. In order to provide security and integrity, the Electronic Curve Cryptography (ECC) algorithm is utilized here. A certain algorithm is utilized in order to generate and encrypt Metadata which will help in enhancing the security and providing confidentiality to the data. With the help of various experimental results, the novelty of the proposed work is to be studied. With the help of authentication, the data is saved within the cloud storage. Further, the Electronic Curve Cryptography algorithm in order to verify the integrity of the data that is being stored and the manner in which the processing time is being minimized.

Xuefeng Liu et al. in 2017 [10] presented a study related to the integrity auditing problems arising within the storage of cloud deduplication 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 deduplication along with the elimination of the cypher-text redundancy, this method is known to be storage efficient. The evaluation of the performance of the proposed method is done with the help of conducting various experiments, and the effectiveness and efficiency of this method are ensured on the basis of the results achieved.

Andrey N. Rukavitsyn et al. in 2017 [11] presented that there is complete access provided to the user's data to the cloud providers. The paper proposes a method that describes the utilization of partitioned services outside the cloud for authentication, data administration and metadata stockpiling to eliminate the likelihood of getting unapproved access to data and the utilization of metadata to perform integrity control. The owner of the database limits the entrance to data that is stored in an encrypted frame and does not enable the provider to connect with the database. The unpredictability of the encryption algorithm and utilization of methods of data handling in distributed computing will enable the enhancement of data security and hacking resistance. Moreover, it will be relatively impossible to compromise data because of confirmation of checksums stored by the auditor.

Ankit Chamoli et al. in 2018 [12] presented that Cloud computing gives a shared pool of assets on the demand of the user in a ubiquitous and simple way that can be provisioned to the user with very little management effort. In this research work, a 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. 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. In future, the TBPRE technique will be further improved using the SHA algorithm to increase the security of the cloud networks. The proposed improvement will be compared with other algorithms to check its reliability.

III. RESEARCH METHODOLOGY

A single-hop unidirectional H-TBPRE scheme consists of the following algorithms:

A. ***Setup (1k):*** Taking a security parameter 1k as input, the setup algorithm outputs a public parameter param, which specifies the plaintext space P and the type space T.

B. ***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.

C. ***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.

D. ***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.

E. ***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.

F. ***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 2 P or an error symbol _|_ indicating the failure of the decryption.

G. ***Elliptical curve:*** Elliptic curve over field K is defined as a set of solutions of non-singular Weierstrass equation, given below:

$$E: Y^2 + a_1XY + a_3\,Y = X^3 + a_2X^2 + a_4\,X + a_6$$

Non-singularity means that for all points P ∈ E, we have ∂E /∂X (P) != 0 or ∂E/∂Y (P) != 0.

H. ***Elliptic curve key generation****:* Let E be an elliptical curve defined over a finite field name it F_p, Let p be a point in E(F_p), in this suppose P has prime order n. Then the cyclic group of E(F_p) generated by P is:

$$(P) = \{\infty, P, 2P, 3P, \ldots\ldots, (n-1)$$

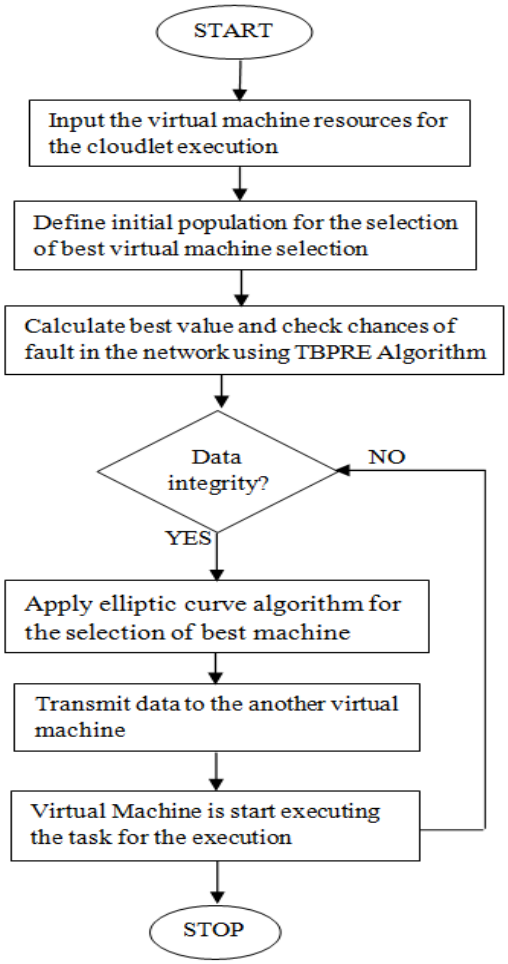
The prime p, the equation of the elliptic curve E, and the point P and its order n are the public domain parameters. A private key is an integer d that is selected uniformly at random from the interval [1, n − 1], and the corresponding public key is Q = d P.

I. ***Elliptic Curve Encryption Scheme:*** Let a plaintext m be first represented as a point M and then encrypted by adding it to kQ, which is a randomly selected integer, and Q is the intended recipient's public key. The sender transmits the points C1 = k P and C2 = M +kQ to the recipient, who uses her private key d to compute

$$dC_1 = d(k\,P) = k(dP)$$

And thereafter recovers M = C2 – kQ. An eavesdropper who wishes to recover M needs to compute kQ. This task of computing k Q from the domain parameters Q, and C1 = k P, is the elliptic curve.

J. ***Flow chart of H-TBPRE:***



IV. RESULTS AND DISCUSSION

A. Graphical Results

The proposed work has been implemented in MATLAB, and the results have been evaluated in terms of several aspects, as shown below.

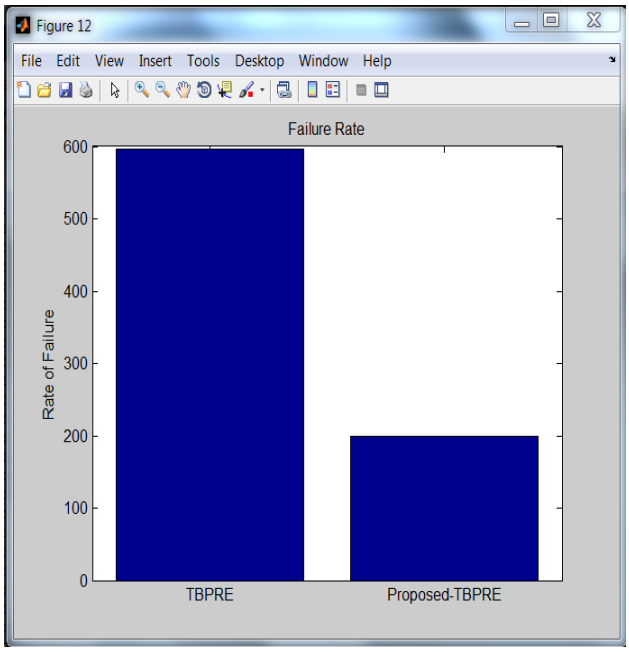


Fig. 1 Failure Rate of TBPRE and Proposed H-TBPRE

As shown in figure 1, the performance of the TBPRE and Proposed H-TBPRE is shown, and it has been analyzed that the failure rate of Proposed H-TBPRE is less.

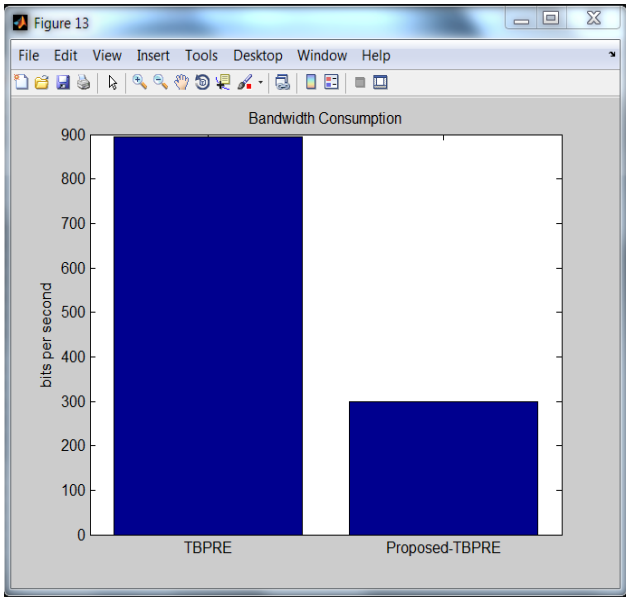


Fig. 2 Bandwidth Consumption of TBPRE and Proposed H-TBPRE

As shown in figure 2, the performance of the TBPRE and Proposed H-TBPRE is shown, and it has been analyzed that bandwidth consumption of Proposed H-TBPRE is less.

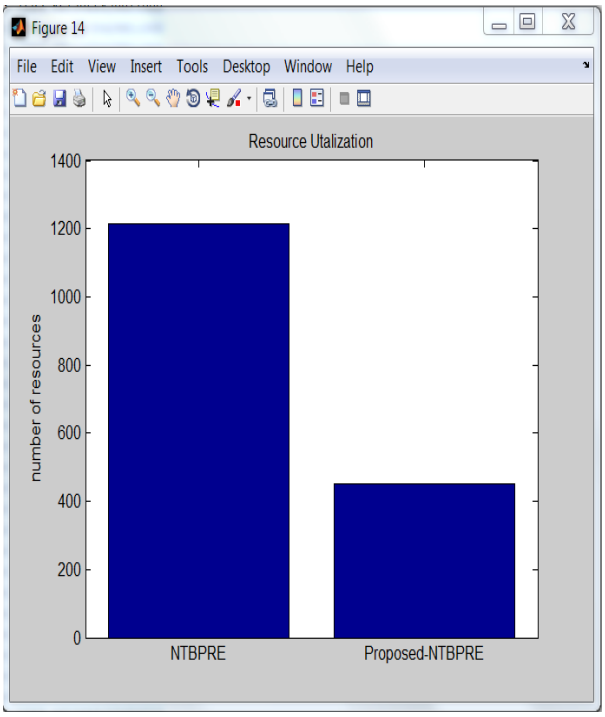


Fig. 3 Resource Utilization of TBPRE and Proposed H-TBPRE

As shown in figure 3, the performance of the TBPRE and Proposed H-TBPRE is shown, and it has been analyzed that resource utilization of Proposed H-TBPRE is less.

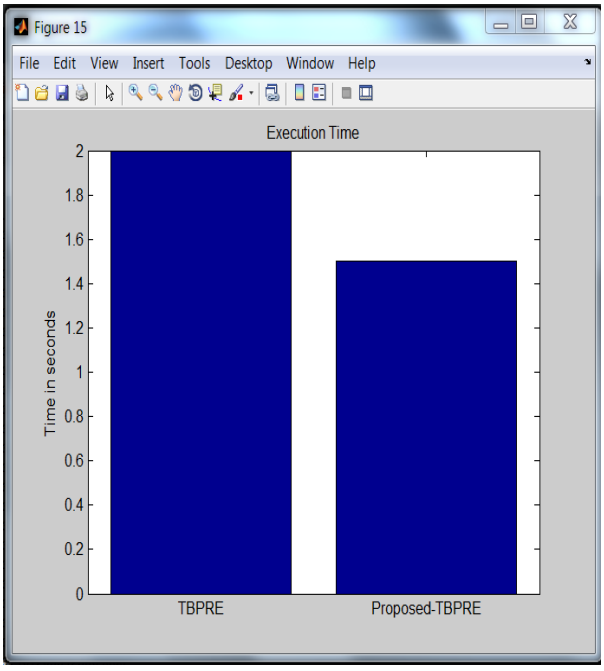


Fig. 4 Execution Time of TBPRE and Proposed H-TBPRE

As shown in figure 4, the performance of the TBPRE and Proposed H-TBPRE is shown, and it has been analyzed that the execution time of Proposed H-TBPRE is less.

B. Qualitative Comparison

PARAMETER	TBPRE	Proposed H-TBPRE
The method used for Data integrity	Key Generation algorithm.	Key Generation algorithm.
Dynamic support	Yes, Dynamic support such as insertion, deletion, modification and updating functions are allowed.	Yes, Dynamic support such as insertion, deletion, modification and updating functions are allowed.
Computation power	It requires low computation power.	It requires more computation power.
Data support	This Technique is applicable for both static and dynamic data.	This Technique is applicable for both static and dynamic data.
Error correction	Lack of error-correcting codes to address.	As same as TBPRE, Lack of error-correcting codes to address.
Client support	Not suitable for the thin client.	As same as TBPRE, Not suitable for the thin client.
Throughput	Low Throughput.	High Throughput.

C. Quantitative Comparison

PARAMETER	TBPRE	Proposed H-TBPRE
Failure rate	400	150
Bandwidth Consumption	600	250
Resource Utilization	1200	420
Execution Time	2	1.5

V. CONCLUSION

In this work, it has been concluded that cloud computing provides shared assets depending on the requirements of the user in the present and in a simpler manner that can be easily accessible by the user. In this research work, these issues have been resolved by proposing a new technique, i.e. H-TBPRE, the new type based proxy re-encryption technique (TBPRE) and Proposed Hybrid new type based proxy re-encryption technique (Proposed H-TBPRE) techniques are implemented and compared on these parameters, i.e. Failure rate, Bandwidth Consumption, Resource Utilization and Execution Time which ensure data integrity in the cloud computing network. From Fig 1, Fig 2, Fig 3 and Fig 4, it is concluded that the Proposed H-TBPRE is more efficient than the TBPRE. It has been analyzed that the Proposed H-TBPRE algorithm is better performance in terms of failure rate, bandwidth consumption, resource utilization and execution time.

REFERENCES

[1] Ravi Jhawar, Vincenzo Piuri, and Marco Santambrogio, Fault Tolerance Management in Cloud Computing: A System-Level Perspective (2012) IEEE 1932-8184

[2] Deepak Poola, Kotagiri Ramamohanarao, and Rajkumar Buyya, Fault-Tolerant Workflow Scheduling Using Spot Instances on Clouds, ICCS, 29(2014) 523–533.

[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, 7(2016) 485-492.

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

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

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

[7] Mahalingam, Nandhalakshmi Nithya, Efficient Load Balancing in Cloud Computing Using Weighted Throttled Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, 3(2015) 5409 – 5415.

[8] Rajat Saxena and Somnath Dey, Cloud Audit: A Data Integrity Verification Approach for Cloud Computing, Procedia Computer Science 89(2016) 142 – 151.

[9] Akanksha Bansal, Arun Agrawal, Providing Security, Integrity and Authentication Using ECC Algorithm in cloud storage, International Conference on Computer Communication and Informatics (ICCCI) (2017).

[10] 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.

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

[12] Ankit Chamoli, Anshika Goyal, Data Integrity and Performance Comparison of New Type- Based Proxy Re-encryption (TB-PRE) and Provable Data Possession (PDP) in Mobile Cloud Computing International Journal of Computer Sciences and Engineering (IJCSE)6(5)(2018).